



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Cox Communications SIP Trunk with Avaya Aura® Communication Manager 8.0, Avaya Aura® Session Manager 8.0 and Avaya Session Border Controller for Enterprise 7.2 – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Cox Communications and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager 8.0, Avaya Aura® Communication Manager 8.0, Avaya Session Border Controller for Enterprise 7.2 and various Avaya endpoints.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Cox 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	5
2.2.	TEST RESULTS	6
2.3.	SUPPORT.....	6
3.	REFERENCE CONFIGURATION	7
4.	EQUIPMENT AND SOFTWARE VALIDATED.....	8
5.	CONFIGURE AVAYA AURA® COMMUNICATION MANAGER.....	10
5.1.	LICENSING AND CAPACITY	10
5.2.	SYSTEM FEATURES.....	12
5.3.	IP NODE NAMES.....	13
5.4.	CODECS.....	13
5.5.	IP NETWORK REGION FOR MEDIA GATEWAY, MEDIA SERVER	15
5.6.	CONFIGURE IP INTERFACE FOR PROCR	18
5.7.	SIGNALING GROUP	18
5.8.	TRUNK GROUP	20
5.9.	CALLING PARTY INFORMATION.....	25
5.10.	OUTBOUND ROUTING	26
5.11.	INCOMING CALL HANDLING TREATMENT	30
5.12.	CONTACT CENTER CONFIGURATION	31
5.12.1.	Announcements	31
5.12.2.	ACD Configuration for Call Queued for Handling by Agent.....	31
5.13.	AVAYA AURA® COMMUNICATION MANAGER STATIONS	35
5.14.	SAVE AVAYA AURA® COMMUNICATION MANAGER CONFIGURATION CHANGES.....	35
6.	CONFIGURE AVAYA AURA® SESSION MANAGER	36
6.1.	AVAYA AURA® SYSTEM MANAGER LOGIN AND NAVIGATION	37
6.2.	SPECIFY SIP DOMAIN	39
6.3.	ADD LOCATION	40
6.4.	ADD SIP ENTITIES	41
6.4.1.	Configure Session Manager SIP Entity.....	42
6.4.2.	Configure Communication Manager SIP Entity	44
6.4.3.	Configure Avaya Session Border Controller for Enterprise SIP Entity	45
6.5.	ADD ENTITY LINKS	45
6.6.	CONFIGURE TIME RANGES	47
6.7.	ADD ROUTING POLICIES	47
6.8.	ADD DIAL PATTERNS	49
7.	CONFIGURE AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE	53
7.1.	LOG IN TO AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE	53
7.2.	GLOBAL PROFILES.....	56
7.2.1.	Configure Server Interworking Profile - Avaya Site	56
7.2.2.	Configure Server Interworking Profile – Cox Communications SIP Trunk Site	57
7.2.3.	Configure Signaling Manipulation.....	58
7.2.4.	Configure Server – Avaya Site	59
7.2.5.	Configure Server – Cox Communications SIP Trunk.....	61
7.2.6.	Configure Routing – Avaya Site	64
7.2.7.	Configure Routing – Cox Communications SIP Trunk Site	65
7.2.8.	Configure Topology Hiding	66

7.3.	DOMAIN POLICIES	68
7.3.1.	Create Media Rules.....	68
7.3.2.	Create Endpoint Policy Groups	70
7.4.	DEVICE SPECIFIC SETTINGS.....	71
7.4.1.	Manage Network Settings.....	71
7.4.2.	Create Media Interfaces.....	74
7.4.3.	Create Signaling Interfaces.....	75
7.4.4.	Configuration Server Flows.....	76
7.4.4.1	Create End Point Flows – SMVM Flow.....	76
7.4.4.2	Create End Point Flows – Cox Communications SIP Trunk Flow.....	77
8.	COX COMMUNICATIONS SIP TRUNK CONFIGURATION.....	78
9.	VERIFICATION STEPS.....	78
10.	CONCLUSION.....	79
11.	REFERENCES.....	80
12.	APPENDIX A – REMOTE WORKER CONFIGURATION	81
12.1.	NETWORK MANAGEMENT ON AVAYA SBCE	82
12.2.	MEDIA INTERFACE ON AVAYA SBCE	84
12.3.	SIGNALING INTERFACE ON AVAYA SBCE.....	85
12.4.	ROUTING PROFILE ON AVAYA SBCE	85
12.5.	USER AGENT ON AVAYA SBCE	88
12.6.	APPLICATION RULES ON AVAYA SBCE	89
12.7.	END POINT POLICY GROUPS ON AVAYA SBCE.....	91
12.8.	END POINT FLOWS ON AVAYA SBCE	91
12.8.1.	Subscriber Flow	91
12.8.2.	Server Flow on Avaya SBCE.....	94
12.8.2.1	Remote Worker Server Flow	94
12.8.2.2	Trunking Server Flow	95
12.9.	SYSTEM MANAGER	96
12.9.1.	Modify Session Manager Firewall: Elements → Session Manager → Network Configuration → SIP Firewall.....	96
12.9.2.	Disable PPM Limiting: Elements → Session Manager → Session Manager Administration	98
12.10.	REMOTE WORKER CLIENT CONFIGURATION	99
	SIP Global Settings Screen	99
13.	APPENDIX B - SIGMA SCRIPT	100
14.	APPENDIX C - COX MANAGED CPE CONFIGURATION	101
14.1.	COX MANAGED CPE LOGIN	101
14.2.	NETWORK CONFIGURATION	102
14.3.	VLAN CONFIGURATION	104
14.4.	VOIP SIP SETTINGS	105
14.5.	VOIP SURVIVABILITY	106
14.6.	ALG TRUNKING CONFIGURATION	107
14.7.	SIP ROUTING CONFIGURATION	109

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Cox Communications and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager 8.0, Avaya Aura® Communication Manager 8.0, Avaya Session Border Controller for Enterprise (Avaya SBCE) 7.2 and various Avaya endpoints. Cox managed CPE (Edgewater Edgemarc 2900E SIP Application-Layer Gateway) is included as part of the Service Provider service and not as part of the CPE solution (See **Section 14 Appendix C** for more information).

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

2. General Test Approach and Test Results

The general test approach was to connect a simulated enterprise site to Cox Communications SIP Trunk 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.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with this Application Note, the interface between Avaya systems and the Cox Communications SIP Trunk Service did not include use of any specific encryption features as requested by Cox Communications.

Encryption (TLS/SRTP) was used internal to the enterprise between Avaya products.

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 Avaya deskphone types including H.323, SIP, digital, and analog 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 Avaya deskphone types including H.323, SIP, digital, and analog 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 softphones. Two Avaya soft phones were used in testing: Avaya one-X[®] Communicator (1XC) and Avaya Equinox[™] for Windows. 1XC supports two work modes (Computer and Other Phone). Each supported mode was tested. 1XC also supports two Voice over IP (VoIP) protocols: H.323 and SIP. Both protocols were tested. Avaya Equinox[™] for Windows was used in testing as a simple SIP endpoint for basic inbound and outbound calls
- SIP transport using UDP, port 5060, between the Avaya enterprise and Cox Communications
- Direct IP-to-IP Media (also known as “Shuffling”) over a SIP Trunk. Direct IP-to-IP Media allows Communication Manager to reconfigure the RTP path after call establishment directly between the Avaya phones and the Avaya SBCE releasing media processing resources on the Avaya Media Gateway or Avaya Media Server.
- Various call types including: local call, international, outbound toll-free, outbound to assisted operator, local directory assistance 411 and 911 emergency call
- Codec G.711MU, G.711A
- 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 EC500 mobility (extension to cellular)
- SIP re-Invite/Update in off-net call transfer
- SIP Diversion/PAI header in off-net call forward
- Call Center scenarios
- Fax G.711 pass-through mode
- DTMF - RFC2833
- Remote Worker

The following was not supported:

- TLS/SRTP SIP transport
- The inbound toll-free service

- Use of the SIP REFER method for network call redirection (transferring calls with the PSTN back to the PSTN)
- Fax T.38 mode

2.2. Test Results

Interoperability testing of Cox Communications was completed with successful results for all test cases.

2.3. Support

For technical support on the Avaya products described in these Application Notes visit:
<http://support.avaya.com>.

For technical support on Cox Communications SIP Trunking, contact Cox Communications at
<http://www.cox.com>

3. Reference Configuration

Figure 1 illustrates a sample Avaya SIP-enabled enterprise solution connected to Cox Communications SIP Trunk. 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.

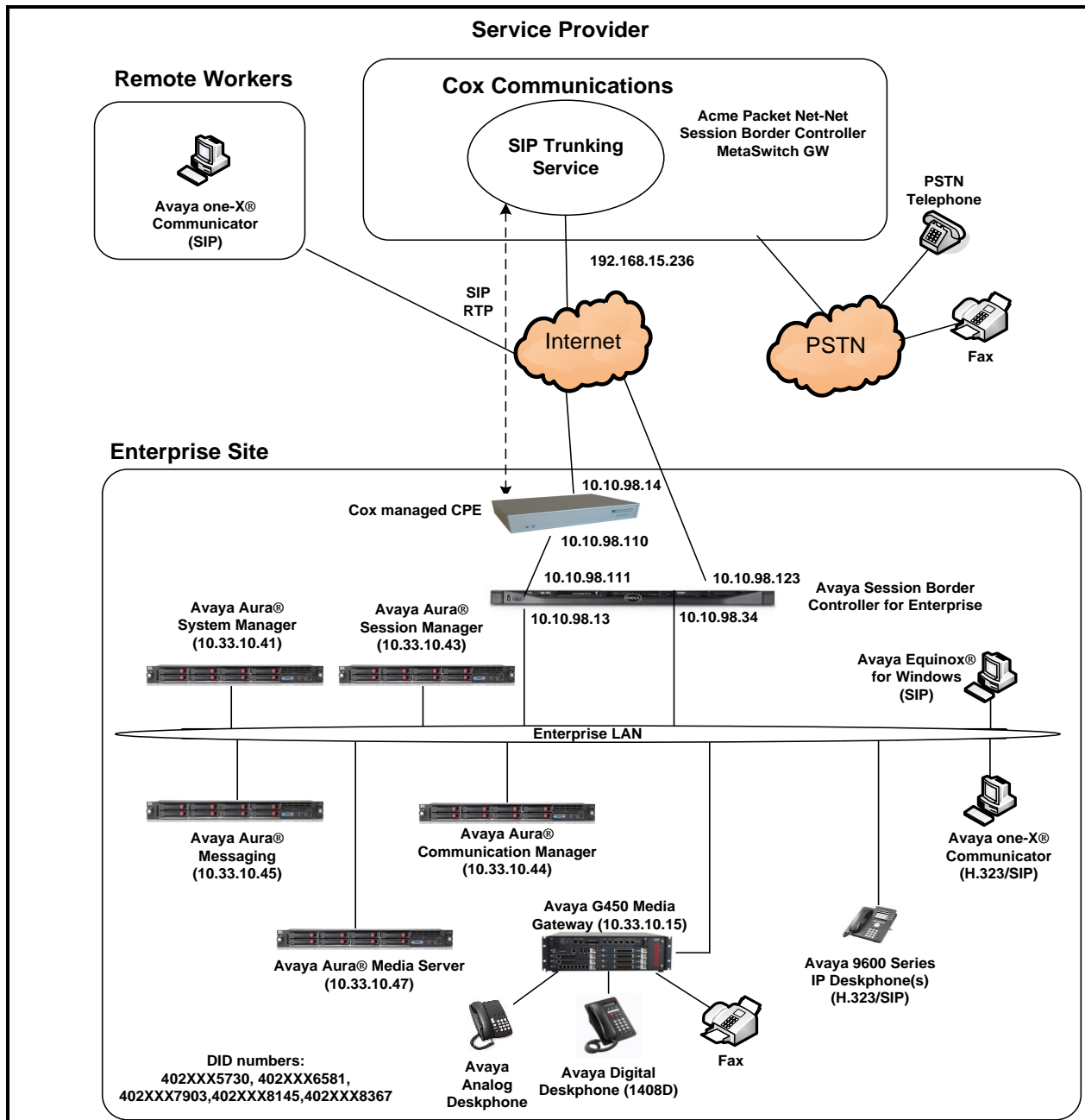


Figure 1: Avaya IP Telephony Network and Cox Communications SIP Trunk

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 Aura® Communication Manager running on VMware®-based Avaya appliance	8.0.0.1.2.822.24826
Avaya G450 Media Gateway <ul style="list-style-type: none"> – MM711AP Analog – MM712AP Digital – MM710AP 	HW2 FW40.20 HW46 FW096 HW10 FW014 HW5 FW020
Avaya Aura® Session Manager running on VMware®-based Avaya appliance	8.0.0.0.800035
Avaya Aura® System Manager running on VMware®-based Avaya appliance	8.0 Build-8.0.0.0.931077 Revision 8.0.0.0.098090
Avaya Aura® Messaging running on VMware®-based Avaya appliance	7.1.0.0.532.0
Avaya Aura® Media Server running on VMware®-based Avaya appliance	8.0.0.169 A6
Avaya Session Border Controller for Enterprise running on Dell R210 V2 Server	7.2.2.1-04-16104
Avaya 9621G IP Deskphone (SIP)	Avaya® Deskphone SIP 7.1.3.0.11
Avaya 9621G IP Deskphone (H.323)	Avaya® IP Deskphone 6.7.1_04
Avaya 9641 IP Deskphone (H.323)	Avaya® IP Deskphone 6.7.1_04
Avaya Digital Deskphone (1408D)	R48
Avaya Equinox™ for Windows	3.4.10.10.2
Avaya one-X® Communicator (H.323 & SIP)	6.2.12.23-SP12P13
Avaya Analog Deskphone	N/A
HP Officejet 4500 Fax	N/A
Cox Communications SIP Trunk Components	
Equipment/Software	Release/Version
Cox managed CPE	Version 14.9.3
MetaSwitch GW	V4.1.40_SU15_P01.03

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.

Note: It is assumed the general installation of VMware®- based Avaya Appliance Virtualization Platform, Avaya Aura® Communication Manager, Avaya Aura® System Manager, Avaya Aura® Session Manager, Avaya Aura® Messaging, Avaya Aura® Media Server and Avaya Media Gateway has been previously completed and is not discussed in this document.

5. Configure Avaya Aura® Communication Manager

This section describes the procedure for configuring Communication Manager for Cox Communications SIP Trunk.

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 30000 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 12
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:		12000	0
Maximum Concurrently Registered IP Stations:		18000	2
Maximum Administered Remote Office Trunks:		12000	0
Maximum Concurrently Registered Remote Office Stations:		18000	0
Maximum Concurrently Registered IP eCons:		414	0
Max Concur Registered Unauthenticated H.323 Stations:		100	0
Maximum Video Capable Stations:		41000	0
Maximum Video Capable IP Softphones:		18000	5
Maximum Administered SIP Trunks:		30000	100
Maximum Administered Ad-hoc Video Conferencing Ports:		24000	0
Maximum Number of DS1 Boards with Echo Cancellation:		688	0

Figure 2: System-Parameters Customer-Options Form – Page 2

On **Page 4**, verify that **ARS** is set to **y**.

display system-parameters customer-options		Page 4 of 12
OPTIONAL FEATURES		
Abbreviated Dialing Enhanced List? n	Audible Message Waiting? y	
Access Security Gateway (ASG)? n	Authorization Codes? y	
Analog Trunk Incoming Call ID? y	CAS Branch? n	
A/D Grp/Sys List Dialing Start at 01? y	CAS Main? n	
Answer Supervision by Call Classifier? y	Change COR by FAC? n	
ARS? y	Computer Telephony Adjunct Links? y	
ARS/AAR Partitioning? y	Cvg Of Calls Redirected Off-net? y	
ARS/AAR Dialing without FAC? n	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	Digital Loss Plan Modification? y	
Async. Transfer Mode (ATM) Trunking? n	DS1 MSP? y	
ATM WAN Spare Processor? n	DS1 Echo Cancellation? y	
ATMS? y		
Attendant Vectoring? Y		

Figure 3: System-Parameters Customer-Options Form – Page 4

On **Page 6**, verify that **Private Networking** and **Processor Ethernet** are set to **y**.

display system-parameters customer-options		Page 6 of 12
OPTIONAL FEATURES		
Multinational Locations? n	Station and Trunk MSP? y	
Multiple Level Precedence & Preemption? n	Station as Virtual Extension? y	
Multiple Locations? n		
Personal Station Access (PSA)? y	System Management Data Transfer? n	
PNC Duplication? n	Tenant Partitioning? y	
Port Network Support? n	Terminal Trans. Init. (TTI)? y	
Posted Messages? y	Time of Day Routing? y	
	TN2501 VAL Maximum Capacity? y	
	Uniform Dialing Plan? y	
Private Networking? y	Usage Allocation Enhancements? y	
Processor and System MSP? y		
Processor Ethernet? y	Wideband Switching? y	
	Wireless? n	
Remote Office? y		
Restrict Call Forward Off Net? y		
Secondary Data Module? y		

Figure 4: System-Parameters Customer-Options Form – Page 6

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? n
      Trunk-to-Trunk Transfer: all
      Automatic Callback with Called Party Queuing? n
      Automatic Callback - No Answer Timeout Interval (rings): 3
      Call Park Timeout Interval (minutes): 10
      Off-Premises Tone Detect Timeout Interval (seconds): 20
      AAR/ARS Dial Tone Required? y
```

Figure 5: System-Parameters Features Form – Page 1

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. The value of **anonymous** is replaced for restricted numbers and unavailable numbers (refer to **Section 5.8**).

```
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:
      International Access Code:

      SCCAN PARAMETERS
      Enable Enbloc Dialing without ARS FAC? n

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

Figure 6: System-Parameters Features Form – Page 9

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 as below:

- Messaging: **Name: AAMVM, IP Address: 10.33.10.45**
- Media Server: **Name: AMS, IP Address: 10.33.10.47**
- Session Manager: **Name: bvwasm2, IP Address: 10.33.10.43**
- Communication Manager: **Name: procr, IP Address: 10.33.10.44**

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	
AAMVM	10.33.10.45	
AMS	10.33.10.47	
bvwasm2	10.33.10.43	
default	0.0.0.0	
procr	10.33.10.44	
procr6	::	

Figure 7: Node-Names IP Form

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. In the compliance test, **ip-codec-set 1** was used for this purpose. Cox Communications supports the **G.711MU**, and **G.711A** codecs. Default values can be used for all other fields.

change ip-codec-set 1

Page1 of 2

IP CODEC SET

Codec Set: 1

Audio	Silence	Frames	Packet
Codec	Suppression	Per Pkt	Size(ms)
1: G.711MU	n	2	20
2: G.711A	n	2	20

Media Encryption

Encryption SRCTP: enforce-unenc-srtp

1: 1-srtp-aescm128-hmac80

2: none

Figure 8: IP-Codec-Set Form – Page 1

On **Page 2**, set the **FAX Mode** to **off**. Cox Communications supports only G.711 pass through mode.

change ip-codec-set 1		Page 2 of 2	
IP CODEC SET			
Allow Direct-IP Multimedia? n			
	Mode	Redundancy	Packet Size (ms)
FAX	off		
Modem	off	0	
TDD/TTY	US	3	
H.323 Clear-channel	n	0	
SIP 64K Data	n	0	20

Figure 9: IP-Codec-Set Form – Page 2

5.5. IP Network Region for Media Gateway, Media Server

Network region provide a means to logically group resources. In the shared Communication Manager configuration used for the testing, both Avaya G450 Media Gateway and Avaya Media Server were tested and used region 1. 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 **bvwddev.com**. This name appears in the From header of SIP messages originating from this IP region
- Enter a descriptive name in the **Name** field
- Enable IP-IP Direct Audio (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya G450 Media Gateway or Avaya Media Server. Set both **Intra-region IP-IP Direct Audio** and **Inter-region IP-IP Direct Audio** to **yes**. Shuffling can be further restricted at the trunk level on the Signaling Group form in **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: 1	Authoritative Domain: bvwddev.com	
Name: procr	Stub Network Region: n	
MEDIA PARAMETERS	Intra-region IP-IP Direct Audio: yes	
Codec Set: 1	Inter-region IP-IP Direct Audio: yes	
UDP Port Min: 2048	IP Audio Hairpinning? n	
UDP Port Max: 3329		
DIFFSERV/TOS PARAMETERS		
Call Control PHB Value: 46		
Audio PHB Value: 46		
Video PHB Value: 26		
802.1P/Q PARAMETERS		
Call Control 802.1p Priority: 6		
Audio 802.1p Priority: 6		
Video 802.1p Priority: 5		
H.323 IP ENDPOINTS		AUDIO RESOURCE RESERVATION PARAMETERS
H.323 Link Bounce Recovery? y	RSVP Enabled? n	
Idle Traffic Interval (sec): 20		
Keep-Alive Interval (sec): 5		
Keep-Alive Count: 5		

Figure 10: IP-Network-Region Form

The following display command shows that **media-gateway 1** is an Avaya G450 Media Gateway configured for **Network Region 1**. It can also be observed that the **Controller IP Address** is the Avaya Processor Ethernet (**10.33.10.44**), and that the gateway **MGP IPv4 Address** is **10.33.10.15**. These fields are not configured in this screen, but just display the current information for the Media Gateway.

```

display media-gateway 1                                     Page 1 of 2
                                MEDIA GATEWAY 1

                                Type: g450
                                Name: g450
                                Serial No: 12TGXXX00244
                                Link Encryption Type: any-ptls/tls
                                Network Region: 1
                                Enable CF? n
                                Location: 1
                                Site Data:

                                Recovery Rule: none

                                Registered? y
                                FW Version/HW Vintage: 40 .20 .0 /2
                                MGP IPV4 Address: 10.33.10.15
                                MGP IPV6 Address:
                                Controller IP Address: 10.33.10.44
                                MAC Address: 3c:3a:73:6b:c5:a8

                                Mutual Authentication? optional

```

Figure 11: Media Gateway – Page 1

The following screen shows Page 2 for Media Gateway 1. The gateway has an **MM712** media module supporting Avaya digital phones in slot **V1**, an **MM711** supporting analog phones on slot **V2**, and the capability to provide announcements and music on hold via “**gateway-announcements**” in logical slot **V9**.

```

display media-gateway 1                                     Page 2 of 2
                                MEDIA GATEWAY 1

                                Type: g450

Slot   Module Type      Name      DSP Type  FW/HW version
V1:    MM712            DCP MM    MP80      170  7
V2:    MM711            ANA MM
V3:
V4:
V5:
V6:
V7:
V8:
V9:    gateway-announcements  ANN VMM

Max Survivable IP Ext: 8

```

Figure 12: Media Gateway – Page 2

The following display command shows that **media-server 1** is an Avaya Media Server configured for **Network Region 1**. It can also be observed that the **Node Name: AMS** (Defined in **Section 5.3**) and the **Signaling Group: 11** (Defined in **Section 5.7**) have been used. These fields are not configured in this screen, but just display the current information for the Media Server.

```
display media-server 1

                                MEDIA SERVER

Media Server ID: 1

    Signaling Group: 11
Voip Channel License Limit: 10
Dedicated Voip Channel Licenses: 10

    Node Name: AMS
    Network Region: 1
                Location: 1
Announcement Storage Area:
```

Figure 13: Media Server

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: 19660
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: 10.33.10.44
Subnet Mask: /24	

Figure 14: IP-Interface Form

5.7. Signaling Group

Use the **add signaling-group** command to create signaling groups.

For the compliance test, signaling group **20** was used for the signaling group between Communication Manager and Session Manager. It was used for outbound and inbound calls between the service provider and the enterprise. It was configured using the parameters highlighted below. Note: The signaling group between Communication Manager and Session Manager used for SIP phones is not mentioned in these Application Notes.

- 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 **tls** (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 **bvwasm2**. 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 unused port for TLS, such as **5061**

- 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 **bvwdev.com**, the enterprise domain
- Set **Direct IP-IP Audio Connections** to **y**. This setting will enable media shuffling on the SIP trunk so that Communication Manager will re-route media traffic directly between the SIP trunk and the enterprise endpoint. Note that the Avaya G450 Media Gateway or Avaya Media Server will not remain in the media path of all calls between the SIP trunk and the endpoint
- Set the **Alternate Route Timer (sec)** to **6**. This defines the number of seconds 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 20                                     Page 1 of 2
                                     SIGNALING GROUP

Group Number: 20                      Group Type: sip
IMS Enabled? n                      Transport Method: tls
  Q-SIP? n
  IP Video? n                      Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y Peer Server: SM
Prepend '+' to Outgoing Calling/Alerting/Diverting/connected Public Numbers? y
Remove '+' from Incoming Called/Calling/Alerting/Diverting/connected Numbers? n

Near-end Node Name: procr                      Far-end Node Name: bvwasm2
Near-end Listen Port: 5061                      Far-end Listen Port: 5061
                                           Far-end Network Region: 1
                                           Far-end Secondary Node Name:

Far-end Domain: bvwdev.com

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

```

Figure 15: Signaling-Group 20

For the compliance test, signaling group **11** was used for the signaling group between Communication Manager and Media Server. It was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**
- Set the **Transport Method** to the value of **tls** (Transport Layer Protocol). The transport method specified here is used between Communication Manager and Media Server
- Set the **Peer Detection Enabled** field to **n** and **Peer Server** to **AMS**
- 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 **AMS**. This node name maps to the IP Address of Media Server as defined in **Section 5.3**
- Set the **Near-end Listen Port** to **9061** and **Far-end Listen Port** to a valid unused port for TLS, such as **5071**
- 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 **10.33.10.47** (This is Media Server IP Address)

change signaling-group 11
Page 1 of 2

SIGNALING GROUP

Group Number: 11

Group Type: sip

Transport Method: tls

Peer Detection Enabled? n

Peer Server: AMS

Near-end Node Name: procr

Far-end Node Name: AMS

Near-end Listen Port: 9061

Far-end Listen Port: 5071

Far-end Network Region: 1

Far-end Domain: 10.33.10.47

Figure 16: Signaling-Group 11

5.8. Trunk Group

Use the **add trunk-group** command to create a trunk group for the signaling group for Session Manager created in **Section 5.7**.

For the compliance test, trunk group **20** was used for both outbound and inbound calls to the service provider. It was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**
- Enter a descriptive name for the **Group Name**
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field. (e.g., ***020**). Note: Refer to **Section 5.10** for adding * in dialing plan
- Set Class of Restriction (**COR**) to **1**
- Set **Direction** to **two-way** for trunk group **20**
- 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 **20** was associated to signaling group **20**
- 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 20		Page 1 of 4	
TRUNK GROUP			
Group Number: 20	Group Type: sip	CDR Reports: y	
Group Name: SIP Trunks	COR: 1	TN: 1	TAC: *020
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: public-ntwrk	Auth Code? n		
		Member Assignment Method: auto	
		Signaling Group: 20	
		Number of Members: 50	

Figure 17: Trunk-Group – Page 1

On **Page 2**, set the **Redirect On OPTIM Failure** timer to the same amount of time as the **Alternate Route Timer** on the signaling group form in **Section 5.7**. Note that the **Redirect On OPTIM Failure** timer is defined in milliseconds. Verify that the **Preferred Minimum Session Refresh Interval (sec)** is set to a value acceptable to the service provider. This value defines the interval that UPDATES must be sent to keep the active session alive. For the compliance test, the value of **1200** seconds was used.

add trunk-group 20		Page 2 of 4
Group Type: sip		
TRUNK PARAMETERS		
Unicode Name: auto		
Redirect On OPTIM Failure: 6000		
SCCAN? n	Digital Loss Group: 18	
Preferred Minimum Session Refresh Interval (sec): 1200		
Disconnect Supervision - In? y Out? y		
XOIP Treatment: auto Delay Call Setup When Accessed Via IGAR? n		

Figure 18: Trunk-Group – Page 2

On **Page 3**, set the **Numbering Format** field to **public**. This field specifies the format of the calling party number (CPN) sent to the far-end (refer to **Section 5.9** for the public-unknown-numbering format). The compliance test used 10-digit numbering format. Thus, **Numbering Format** was set to **public** and the **Numbering Format** field in the route pattern was set to **public** (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.

add trunk-group 20		Page 3 of 4
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Maintenance Tests? y
Numbering Format: public		
UI Treatment: service-provider		
Replace Restricted Numbers? y		
Replace Unavailable Numbers? y		
Hold/Unhold Notifications? y		
Modify Tandem Calling Number: no		
Show ANSWERED BY on Display? y		

Figure 19: Trunk-Group – Page 3

On **Page 4**, the **Network Call Redirection** field should be set to **n** so that CM will not send SIP Refer in redirected calls. Note: In the compliance test, Cox Communications did not support SIP Refer. Cox Communications supported SIP re-Invite/Update in redirected calls.

Set the **Send Diversion Header** field to **y** and the **Support Request History** field to **y**. The **Send Diversion Header** and **Support Request History** fields provide additional information to the network if the call has been redirected. Note: For voice mail purposes, Communication Manager sends SIP Invite with History Info to Avaya Aura Messaging. The **Diversion Header** is needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios.

add trunk-group 20	Page 4 of 4
PROTOCOL VARIATIONS	
Mark Users as Phone? n	
Prepend '+' to Calling/Alerting/Diverting/Connected Number? n	
Send Transferring Party Information? n	
Network Call Redirection? n	
Send Diversion Header? y	
Support Request History? y	
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	
Accept Redirect to Blank User Destination? n	
Enable Q-SIP? n	
Interworking of ISDN Clearing with In-Band Tones: keep-channel-active	

Figure 20: Trunk-Group – Page 4

5.9. Calling Party Information

The calling party number is sent in the SIP “From”, “Contact” and “P-Asserted-Identity” headers. Since public numbering was selected to define the format of this number (**Section 5.8**), use the **change public-unknown-numbering** command to create an entry for each extension which has a DID assigned. The DID numbers are provided by the service provider. Each DID number is assigned to one enterprise internal extension or Vector Directory Numbers (VDNs), and 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 public-unknown-numbering entry can be applied for all extensions. In the compliance test, stations with a 4-digit extension beginning with **57, 65, 79, 81, 83** will send the calling party number as the **CPN Prefix** plus the extension number.

Note: The entry applies to SIP connection to Session Manager, therefore the resulting number must be a complete E.164 number. Communication Manager automatically inserts a ‘+’ in front of user number in From, P-Asserted-Identity, Contact, and Diversion headers. This plus sign will be removed by using the SIP manipulation on SBCE (See **Session 7.2.3**).

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp (s)	CPN Prefix	Total CPN Len	
4	57	20	402XXX	10	
4	65	20	402XXX	10	
4	79	20	402XXX	10	
4	81	20	402XXX	10	
4	83	20	402XXX	10	
					Total Administered: 3
					Maximum Entries: 240

Figure 21: Public-Unknown-Numbering Form

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 configuration is illustrated below. Use the **change dialplan analysis** command to define the **Dialed String** as following:

- **Dialed String** beginning with **57, 65, 79, 81, 83** for extension (**ext**)
- **Dialed String** beginning with **9** for feature access code (**fac**)
- **Dialed String** beginning with ***** for dial access code (**dac**). It is used for Trunk Access Code (TAC) defined on Trunk Group 20 in **Section 5.8**

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	
57	4	ext							
65	4	ext							
79	4	ext							
81	4	ext							
83	4	ext							
181	4	ext							
189	4	ext							
3	4	ext							
9	1	fac							
800	4	ext							
*	4	dac							

Figure 22: Dialplan–Analysis Form

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

change feature-access-codes	Page 1 of 11
FEATURE ACCESS CODE (FAC)	
Abbreviated Dialing List1 Access Code:	
Abbreviated Dialin3g List2 Access Code:	
Abbreviated Dialing List3 Access Code:	
Abbreviated Dial - Prgm Group List Access Code:	
Announcement Access Code: *111	
Answer Back Access Code:	
Attendant Access code:	
Auto Alternate Routing (AAR) Access Code:	
Auto Route Selection (ARS) - Access Code 1: 9	Access Code 2:
Automatic Callback Activation:	Deactivation:
Call Forwarding Activation Busy/DA: All:	Deactivation:
Call Forwarding Enhanced Status: Act:	Deactivation:
Call Park Access Code:	
Call Pickup Access Code:	
CAS Remote Hold/Answer Hold-Unhold Access Code:	
CDR Account Code Access Code:	
Change COR Access Code:	
Change Coverage Access Code:	
Conditional Call Extend Activation:	Deactivation:
Contact Closure Open Code:	Close Code:

Figure 23: Feature–Access-Codes Form

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 20** which contains the SIP trunk group 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 String	Total		Route	Call	Node	ANI
	Min	Max	Pattern	Type	Num	Req'd
0	1	15	20	pubu		
1404	11	11	20	pubu		n
1613	11	11	20	pubu		n
1647	11	11	20	pubu		n
1800	11	11	20	pubu		n
4026	10	10	20	pubu		n
411	3	3	20	svcl		n
911	3	3	20	svcl		n

Figure 24: ARS–Analysis Form

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 **20** 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 **20** 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 **pub-unk** since public-unknown-numbering format should be used for this route (see **Section 5.8**)

change route-pattern 20															Page 1 of 3			
Pattern Number: 5 Pattern Name: SP																		
SCCAN? n Secure SIP? n																		
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted								DCS/	IXC		
No			Mrk	Lmt	List	Del	Digits								QSIG			
								Dgts							Intw			
1:	20	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	pub-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

Figure 25: Route-Pattern Form

Use the **change cor 1** command to change the Class of Restriction (COR) for the outbound call over SIP trunk. Set **Calling Party Restriction: none**. This setting allows the outbound call using feature access code (fac) 9 over SIP trunks.

change cor 1		Page 1 of 23	
CLASS OF RESTRICTION			
COR Number: 1			
COR Description:			
FRL: 0	APLT? y		
Can Be Service Observed? n	Calling Party Restriction: none		
Can Be A Service Observer? n	Called Party Restriction: none		
Time of Day Chart: 1	Forced Entry of Account Codes? n		
Priority Queuing? n	Direct Agent Calling? n		
Restriction Override: none	Facility Access Trunk Test? n		
Restricted Call List? n	Can Change Coverage? n		
Access to MCT? y	Fully Restricted Service? n		
Group II Category For MFC: 7	Hear VDN of Origin Annc.? n		
Send ANI for MFE? n	Add/Remove Agent Skills? n		
MF ANI Prefix:	Automatic Charge Display? n		
Hear System Music on Hold? y	PASTE (Display PBX Data on Phone)? n		
	Can Be Picked Up By Directed Call Pickup? n		
	Can Use Directed Call Pickup? n		
	Group Controlled Restriction: inactive		

Figure 26: Class of Restriction Form

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 the 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 **20**. Use the **change inc-call-handling-trmt trunk-group 20** to convert incoming DID numbers as follows:

- The incoming DID number **402XXX8367** to **8000** by deleting **10** of the incoming digits for voicemail testing purpose. (8000 is voice mail pilot number)
- The incoming DID number **402XXX** to 4-digit extension by deleting **6** of the incoming digits for inbound call testing purpose

change inc-call-handling-trmt trunk-group 20				Page	1 of	3
INCOMING CALL HANDLING TREATMENT						
Service/	Number	Number	Del Insert			
Feature	Len	Digits				
public-ntwrk	10	402XXX8367	10	8000		
public-ntwrk	10	402XXX	6			

Figure 27: Inc-Call-Handling-Trmt Form

5.12. Contact Center Configuration

This section describes the basic commands used to configure Announcements, Hunt-Groups, Vector Directory Numbers (VDNs) and corresponding vectors. These vectors contain steps that invoke Communication Manager to perform various call-related functions.

5.12.1. Announcements

Various announcements will be used within the vectors. In the sample configuration, these announcements were sourced by the Avaya G450 Media Gateway. The following abridged list command summarizes the announcements used in conjunction with the vectors in this section. To add an announcement extension, use the command “add announcement <extension>”. The extension is an unused extension number.

```
list announcement
```

ANNOUNCEMENTS/AUDIO SOURCES				
Announcement Extension	Type	Name	Source	Num of Files
1898	integrated	SP2	001V9	1
1899	integrated	SP1	001V9	1

Figure 28: Announcement Configuration

5.12.2. ACD Configuration for Call Queued for Handling by Agent

This section provides a simple example configuration for VDN, vector, hunt-group, and agent-loginID used to queue inbound calls for handling by an agent.

The following screens show an example ACD hunt group. On page 1, note the bolded values.

display **hunt-group 13**

Page 1 of 3

HUNT GROUP

GROUP NUMBER: 13

ACD? y

Group Name: SP

Queue? y

GROUP EXTENSION: 3211

Vector? y

GROUP TYPE: UCD-MIA

TN: 1

COR: 1

MM Early Answer? n

SECURITY CODE: 1234

Local Agent Preference? n

ISDN/SIP Caller Display:

Queue Limit: unlimited

Calls Warning Threshold: Port:

Time Warning Threshold: Port:

Figure 29: Hunt Group Configuration – Page 1

The following screens show an example ACD hunt group. On the abbreviated page 2 shown below, note that **Skill** is set to **y**.

display hunt-group 13	HUNT GROUP	Page 2 of 3
Skill? y	Expected Call Handling Time (sec): 180	
AAS? n	Service Level Target (% in sec): 80 in 20	

Figure 30: Hunt Group Configuration – Page 2

VDN 7903, shown below, is associated with vector 3

display vdn 7903	VECTOR DIRECTORY NUMBER	Page 1 of 3
	EXTENSION: 7903	
	Name*: Contact Center	
	DESTINATION: VECTOR NUMBER	3
	Attendant Vectoring? n	
	Meet-me Conferencing? n	
	Allow VDN Override? n	
	COR: 1	
	TN*: 1	
	Measured: none	

Figure 31: VDN Configuration

In this simple example, vector 3 briefly plays ring back, then plays announcement 1899 (Step 02). This is an announcement heard when the call is first answered before the call is queued to the skill 13 (Step 03). If an agent is immediately available to handle the call, the call will be delivered to the agent. If an agent is not immediately available, the call will be queued, and the caller will hear announcement 1898 (Step 05). Once an agent becomes available, the call will be delivered to the agent.

```

display vector 3                                     Page 1 of 6

                                CALL VECTOR

      Number: 3                Name: Contact Center
Multimedia? n      Attendant Vectoring? n      Meet-me Conf? n      Lock? n
Basic? y    EAS? y    G3V4 Enhanced? y    ANI/II-Digits? y    ASAI Routing? y
Prompting? y    LAI? y    G3V4 Adv Route? y    CINFO? y    BSR? y    Holidays? y
Variables? y    3.0 Enhanced? y

01 wait-time      2      secs hearing ringback
02 announcement 1899
03 queue-to       skill 13      pri m
04 wait-time      2      secs hearing silence
05 announcement 1898
06 goto step      3              if unconditionally

```

Figure 32: Vector 3 Configuration

The following screen illustrates an example agent-loginID 3311. In the sample configuration, an Avaya IP Deskphone logged in using agent-loginID 3311 and the configured password to staff and take a call for skill 13.

```

add agent-loginID 3311                               Page 1 of 2

                                AGENT LOGINID

      Login ID: 3311                                AAS? n
      Name: SP                                       AUDIX? n
      TN: 1                                         LWC Reception: spe
      COR: 1                                       LWC Log External Calls? n
Coverage Path:                                     AUDIX Name for Messaging:
Security Code: 1234

      LoginID for ISDN/SIP Display? n
      Password: 1234
      Password (enter again): 1234
      Auto Answer: station
      MIA Across Skills: system
      ACW Agent Considered Idle: system
      Aux Work Reason Code Type: system
      Logout Reason Code Type: system
      Maximum time agent in ACW before logout (sec): system
      Forced Agent Logout Time:

```

Figure 33: Agent-loginID Configuration – Page 1

The following abridged screen shows Page 2 for agent-loginID 3311. Note that the Skill Number (SN) has been set to **13**.

Display agent-loginID 3311				Page 2 of 2			
AGENT LOGINID							
Direct Agent Skill:				Service Objective? n			
Call Handling Preference: skill-level				Local Call Preference? n			
	SN	RL	SL		SN	RL	SL
1:	13		1	16:			
2:				17:			

Figure 34: Agent LoginID Configuration – Page 2

To enable a telephone or one-X[®] Agent client to log in with the agent-loginID shown above, ensure that **Expert Agent Selection (EAS) Enabled** is set to **y** as shown in the screen below.

change system-parameters features		Page 11 of 19
FEATURE-RELATED SYSTEM PARAMETERS		
CALL CENTER SYSTEM PARAMETERS		
EAS		
Expert Agent Selection (EAS) Enabled? y		
Minimum Agent-LoginID Password Length: 4		

Figure 35: Enable Expert Agent Selection

5.13. Avaya Aura® Communication Manager Stations

In the sample configuration, a 4-digit station extension was used with the format 5730. Use the **add station 5730** command to add an Avaya H.323 IP Deskphone.

- Enter **Type: 9621, Name: H323-5730, Security Code: 1234, Coverage Path 1: 1, IP SoftPhone: y** (if using this extension as a Softphone such as Avaya one-X® Communicator)
- Leave other values as default

add station 5730		Page 1 of 5
STATION		
Extension: 5730	Lock Messages? n	BCC: 0
Type: 9621	Security Code: *	TN: 1
Port: S000055	Coverage Path 1: 1	COR: 1
Name: H323-5730	Coverage Path 2:	COS: 1
	Hunt-to Station:	Tests? y
STATION OPTIONS		
	Time of Day Lock Table:	
Loss Group: 19	Personalized Ringing Pattern: 1	
	Message Lamp Ext: 5730	
Speakerphone: 2-way	Mute Button Enabled? y	
Display Language: English	Button Modules: 0	
Survivable GK Node Name:		
Survivable COR: internal	Media Complex Ext:	
Survivable Trunk Dest? y	IP SoftPhone? y	
	IP Video softphone? n	
	Short/Prefixed Registration Allowed: default	
	Customizable Labels? y	

Figure 36: Add-Station Form

5.14. 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, Avaya SBCE and Session Manager
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Time Ranges, which define the time-based-routing
- 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.

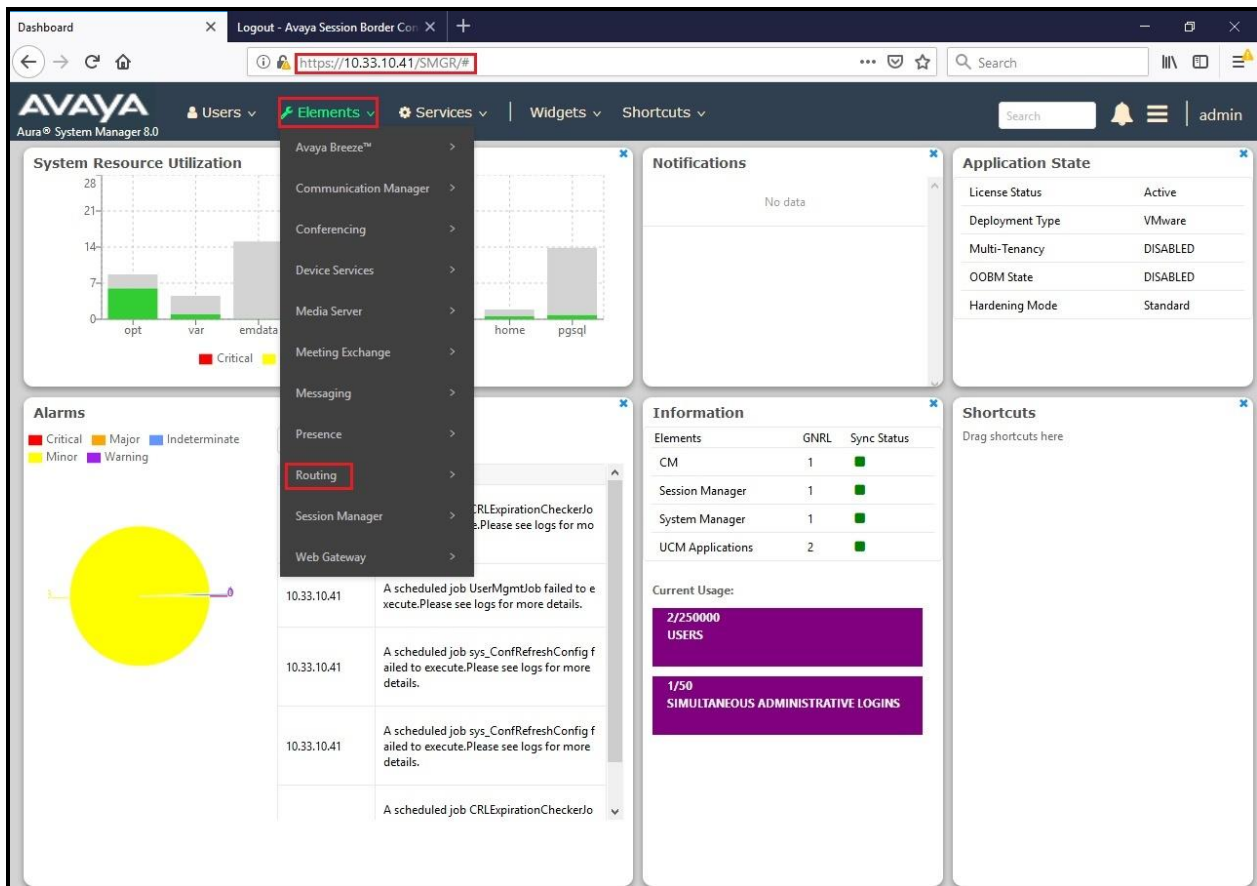


Figure 37: System Manager Home Screen

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.

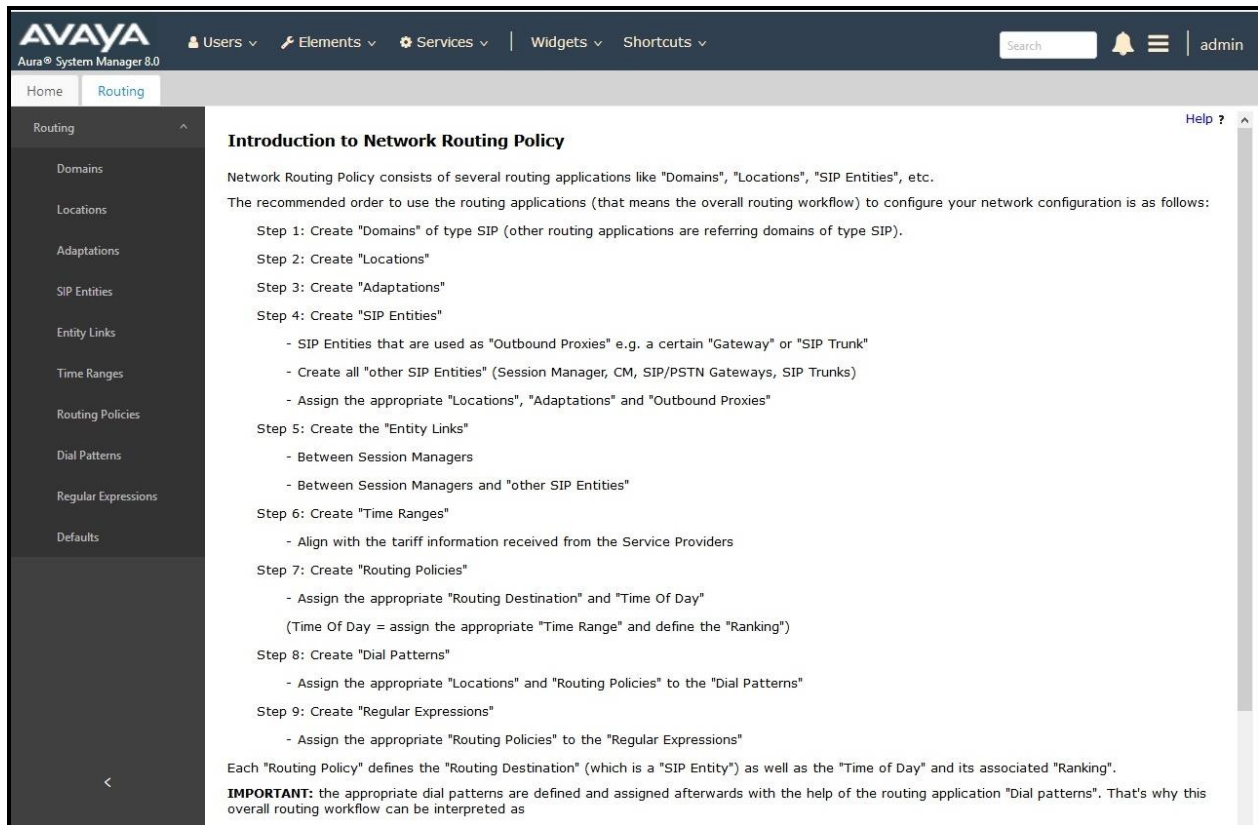


Figure 38: Network Routing Policy

6.2. Specify SIP Domain

Create a SIP Domain for each domain of which Session Manager will need to be aware of in order to route calls. For the compliance test, this includes the enterprise domain **bvwdev.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.

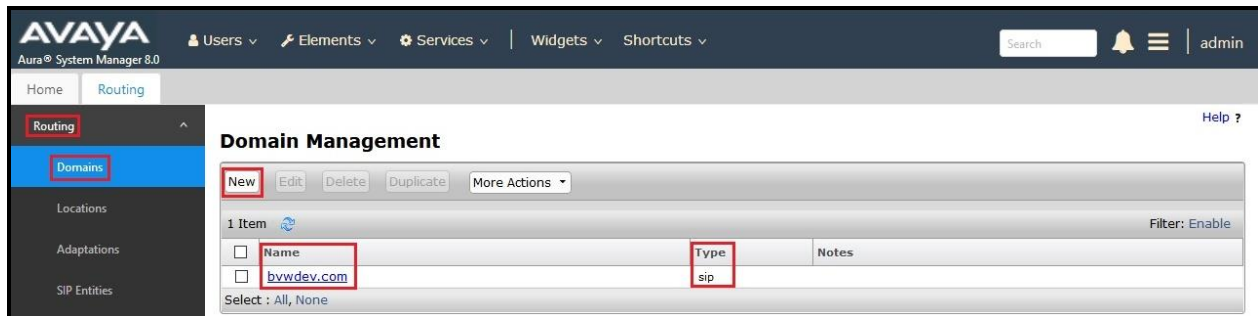


Figure 39: Domain Management

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-GSSCP**, 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

The screenshot shows the Avaya Aura System Manager 8.0 interface. The left navigation pane has 'Routing' and 'Locations' highlighted. The main area is titled 'Location Details' with a 'General' tab selected. The 'Name' field is set to 'Belleville-GSSCP'. Other fields like 'Notes', 'Dial Plan Transparency in Survivable Mode', 'Overall Managed Bandwidth', 'Per-Call Bandwidth Parameters', and 'Alarm Threshold' are visible with their default values.

Section	Field	Value
General	Name	Belleville-GSSCP
	Notes	
Dial Plan Transparency in Survivable Mode	Enabled	<input type="checkbox"/>
	Listed Directory Number	
	Associated CM SIP Entity	
Overall Managed Bandwidth	Managed Bandwidth Units	Kbit/sec
	Total Bandwidth	
	Multimedia Bandwidth	
	Audio Calls Can Take Multimedia Bandwidth	<input checked="" type="checkbox"/>
Per-Call Bandwidth Parameters	Maximum Multimedia Bandwidth (Intra-Location)	2000 Kbit/Sec
	Maximum Multimedia Bandwidth (Inter-Location)	2000 Kbit/Sec
	* Minimum Multimedia Bandwidth	64 Kbit/Sec
	* Default Audio Bandwidth	80 Kbit/sec
Alarm Threshold	Overall Alarm Threshold	80 %

Figure 40: Location Configuration

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

- **IP Address Pattern:** 10.33.10.*, 10.33.5.*, 10.10.98.*
- Click **Commit** to save

IP Address Pattern	Notes
* 10.33.10.*	
* 10.33.5.*	
* 10.10.98.*	

Figure 41: IP Ranges Configuration

Note: 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 on the next page), 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 **SIP Trunk** for Avaya SBCE
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. Adaptation modules were 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-GSSCP**
- **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 **bvwasrm2**. The IP Address of Session Manager's signaling interface is entered for **FQDN or IP Address** **10.33.10.43**. The user will need to select the specific values for the **Location** and **Time Zone**.

The screenshot displays the Avaya Aura System Manager 8.0 web interface. The left sidebar shows the navigation menu with 'Routing' selected. The main content area is titled 'SIP Entity Details' and includes a 'General' tab. The form contains the following fields:

- Name:** bvwasrm2
- IP Address:** 10.33.10.43
- SIP FQDN:** (empty)
- Type:** Session Manager
- Notes:** SM
- Location:** Belleville-GSSCP
- Outbound Proxy:** (empty)
- Time Zone:** America/Toronto
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty)
- SIP Link Monitoring:** Use Session Manager Configuration
- CRLF Keep Alive Monitoring:** CRLF Monitoring Disabled

Buttons for 'Commit' and 'Cancel' are located at the top right of the form. The 'Monitoring' section is visible at the bottom of the form.

Figure 42: Session Manager SIP Entity

To define the ports used by Session Manager, scroll down to the **Listen Ports** section of the **SIP Entity Details** screen. This section is only present for the **Session Manager** SIP Entity.

In the **Listen Ports** 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 **5061** with **TLS** for connecting to Communication Manager and Avaya SBCE

Listen Ports	Protocol	Default Domain	Notes
5061	TLS	bvwdev.com	

Figure 43: 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 **CM8**. 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 **10.33.10.44**. Note that **CM** was selected for **Type**. The user will need to select the specific values for the **Location** and **Time Zone**.

The screenshot displays the Avaya Aura System Manager 8.0 web interface. The left sidebar shows the navigation menu with 'Routing' selected. The main content area is titled 'SIP Entity Details' and includes a 'General' tab. The form contains the following fields and values:

- Name:** CM8
- FQDN or IP Address:** 10.33.10.44
- Type:** CM
- Notes:** (empty)
- Adaptation:** (empty dropdown)
- Location:** Belleville-GSSCP
- Time Zone:** America/Toronto
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:** (empty)
- Securable:** ☐
- Call Detail Recording:** none
- Loop Detection Mode:** Off
- SIP Link Monitoring:** Link Monitoring Enabled

The 'Commit' and 'Cancel' buttons are located at the top right of the form. The 'Loop Detection' and 'Monitoring' sections are visible at the bottom of the form.

Figure 44: 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 **SBCE**. The **FQDN** or **IP Address** field is set to the IP Address of the SBCE's private network interface **10.10.98.13**. Note that **SIP Trunk** was selected for **Type**. The user will need to select the specific values for the **Location** and **Time Zone**.

The screenshot displays the 'SIP Entity Details' configuration page in the Avaya Aura System Manager 8.0. The left-hand navigation pane shows 'Routing' selected, with 'SIP Entities' highlighted. The main content area is titled 'SIP Entity Details' and includes a 'General' tab. The configuration fields are as follows:

- Name:** SBCE
- FQDN or IP Address:** 10.10.98.13
- Type:** SIP Trunk
- Notes:** (empty)
- Adaptation:** (dropdown menu)
- Location:** Belleville-GSSCP
- Time Zone:** America/Toronto
- SIP Timer B/F (in seconds):** 4
- Minimum TLS Version:** Use Global Setting
- Credential name:** (text input)
- Securable:** ☐
- Call Detail Recording:** egress
- Loop Detection Mode:** On
- Loop Count Threshold:** 5
- Loop Detection Interval (in msec):** 200
- SIP Link Monitoring:** Link Monitoring Enabled

Figure 45: 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 the 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 on the next page), 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

- **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
- **Connection Policy:** Select **trusted**. **Note:** If **trusted** is not selected, 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**.

The screenshot shows the Avaya Aura System Manager 8.0 interface. The sidebar on the left has 'Routing' and 'Entity Links' highlighted. The main area is titled 'Entity Links' and contains a table with one item. The table has the following columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, DNS Override, and Connection Policy. The values in the table are: Name: *SM_CM_TLS_5061, SIP Entity 1: *Q.bvwasm2, Protocol: TLS, Port: *5061, SIP Entity 2: *Q.CM8, Port: *5061, DNS Override: unchecked, and Connection Policy: trusted. There are 'Commit' and 'Cancel' buttons at the top right of the table area.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	DNS Override	Connection Policy
*SM_CM_TLS_5061	*Q.bvwasm2	TLS	*5061	*Q.CM8	*5061	<input type="checkbox"/>	trusted

Figure 46: Communication Manager Entity Link

The following screen illustrates the Entity Links to Avaya SBCE. The protocol and ports defined here must match the values used on the Avaya SBCE mentioned in **Section 7.2.4**, **7.2.6** and **7.4.3**.

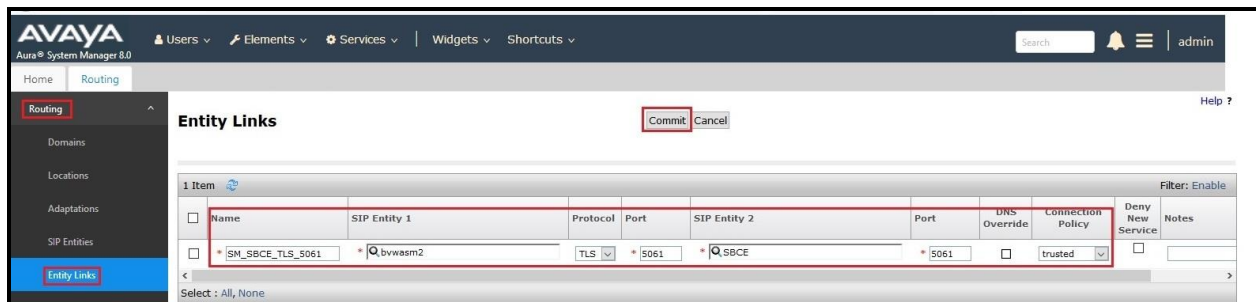


Figure 47: Avaya SBCE Entity Link

6.6. Configure Time Ranges

Time Ranges are configured for time-based-routing. In order to add a Time Range, 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.

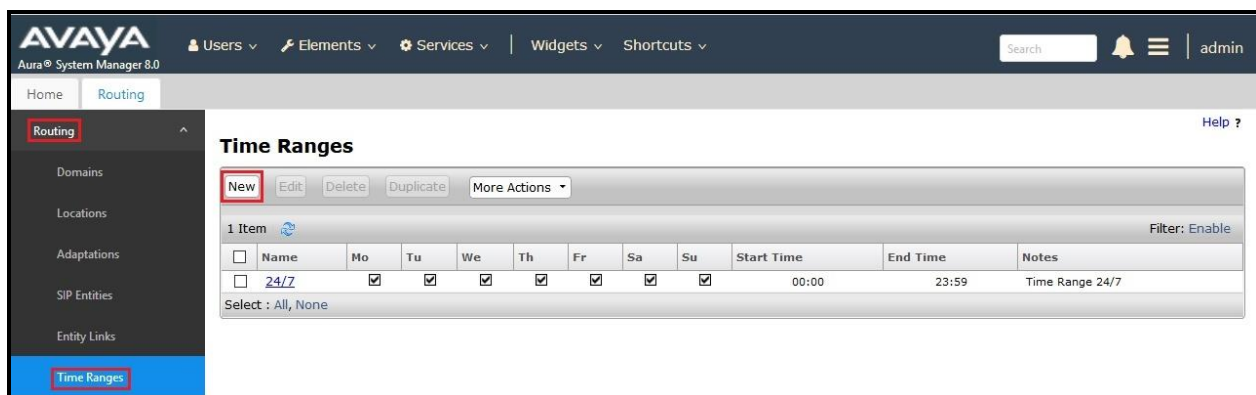


Figure 48: Time Ranges

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 on the next page), 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 **Cox Inbound Calls** associated with incoming PSTN calls from Cox Communications to Communication Manager. Observe the **SIP Entity as Destination** is the entity named **CM8**.

The screenshot displays the Avaya Aura System Manager 8.0 interface. The left sidebar shows the navigation menu with 'Routing Policies' highlighted. The main content area is titled 'Routing Policy Details' and includes a 'Commit' button. The 'General' section contains fields for 'Name' (Cox Inbound Calls), 'Disabled' (checkbox), 'Retries' (0), and 'Notes'. The 'SIP Entity as Destination' section features a 'Select' button and a table listing available SIP entities.

Name	FQDN or IP Address	Type	Notes
CM8	10.33.10.44	CM	

Figure 49: Routing to Communication Manager

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

The screenshot displays the Avaya Aura System Manager 8.0 interface. The left-hand navigation pane shows the 'Routing' menu with 'Routing Policies' selected. The main content area is titled 'Routing Policy Details' and shows the 'General' tab. The 'Name' field is 'Cox Outbound Calls'. The 'Disabled' checkbox is unchecked. The 'Retries' field is '0'. The 'Notes' field is empty. Below this, the 'SIP Entity as Destination' section shows a table with one entry: 'SBCE' with the FQDN or IP Address '10.10.98.13' and the Type 'SIP Trunk'. The 'Commit' and 'Cancel' buttons are visible at the top right of the form.

Figure 50: Routing to Cox Communications SIP Trunk

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 Cox Communications SIP Trunk 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 on the next page), 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 were similarly defined.

The first example shows that outbound 11-digit dialed numbers that begin with **1613** and have a destination **SIP Domain** of **bwvdev.com** uses **Routing Policy Name** as **Cox Outbound Calls** which is defined in **Section 6.7**.

The screenshot displays the Avaya Aura System Manager 8.0 interface. The left sidebar shows the 'Routing' menu with 'Dial Patterns' selected. The main area is titled 'Dial Pattern Details' and includes a 'Commit' button. The 'General' tab is active, showing the following fields:

- Pattern:** 1613
- Min:** 4
- Max:** 11
- Emergency Call:** ☐
- SIP Domain:** bwvdev.com
- Notes:** Cox Outbound Calls

Below the general fields is a section titled 'Originating Locations and Routing Policies' with an 'Add' button. A table lists one item:

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
-ALL-		Cox Outbound Calls	0	<input type="checkbox"/>	SBCE	

Figure 51: Dial Pattern_1613

Note that with the above Dial Pattern, Cox Communications did not restrict outbound calls to specific US/Canada area codes. In real deployments, appropriate restriction can be exercised 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 back to the PSTN.

The second example shows that inbound 10-digit numbers that start with **402** use **Routing Policy Name** as **Cox Inbound Calls** which is defined in **Section 6.7**. This Dial Pattern matches the DID numbers assigned to the enterprise by Cox Communications.

AVAYA
Aura® System Manager 8.0

Users ▾ Elements ▾ Services ▾ Widgets ▾ Shortcuts ▾ Search | admin

Home Routing

Dial Pattern Details Commit Cancel

General

* Pattern: 402
 * Min: 4
 * Max: 36

Emergency Call: ☐

SIP Domain: bvwddev.com ▾

Notes: Cox Inbound Call

Originating Locations and Routing Policies

Add Remove

1 Item

	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-		Cox Inbound Calls	0	<input type="checkbox"/>	CM8	

Select : All, None

Figure 52: Dial Pattern_402

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

Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Notes
0	1	36	<input type="checkbox"/>			bvwdev.com	Cox Outbound Calls
1404	4	36	<input type="checkbox"/>			bvwdev.com	Cox Outbound Calls
1613	4	11	<input type="checkbox"/>			bvwdev.com	Cox Outbound Calls
1647	4	36	<input type="checkbox"/>			bvwdev.com	Cox Outbound Calls
1800	4	36	<input type="checkbox"/>			bvwdev.com	Cox Outbound Calls
402	4	36	<input type="checkbox"/>			bvwdev.com	Cox Inbound Call
4026	4	36	<input type="checkbox"/>			bvwdev.com	Cox Outbound Calls
411	3	36	<input type="checkbox"/>			bvwdev.com	Cox Outbound Calls
65	4	4	<input type="checkbox"/>			bvwdev.com	Cox SIP Phones
790	4	4	<input type="checkbox"/>			bvwdev.com	Cox SIP Phones
81	4	4	<input type="checkbox"/>			bvwdev.com	Cox SIP Phones
83	4	4	<input type="checkbox"/>			bvwdev.com	Cox SIP Phones
911	3	36	<input type="checkbox"/>			bvwdev.com	Cox Outbound Calls

Figure 53: 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 the Cox managed CPE.

In this testing, according to the configuration reference **Figure 1**, the Avaya elements reside on the Private side and the Cox managed CPE 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, refer to the documentation listed in **Section 11** of these Application Notes.

7.1. Log in to 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** and click on **Log In** button.

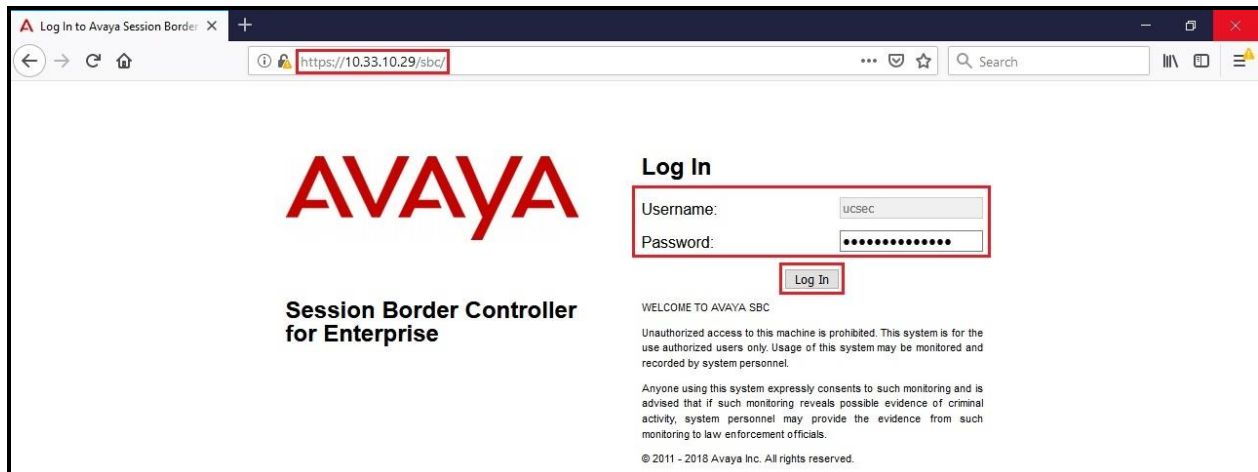


Figure 54: Avaya SBCE Login

The **Dashboard** main page will appear as shown below.

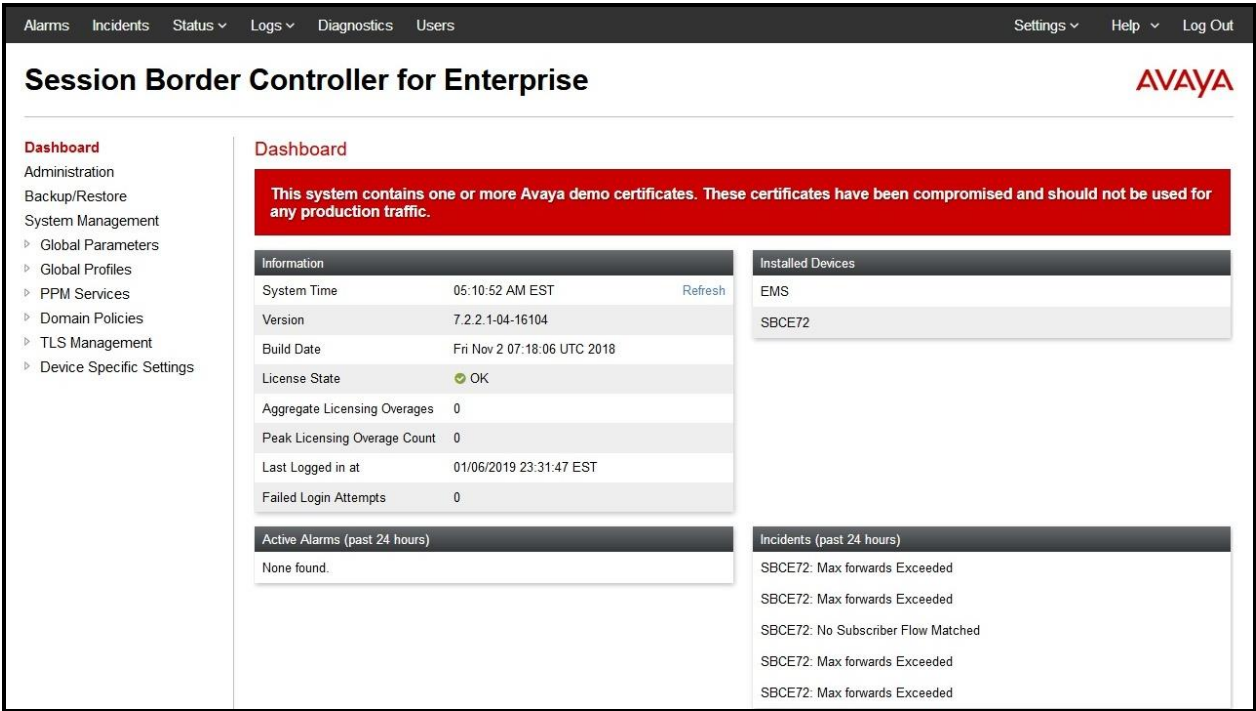


Figure 55: Avaya SBCE Dashboard

To view system information that has been configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the compliance testing, a single Device Name **SBCE72** was already added. To view the configuration of this device, click **View** as shown in the screenshot below.



Figure 56: Avaya SBCE System Management

The **System Information** screen shows **General Configuration**, **Device Configuration**, **Network Configuration**, **DNS Configuration** and **Management IP(s)** information provided during installation and corresponds to **Figure 1**.

System Information: SBCE72
X

General Configuration

Appliance Name	SBCE72
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

License Allocation

Standard Sessions	0
Requested: 0	
Advanced Sessions	0
Requested: 0	
Scopia Video Sessions	0
Requested: 0	
CES Sessions	0
Requested: 0	
Transcoding Sessions	0
Requested: 0	
Encryption	<input checked="" type="checkbox"/>

Network Configuration

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.10.98.13	10.10.98.13	255.255.255.192	10.10.98.1	A1
10.10.98.34	10.10.98.34	255.255.255.192	10.10.98.1	A1
10.10.98.111	10.10.98.111	255.255.255.224	10.10.98.97	B1
10.10.98.123	10.10.98.123	255.255.255.224	10.10.98.97	B1

DNS Configuration

Primary DNS	10.10.98.60
Secondary DNS	
DNS Location	DMZ
DNS Client IP	10.10.98.13

Management IP(s)

IP #1 (IPv4)	10.33.10.29
--------------	-------------

Figure 57: Avaya SBCE System Information

7.2. Global Profiles

When selected, Global Profiles allows for configuration of parameters across all Avaya SBCE 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, etc.

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

- Select **avaya-ru** in **Interworking Profiles**
- Click **Clone**
- Enter **Clone Name: SMVM** and click **Finish** (not shown)

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

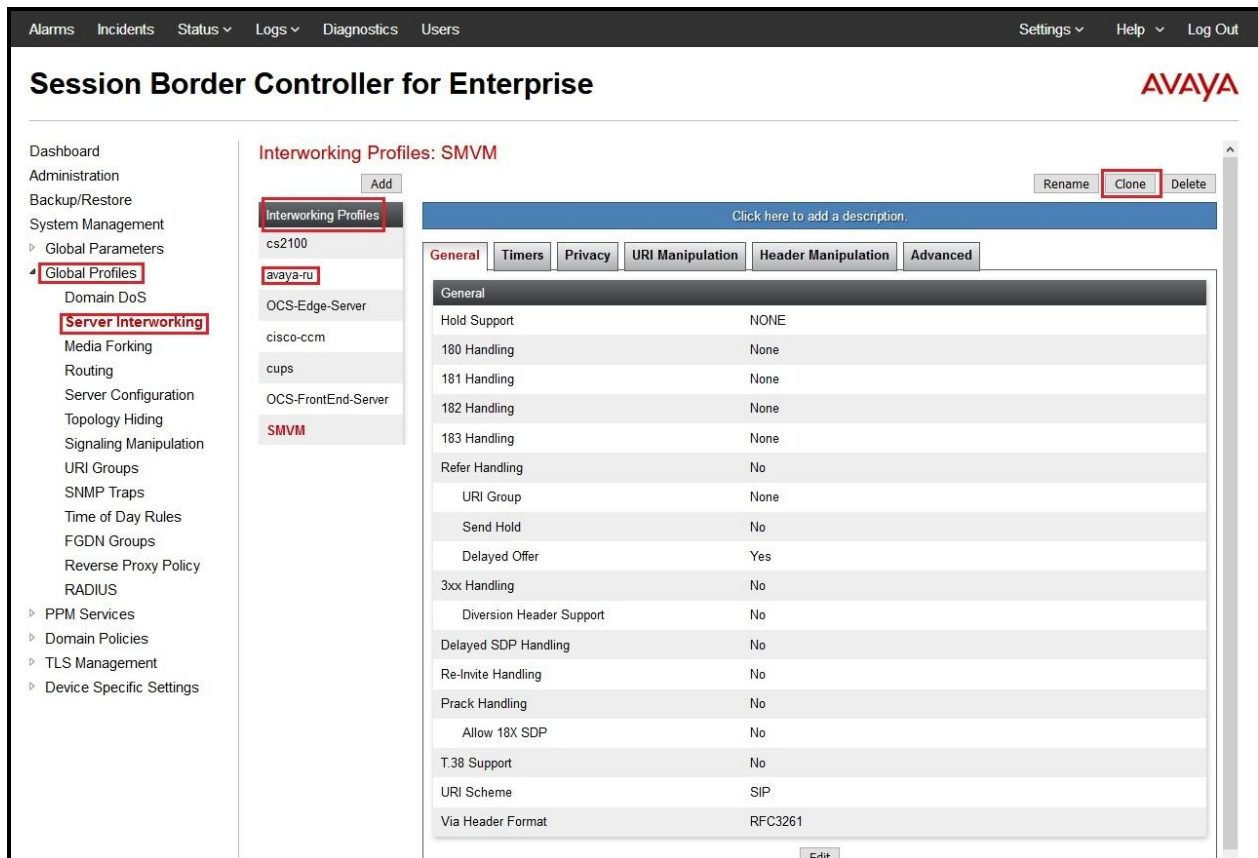


Figure 58: Server Interworking – Avaya site

7.2.2. Configure Server Interworking Profile – Cox Communications SIP Trunk Site

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

- Enter **Profile Name: SP4** (not shown)
- Click **Next** button to leave all options at default
- Click **Finish** (not shown)

The following screen shows that Cox Communications server interworking profile (named: **SP4**) 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: SP4" and includes an "Add" button. Below this, a list of interworking profiles is shown, with "SP4" highlighted. The "General" tab is selected, displaying a table of configuration parameters.

Parameter	Value
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None
Send Hold	No
Delayed Offer	Yes
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
Re-Invite Handling	No
Prack Handling	No
Allow 18X SDP	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261

Figure 59: Server Interworking – Cox Communications SIP Trunk site

7.2.3. Configure Signaling Manipulation

The SIP signaling header manipulation feature adds the ability to add, change and delete any of the headers and other information in a SIP message.

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

- Enter script **Title: SP4**. In the script editing window, enter the text exactly as shown in the below screenshot to perform the following:
 - Manipulate the SIP headers for outbound calls
 - Remove un-wanted headers
 - Modify user of SIP URI in PAI header on off-net call forward
 - Click **Save** (not shown)

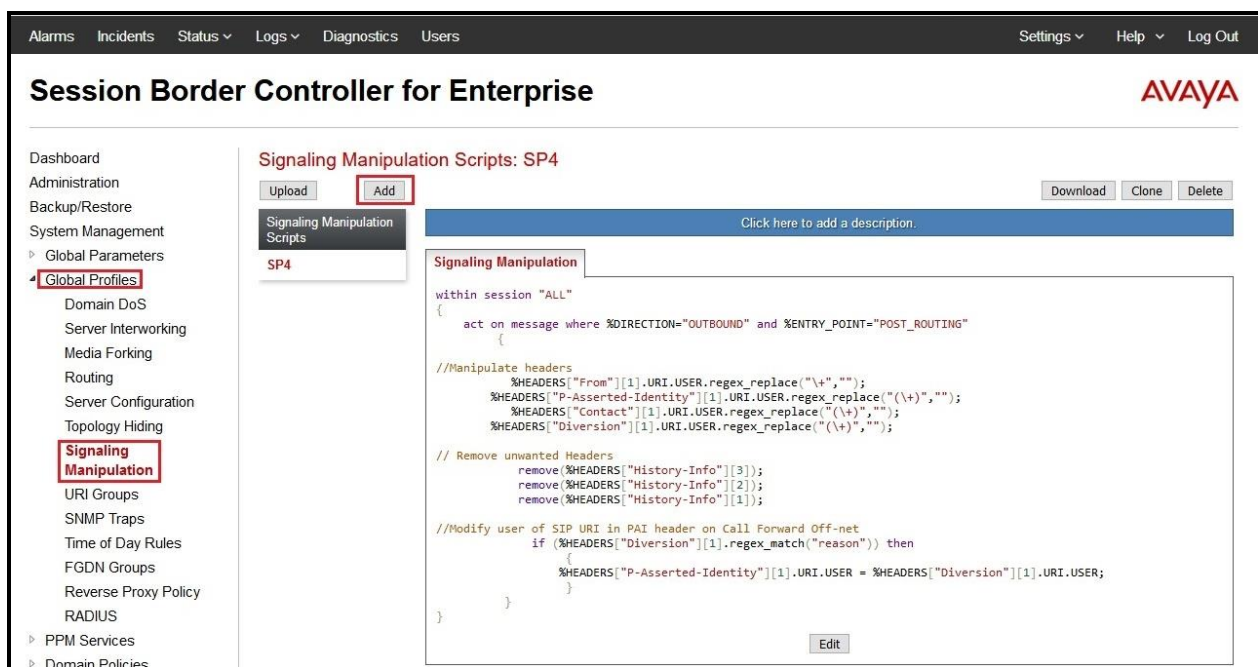


Figure 60: Signaling Manipulation

Note: See **Appendix B** in **Section 13** for the reference of this signaling manipulation (SigMa) script.

7.2.4. Configure Server – Avaya Site

The **Server Configuration** screen contains six tabs: **General**, **Authentication**, **Heartbeat**, **Registration**, **Ping** and **Advanced**. Together, these tabs allow one to configure and manage various SIP call server specific parameters such as 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**: **SMVM**

On **General** tab, enter the following:

- **Server Type**: Select **Call Server**
- **TLS Client Profile**: Select **AvayaSBCClient8**. Note: During the compliance test in the lab environment, demo certificates are used on Session Manager, and are not recommended for production use.
- **IP Address/FQDN**: **10.33.10.43** (Session Manager IP Address)
- **Port**: **5061**
- **Transport**: **TLS**
- Click **Finish** (not shown)

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with items like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (highlighted), Domain DoS, Server Interworking, Media Forking, Routing, Server Configuration (highlighted), and Topology Hiding. The main content area is titled 'Server Configuration: SMVM' and features an 'Add' button. Below this is a tabbed interface with 'General', 'Authentication', 'Heartbeat', 'Registration', 'Ping', and 'Advanced' tabs. The 'General' tab is active, showing the following configuration:

Server Type	Call Server	
TLS Client Profile	AvayaSBCClient8	
DNS Query Type	NONE/A	
IP Address / FQDN	Port	Transport
10.33.10.43	5061	TLS

Buttons for 'Rename', 'Clone', 'Delete', and 'Edit' are also visible.

Figure 61: Server Configuration – General - Avaya site

On the **Advanced** tab:

- **Enable Grooming** box is checked
- Select **SMVM** for **Interworking Profile** (see **Section 7.2.1**)
- Click **Finish** (not shown)

General	Authentication	Heartbeat	Registration	Ping	Advanced
Enable DoS Protection <input type="checkbox"/>					
Enable Grooming <input checked="" type="checkbox"/>					
Interworking Profile SMVM					
Signaling Manipulation Script None					
Securable <input type="checkbox"/>					
Enable FGDN <input type="checkbox"/>					
Tolerant <input type="checkbox"/>					
URI Group None					
<div>Edit</div>					

Figure 62: Server Configuration – Advanced - Avaya site

7.2.5. Configure Server – Cox Communications SIP Trunk

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

Enter **Profile Name: SP4**

On **General** tab, enter the following:

- **Server Type:** Select **Trunk Server**
- **IP Address/FQDN:** **10.10.98.110** (Cox managed CPE LAN port IP Address)
- **Port:** **5060**
- **Transport:** **UDP**
- Click **Finish** (not shown)

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left-hand navigation menu includes: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, Domain DoS, Server Interworking, Media Forking, Routing, Server Configuration (highlighted), and Topology Hiding. The main content area is titled "Server Configuration: SP4" and features an "Add" button. Below this, there are tabs for General, Authentication, Heartbeat, Registration, Ping, and Advanced. The General tab is selected, showing the following configuration details:

IP Address / FQDN	Port	Transport
10.10.98.110	5060	UDP

Other fields include "Server Type" set to "Trunk Server" and "DNS Query Type" set to "NONE/A". An "Edit" button is located at the bottom right of the configuration area.

Figure 63: Server Configuration – General – Cox Communication site

On **Heartbeat** tab, enter the following:

- Check **Enable Heartbeat**
- Select **Method: OPTIONS**
- Set **Frequency: 30 seconds**
- Input **From URI: ping@10.10.98.111** (Avaya SBCE public interface IP Address)
- Input **To URI: ping@10.10.98.110** (Cox managed CPE LAN port IP Address)

General	Authentication	Heartbeat	Registration	Ping	Advanced								
<div>Enable Heartbeat <input checked="" type="checkbox"/></div> <table><tr><td>Method</td><td>OPTIONS</td></tr><tr><td>Frequency</td><td>30 seconds</td></tr><tr><td>From URI</td><td>ping@10.10.98.111</td></tr><tr><td>To URI</td><td>ping@10.10.98.110</td></tr></table> <div>Edit</div>						Method	OPTIONS	Frequency	30 seconds	From URI	ping@10.10.98.111	To URI	ping@10.10.98.110
Method	OPTIONS												
Frequency	30 seconds												
From URI	ping@10.10.98.111												
To URI	ping@10.10.98.110												

Figure 64: Server Configuration – Heartbeat – Cox Communications site

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

- **Interworking Profile: SP4** (see **Section 7.2.2**)
- **Signaling Manipulation Script: SP4** (see **Section 7.2.3**)
- Click **Finish** (not shown)

General	Authentication	Heartbeat	Registration	Ping	Advanced
Enable DoS Protection <input type="checkbox"/>					
Enable Grooming <input type="checkbox"/>					
Interworking Profile SP4					
Signaling Manipulation Script SP4					
Securable <input type="checkbox"/>					
Enable FGDN <input type="checkbox"/>					
Tolerant <input type="checkbox"/>					
URI Group None					
<div>Edit</div>					

Figure 65: Server Configuration – Advanced – Cox Communications site

7.2.6. 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** and click **Add** as highlighted below.

Enter **Profile Name: SP4_To_SMVM** and click **Next** button (Not Shown)

- Select **Load Balancing: Priority**
- Check **Next Hop Priority**
- Click **Add** button to add a Next-Hop Address
- **Priority/Weight: 1**
- **Server Configuration: SMVM** (see Section 7.2.4)
- **Next Hop Address: 10.33.10.43:5061 (TLS)** (Session Manager IP Address)
- Click **Finish**

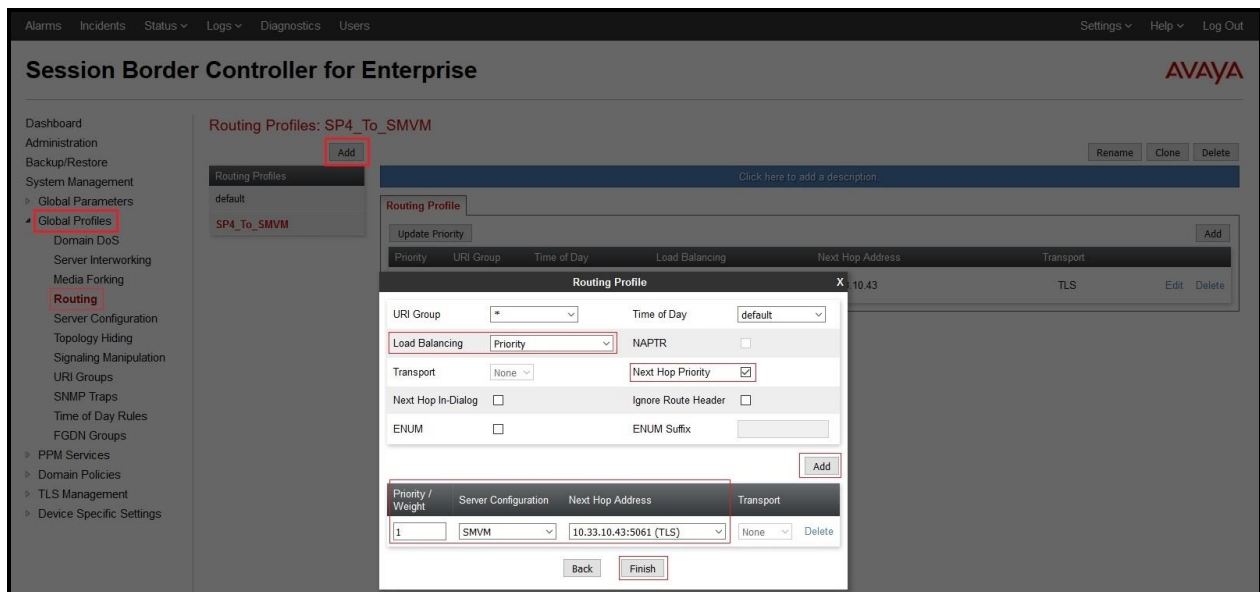


Figure 66: Routing to Session Manager

7.2.7. Configure Routing – Cox Communications SIP Trunk Site

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

From the menu on the left-hand side, select **Global Profiles → Routing** and click **Add** as highlighted below.

Enter **Profile Name: SMVM_To_SP4** and click **Next** button (not shown)

- **Load Balancing: Priority**
- **Check Next Hop Priority**
- **Click Add** button to add a Next-Hop Address
- **Priority/Weight: 1**
- **Server Configuration: SP4** (see Section 7.2.5)
- **Next Hop Address: 10.10.98.110:5060 (UDP)** (Cox managed CPE LAN port IP Address)
- **Click Finish**

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left-hand navigation menu has 'Global Profiles' expanded, and 'Routing' is selected. The main content area is titled 'Routing Profiles: SMVM_To_SP4'. An 'Add' button is highlighted in the top right of the main area. Below this, a 'Routing Profile' modal window is open. The modal has a 'Load Balancing' section with 'Priority' selected. The 'Transport' section has 'None' selected. The 'Next Hop Priority' checkbox is checked. The 'Next Hop Address' field is set to '10.10.98.110:5060 (UDP)'. The 'Priority / Weight' field is set to '1'. The 'Server Configuration' dropdown is set to 'SP4'. The 'Add' button at the bottom right of the modal is highlighted. The 'Finish' button at the bottom of the modal is also highlighted.

Figure 67: Routing to Cox Communications SIP Trunk

7.2.8. Configure Topology Hiding

The **Topology Hiding** screen allows an 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 **default** in **Topology Hiding Profiles**
- Click **Clone**
- Enter **Clone Name: SP4_To_SMVM** and click **Finish** (not shown)
- Select **SP4_To_SMVM** in **Topology Hiding Profiles** and click **Edit** button to enter as below:
- For the Header **Request-Line**,
 - In the **Criteria** column select **IP/Domain**
 - In the **Replace Action** column select: **Overwrite**
 - In the **Overwrite Value** column: **bwdev.com**
Note: bwdev.com is SIP Domain of enterprise
- For the Header **To**,
 - In the **Criteria** column select **IP/Domain**
 - In the **Replace Action** column select: **Overwrite**
 - In the **Overwrite Value** column: **bwdev.com**
- For the Header **From**,
 - In the **Criteria** column select **IP/Domain**
 - In the **Replace Action** column select: **Overwrite**
 - In the **Overwrite Value** column: **bwdev.com**

Click **Finish** (not shown)

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left-hand navigation menu is expanded, showing the path: Dashboard > Administration > System Management > Global Parameters > Global Profiles > Topology Hiding. The main content area is titled "Topology Hiding Profiles: SP4_To_SMVM". It shows a list of profiles: "default" and "SP4_To_SMVM". The "SP4_To_SMVM" profile is selected. Below the list, there is a table titled "Topology Hiding" with the following columns: Header, Criteria, Replace Action, and Overwrite Value. The table contains the following rows:

Header	Criteria	Replace Action	Overwrite Value
Referred-By	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	bwdev.com
Refer-To	IP/Domain	Auto	---
To	IP/Domain	Overwrite	bwdev.com
From	IP/Domain	Overwrite	bwdev.com
Via	IP/Domain	Auto	---

At the bottom of the table, there is an "Edit" button. Above the table, there are buttons for "Rename", "Clone", and "Delete".

Figure 68: Topology Hiding To Session Manager

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

- Select **default** in **Topology Hiding Profiles**
- Click **Clone**
- Enter **Clone Name: SMVM_To_SP4** and click **Finish** (not shown)

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left-hand navigation menu is expanded, showing 'Global Profiles' and 'Topology Hiding' selected. The main content area displays 'Topology Hiding Profiles: SMVM_To_SP4'. A list of profiles is shown, including 'default', 'cisco_th_profile', 'Topo_CAR276', 'Topo_SM63', 'SP4_To_SMVM', and 'SMVM_To_SP4'. The 'SMVM_To_SP4' profile is selected. The 'Topology Hiding' table is displayed, showing headers, criteria, replace actions, and overwrite values.

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

Figure 69: Topology Hiding To Cox 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 an administrator can create a custom domain policy.

7.3.1. Create Media Rules

Media Rules allow one to define media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the Avaya SBCE security product. For the compliance test, the predefined **default-low-med-enc** media rule (shown below) was used to clone and edit.

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

- Select the **default-low-med-enc** rule, click **Clone**. Enter **Clone Name: SMVM_SP4**
Click **Finish** (not shown)
- Select **SMVM_SP4** under **Media Rules** to **Edit**

The **Encryption** tab indicates that **RTP** and **SRTP_AES_CM_128_HMAC_SHA1_80** encryption was used as **Preferred Formats** for Audio Encryption.

Alarms
Incidents
Status
Logs
Diagnostics
Users

Settings
Help
Log Out

Session Border Controller for Enterprise

Dashboard
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
PPM Services
Domain Policies
Application Rules
Border Rules
Media Rules
Security Rules
Signaling Rules
Charging Rules
End Point Policy
Groups
Session Policies
TLS Management
Device Specific Settings

Media Rules: SMVM_SP4

Add
Filter By Device...
Rename
Clone
Delete

Click here to add a description.

Encryption
Codec Prioritization
Advanced
QoS

Audio Encryption

Preferred Formats	RTP SRTP_AES_CM_128_HMAC_SHA1_80
Encrypted RTCP	<input checked="" type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime	Any
Interworking	<input checked="" type="checkbox"/>

Video Encryption

Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80 SRTP_AES_CM_128_HMAC_SHA1_80 NONE NONE
Encrypted RTCP	<input type="checkbox"/>
MKI	<input type="checkbox"/>
Lifetime	Any
Interworking	<input checked="" type="checkbox"/>

Miscellaneous

Capability Negotiation	<input checked="" type="checkbox"/>
------------------------	-------------------------------------

Edit

Figure 70: Media Rule

7.3.2. Create Endpoint Policy Groups

The End Point Policy Group feature allows one 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, Signaling, Security, Charging and RTCP Mon Gen, 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 Avaya SBCE 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: SMVM_SP4**
 - **Application Rule: default**
 - **Border Rule: default**
 - **Media Rule: SMVM_SP4** (See in Section 7.3.1)
 - **Security Rule: default-low**
 - **Signaling Rule: default**
- Select **Finish** (not shown)

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with the following items: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies (highlighted), Application Rules, Border Rules, Media Rules, Security Rules, Signaling Rules, Charging Rules, End Point Policy Groups (highlighted), Session Policies, TLS Management, and Device Specific Settings. The main content area is titled 'Policy Groups: SMVM_SP4' and includes an 'Add' button, a 'Filter By Device...' dropdown, and buttons for 'Rename', 'Clone', and 'Delete'. Below this is a table of policy rules. The table has columns: Order, Application, Border, Media, Security, Signaling, Charging, and RTCP Mon Gen. The first row shows the following values: 1, default, default, SMVM_SP4, default-low, default, None, and Off. The 'Media' column is highlighted in red. A 'Summary' button is located to the right of the table. The Avaya logo is visible in the top right corner.

Order	Application	Border	Media	Security	Signaling	Charging	RTCP Mon Gen
1	default	default	SMVM_SP4	default-low	default	None	Off

Figure 71: Endpoint Policy

7.4. Device Specific Settings

The Device Specific Settings feature for SIP allows one 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, one 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**.

- Select **Networks** tab and click the **Add** button to add a network for the inside interface as follows:
 - **Name:** Network_A1
 - **Default Gateway:** 10.10.98.1
 - **Subnet Mask:** 255.255.255.192
 - **Interface:** A1 (This is the Avaya SBCE inside interface)
 - Click the **Add** button to add the **IP Address** for inside interface: 10.10.98.13
 - Click the **Finish** button to save the changes

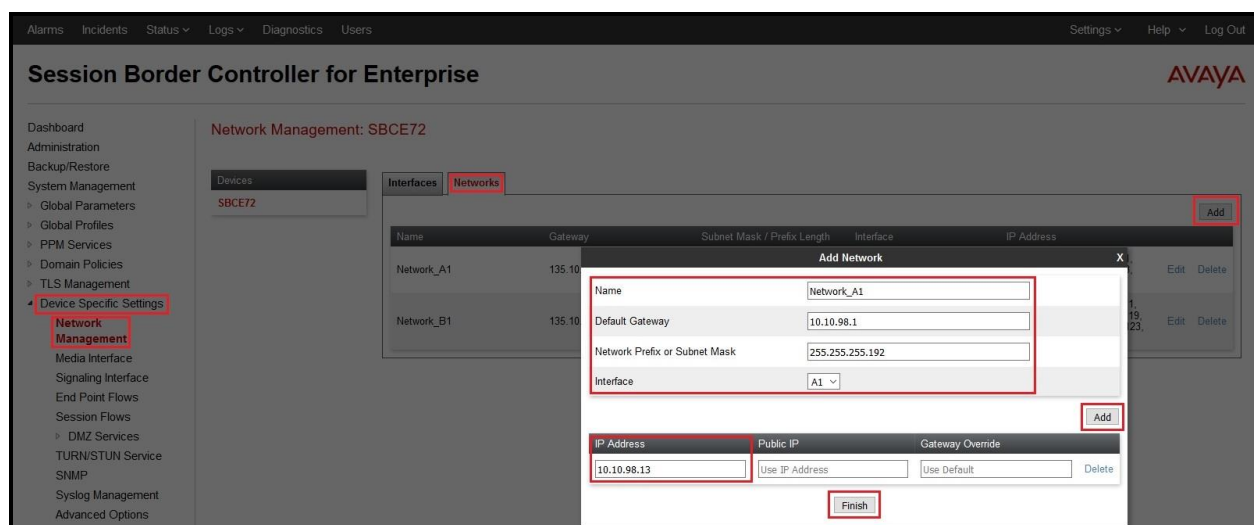


Figure 72: Network Management – Inside Interface

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

- Select **Networks** tab and click **Add** button to add a network for the outside interface as follows:
 - **Name: Network_B1**
 - **Default Gateway: 10.10.98.97**
 - **Subnet Mask: 255.255.255.224**
 - **Interface: B1** (This is the Avaya SBCE outside interface)
 - Click the **Add** button to add the **IP Address** for outside interface: **10.10.98.111**
 - Click the **Finish** button to save the changes

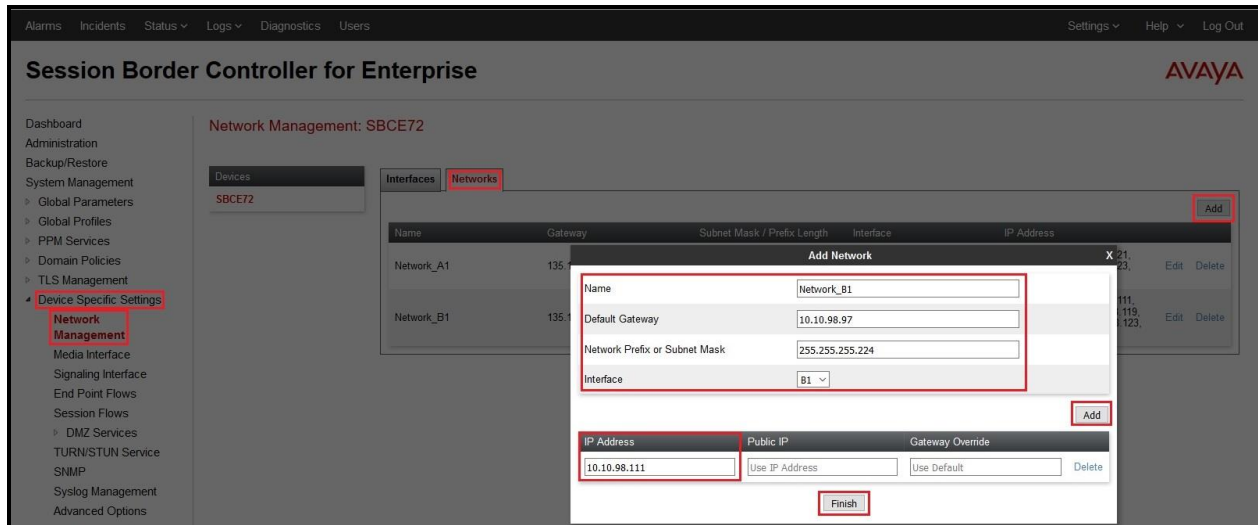


Figure 73: Network Management – Outside Interface

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

- Select the **Interfaces** tab
- Click on the **Status** of the physical interfaces being used and change them to **Enabled** state

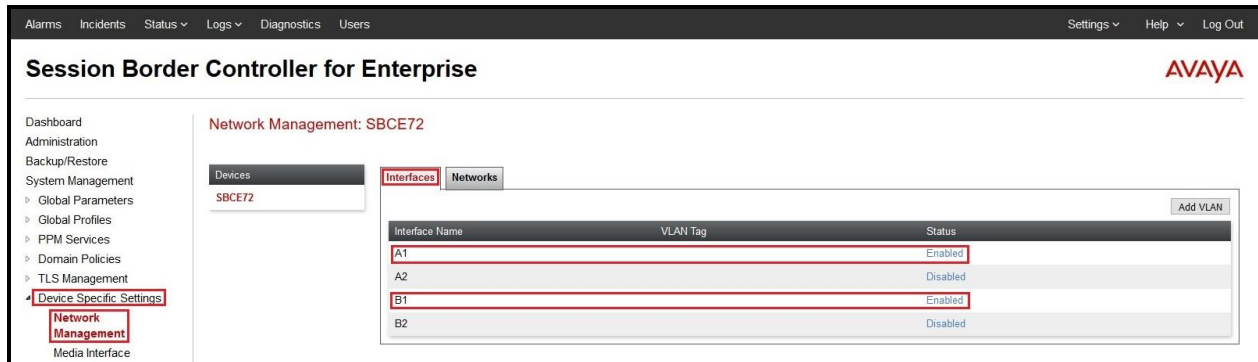


Figure 74: Network Management – Interface Status

7.4.2. Create Media Interfaces

Media Interfaces define the IP Addresses and port ranges in which the Avaya SBCE will accept media streams on each interface. The default media port range on the Avaya SBCE can be used for inside port.

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

- Select the **Add** button and enter the following:
 - **Name:** **InsideMedia1**
 - **IP Address:** Select **Network_A1 (A1,VLAN0)** and **10.10.98.13** (Internal IP Address toward Session Manager)
 - **Port Range:** **35000 – 40000**
 - Click **Finish** (not shown)
- Select the **Add** button and enter the following:
 - **Name:** **OutsideMedia1**
 - **IP Address:** Select **Network_B1 (B1,VLAN0)** and **10.10.98.111** (External IP Address toward Cox managed CPE)
 - **Port Range:** **35000 – 40000**
 - Click **Finish** (not shown)



Figure 75: 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 the **Add** button and enter the following:
 - **Name: OutsideUDP**
 - **IP Address:** Select **Network_B1 (B1,VLAN0)** and **10.10.98.111** (External IP Address toward Cox managed CPE)
 - **UDP Port: 5060**
 - Click **Finish** (not shown)

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

- Select the **Add** button and enter the following:
 - **Name: InsideTLS**
 - **IP Address:** Select **Network_A1 (A1,VLAN0)** and **10.10.98.13** (Internal IP Address toward Session Manager)
 - **TLS Port: 5061**
 - **TLS Profile: AvayaSBCServer8**. Note: During the compliance test in the lab environment, demo certificates are used on Session Manager, and are not recommended for production use.
 - Click **Finish** (not shown)

Note: For the external interface, the Avaya SBCE was configured to listen for UDP on port 5060 the same as Cox Communications used. For the internal interface, the Avaya SBCE was configured to listen for TLS on port 5061.

The screenshot shows the Avaya Session Border Controller for Enterprise (SBCE) web interface. The left sidebar contains a navigation menu with options like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, PPM Services, Domain Policies, TLS Management, Device Specific Settings (highlighted), Network Management, Media Interface, Signaling Interface (highlighted), and End Point Flows. The main content area is titled 'Signaling Interface: SBCE72' and shows a table of signaling interfaces. The table has columns for Name, Signaling IP Network, TCP Port, UDP Port, TLS Port, and TLS Profile. Two interfaces are listed: OutsideUDP and InsideTLS. The OutsideUDP interface has a Signaling IP of 10.10.98.111 (Network_B1 (B1, VLAN 0)), TCP Port ---, UDP Port 5060, TLS Port ---, and TLS Profile None. The InsideTLS interface has a Signaling IP of 10.10.98.13 (Network_A1 (A1, VLAN 0)), TCP Port ---, UDP Port ---, TLS Port 5061, and TLS Profile AvayaSBCServer8. Both interfaces have Edit and Delete buttons. A warning message at the top states: 'Modifying or deleting an existing signaling interface will require an application restart before taking effect. Application restarts can be issued from System Management.' An Add button is also present.

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
OutsideUDP	10.10.98.111 Network_B1 (B1, VLAN 0)	---	5060	---	None	Edit Delete
InsideTLS	10.10.98.13 Network_A1 (A1, VLAN 0)	---	---	5061	AvayaSBCServer8	Edit Delete

Figure 76: Signaling Interface

7.4.4. Configuration Server Flows

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

7.4.4.1 Create End Point Flows – SMVM Flow

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: SMVM Flow**
 - **Server Configuration: SMVM** (see Section 7.2.4)
 - **URI Group: ***
 - **Transport: ***
 - **Remote Subnet: ***
 - **Received Interface: OutsideUDP** (see Section 7.4.3)
 - **Signaling Interface: InsideTLS** (see Section 7.4.3)
 - **Media Interface: InsideMedia1** (see Section 7.4.2)
 - **Secondary Media Interface: None**
 - **End Point Policy Group: SMVM_SP4** (see Section 7.3.2)
 - **Routing Profile: SMVM_To_SP4** (see Section 7.2.7)
 - **Topology Hiding Profile: SP4_To_SMVM** (see Section 7.2.8)
 - Leave other parameters as default
 - Click **Finish**

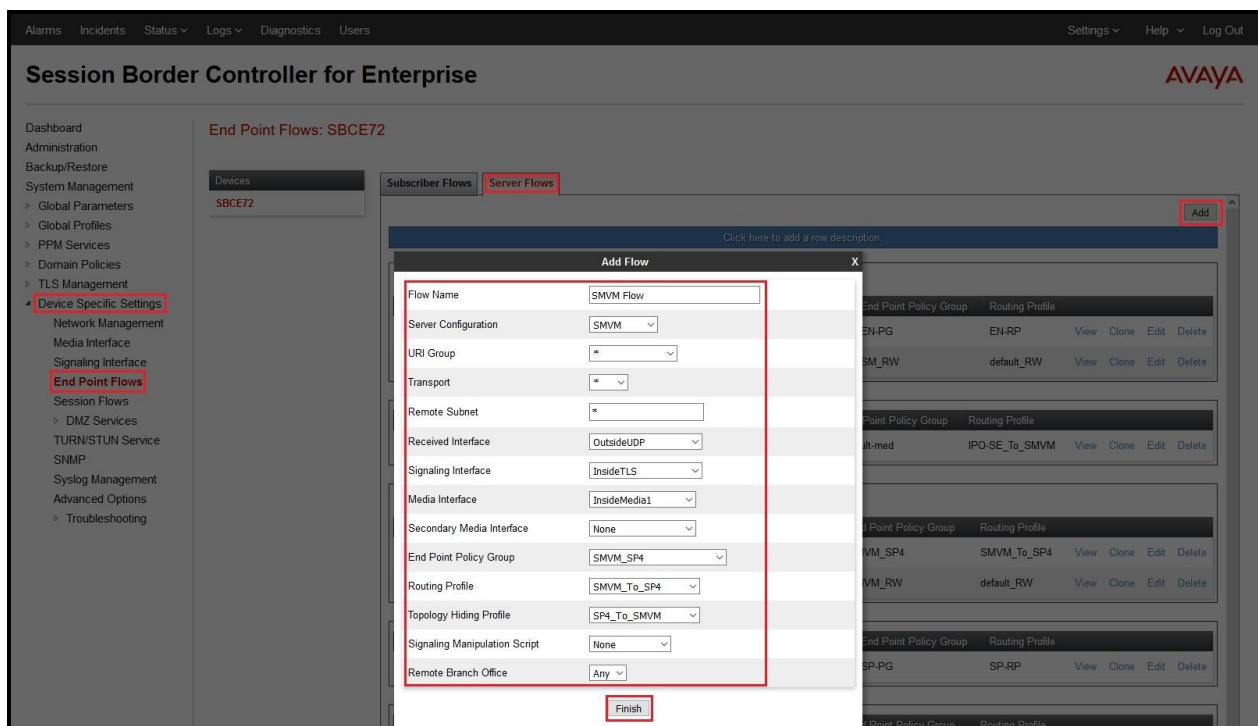


Figure 77: End Point Flow 1

7.4.4.2 Create End Point Flows – Cox Communications SIP Trunk Flow

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: SP4 Flow**
 - **Server Configuration: SP4** (see Section 7.2.5)
 - **URI Group: ***
 - **Transport: ***
 - **Remote Subnet: ***
 - **Received Interface: InsideTLS** (see Section 7.4.3)
 - **Signaling Interface: OutsideUDP** (see Section 7.4.3)
 - **Media Interface: OutsideMedia1** (see Section 7.4.2)
 - **Secondary Media Interface: None**
 - **End Point Policy Group: SMVM_SP4** (see Section 7.3.2)
 - **Routing Profile: SP4_To_SMVM** (see Section 7.2.6)
 - **Topology Hiding Profile: SMVM_To_SP4** (see Section 7.2.8)
 - Leave other parameters as default
 - Click **Finish**

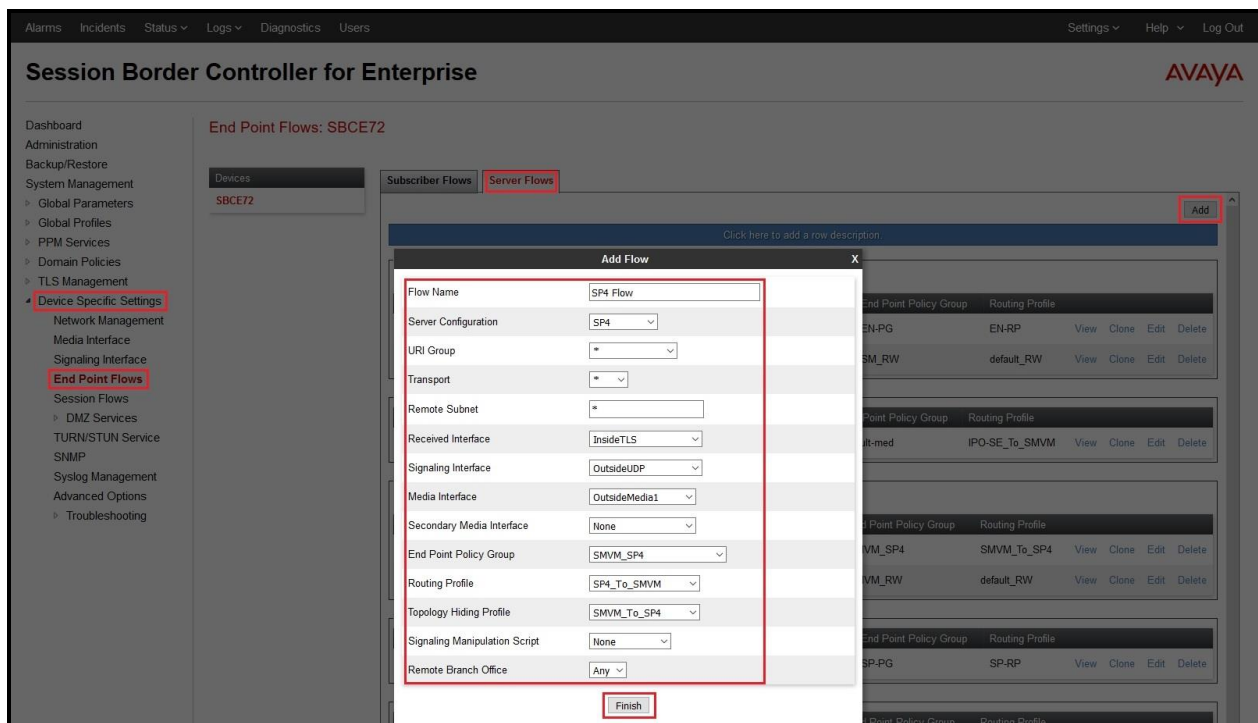


Figure 78: End Point Flow 2

8. Cox Communications SIP Trunk Configuration

Cox Communications is responsible for the configuration of Cox Communications SIP Trunk Service. Cox Communications will provide the Cox managed CPE to the customer when the customer orders the Cox Communications SIP trunk service. Cox Communications will be responsible for managing the Cox managed CPE. Customer must provide the IP Address used to reach the Avaya SBCE public interface at the enterprise. Cox Communications will provide the customer necessary information to configure the SIP connection between Avaya SBCE and Cox managed CPE. Cox Communications also provides the Cox Communications SIP Specification document for reference. This information is used to complete configurations for Communication Manager, Session Manager, and the Avaya SBCE discussed in the previous sections.

The configuration between Cox Communications SIP Trunk and the enterprise is a static IP Address configuration.

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. Communication Manager: Enter the following commands using the 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** – Session Manager command line tool for traffic analysis. Log into the Session Manager management interface to run this command.
3. Avaya SBCE: Debug logging can be started in two different ways:
 - **GUI of the SBC: Device Specific Settings → Troubleshooting → Debugging.**
 - SIP only: enable LOG_SUB_SIPCC subsystem under SSYNDI process.
 - CALL PROCESSING: enable all subsystems under SSYNDI process.
 - PPM: enable all subsystems under CONFIG_PROXY process.The log files are stored at: /usr/local/ipcs/log/ss/logfiles/elog/SSYNDI.
 - **Command Line Interface:** Login with root user and enter the command: **#traceSBC**. The tool updates the database directly based on which trace mode is selected.

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 Cox Communications. This solution successfully passed compliance testing via the Avaya DevConnect Program.

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*, Release 8.0.1, Issue 3, December 2018
- [2] *Administering Avaya Aura® System Manager*, Release 8.0.1, Issue 6, January 2019

Avaya Aura® Communication Manager

- [3] *Administering Avaya Aura® Communication Manager*, Release 8.0.1, Issue 3, December 2018

Avaya Phones

- [4] *Administering 9608/9808G/9611G/9621G/9641G/9641GS IP Deskphones H.323*, Issue 2, March 2018
- [5] *Installing and Administering 9608/9808G/9611G/9621G/9641G/9641GS IP Deskphones SIP*, Issue 3, March 2018
- [6] *Avaya one-X® Communicator Release 6.2 SP12 Patch10 Release Notes, Issue 1.0, January 2018*
- [7] *Equinox™ Client (Windows) Release 3.3.4 (SP4), Release Notes, Issue 1.0, June 2018*

Avaya Session Border Controller for Enterprise

- [8] *Administering Avaya Session Border Controller for Enterprise*, Release 7.2.2, Issue 11, November 2018

IETF (Internet Engineering Task Force) SIP Standard Specifications

- [9] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>

Product documentation for Cox Communications SIP Trunking may be found at:

<http://www.cox.com>

12. Appendix A – Remote Worker Configuration

This section describes the process for connecting remote Avaya SIP endpoints on the public Internet, access through the Avaya SBCE to Session Manager on the private enterprise. It builds on the Avaya SBCE configuration described in previous sections of this document.

In the reference configuration, an existing Avaya SBCE is provisioned to access the Cox Communications SIP Trunk Services (see **Section 2.1** of this document). The Avaya SBCE also supports Remote Worker configurations, allowing remote SIP endpoints (connected via the public Internet) to access the private enterprise.

Supported endpoints are Avaya 96x1 SIP Deskphones, Avaya one-X[®] Communicator SIP softphone and Avaya Equinox[™] for Windows SIP softphone.

Note: In the compliance testing, only Avaya one-X[®] Communicator SIP softphone was used to test as the remote worker.

Standard and Advanced Session Licenses are required for the Avaya SBCE to support Remote Workers. Contact an authorized Avaya representative for assistance if additional licensing is required. The settings presented here illustrate a sample configuration and are not intended to be prescriptive.

12.1. Network Management on Avaya SBCE

The following screen shows the **Network Management** of the Avaya SBCE. The Avaya SBCE is configured with two “outside” IP Addresses assigned to physical interface B1, and two “inside” IP Addresses assigned to physical interface A1.

Note: A SIP Entity in Session Manager was not configured for the Avaya SBCE’s internal IP Address used for Remote Worker. This keeps the Remote Worker interface untrusted in Session Manager, thereby allowing Session Manager to properly challenge user registration requests.

These are the IP Addresses used in the reference configuration:

- **10.10.98.13** is the Avaya SBCE “inside” IP Address previously provisioned for SIP Trunking with Cox managed CPE (see **Section 7.4.1**)
- **10.10.98.34** is the new Avaya SBCE “inside” IP Address for Remote Worker access to Session Manager
- **10.10.98.111** is the Avaya SBCE “outside” IP Address previously provisioned for SIP Trunking with Cox managed CPE (see **Section 7.4.1**)
- **10.10.98.123** is the new Avaya SBCE “outside” IP Address for Remote Worker access to Session Border Controller

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

- Enter the above **IP Addresses** and **Gateway Addresses** for both the Inside and the Outside interfaces
- Select the physical interface used in the **Interface** column accordingly

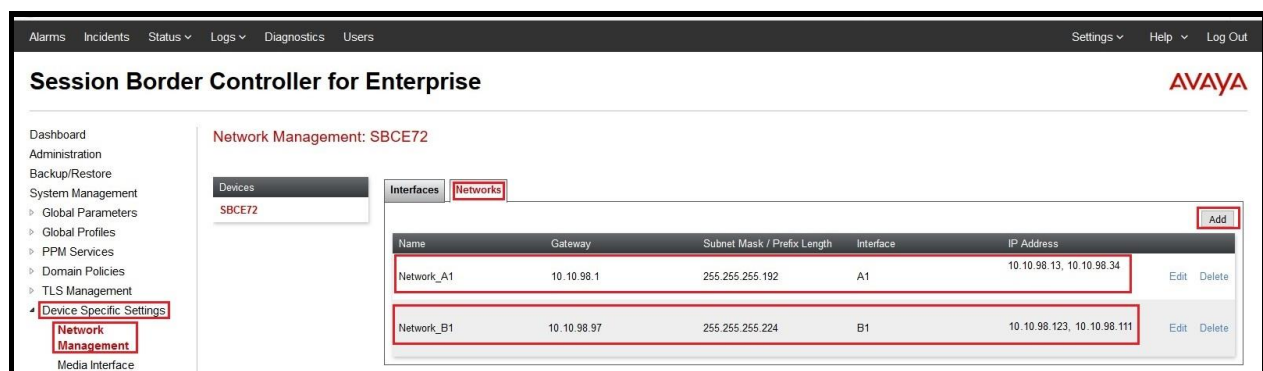


Figure 79: Network Management

On the **Interfaces** tab, verify that Interfaces **A1** and **B1** are both set to **Enabled** as previously configured for the Cox Communications SIP Trunk access in **Section 7.4.1**.



Figure 80: Network Interface Status

12.2. Media Interface on Avaya SBCE

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

- Select the **Add** button and enter the following:
 - **Name:** **InsideMedRW**
 - **IP Address:** Select **Network_A1 (A1, VLAN0)** and **10.10.98.34** (Internal IP Address toward Session Manager)
 - **Port Range:** **35000 – 40000**
 - Click **Finish** (not shown)
- Select the **Add** button and enter the following:
 - **Name:** **OutsideMedRW**
 - **IP Address:** Select **Network_B1 (B1, VLAN0)** and **10.10.98.123** (External IP Address toward Remote Worker phones)
 - **Port Range:** **35000 – 40000**
 - Click **Finish** (not shown)

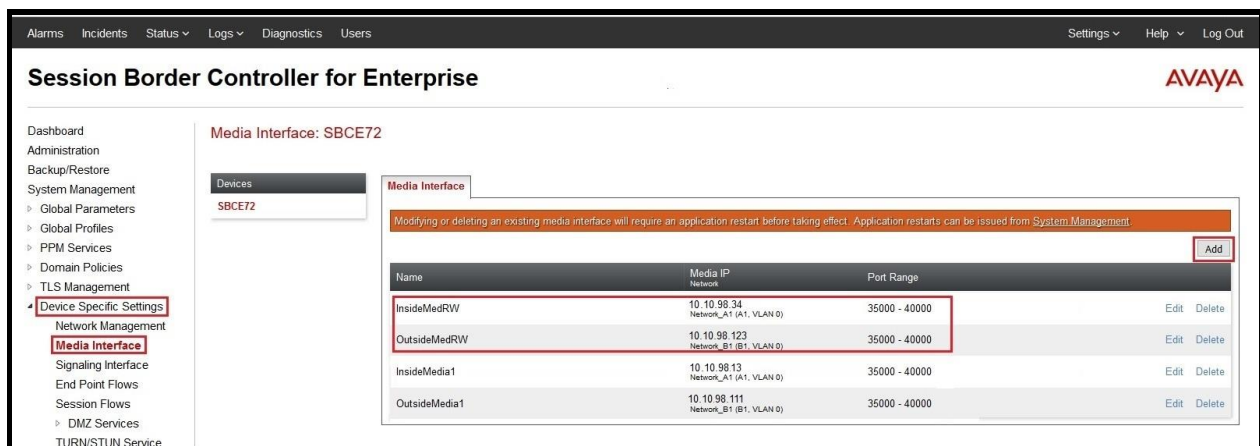


Figure 81: Media Interface

Note: Media Interface **OutsideMedRW** is used in the Remote Worker Subscriber Flow (**Section 12.8.1**), and Media Interface **InsideMedRW** is used in the Remote Worker Server Flow (**Section 12.8.2.1**).

12.3. Signaling Interface on Avaya SBCE

The following screen shows the Signaling Interface settings. Signaling interfaces were created for the inside and outside IP interfaces used for Remote Worker SIP traffic.

Select the **Add** button to create Signaling Interface **InsideSIGRW** using the parameters:

- **IP Address:** Select **Network_A1 (A1, VLAN0)** and **10.10.98.34** (Internal IP Address toward Session Manager)
- **TLS Port: 5061**
- **TLS Profile:** **AvayaSBCServer8**. Note: During the compliance test in the lab environment, demo certificates are used on Session Manager, and are not recommended for production use
- Click on **Finish** (not shown)

Select the **Add** button to create Signaling Interface **OutsideSIGRW** using the parameters:

- **IP Address:** Select **Network_B1 (B1, VLAN0)** and **10.10.98.123** (External IP Address toward Remote Worker phones)
- **TLS Port: 5061**
- **TLS Profile:** **AvayaSBCServer8**. Note: During the compliance test in the lab environment, demo certificates are used on Session Manager, and are not recommended for production use
- Click on **Finish** (not shown)

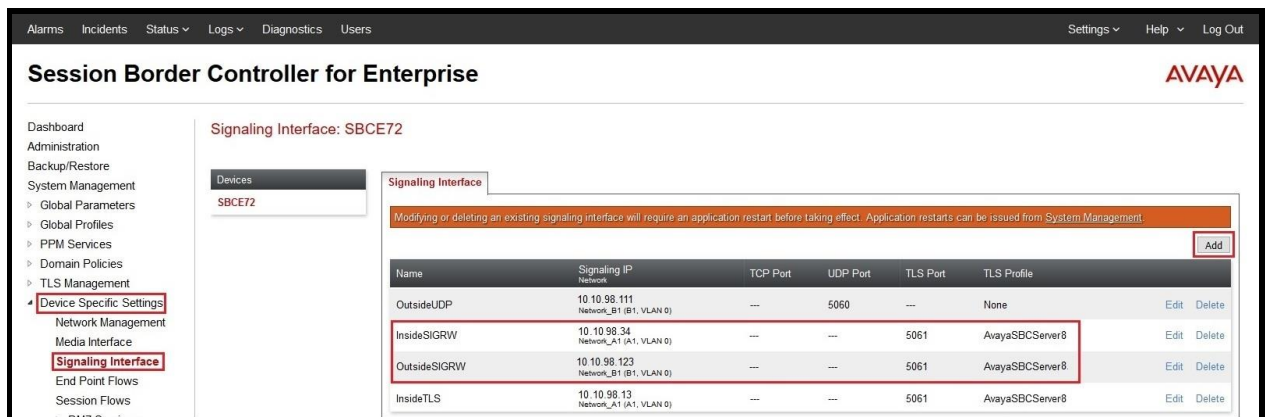


Figure 82: Signaling Interface

Note: Signaling Interface **OutsideSIGRW** is used in the Subscriber Flows (Section 12.8.1), and in the Remote Worker Server Flow (Section 12.8.2.1). Signaling Interface **InsideSIGRW** is used in the Remote Worker Server Flow (Section 12.8.2.1).

12.4. Routing Profile on Avaya SBCE

The Routing Profile **To_SMVM_RW** is created for routing the SIP traffic from Remote Worker to Session Manager via Avaya SBCE.

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

Enter **Profile Name: To_SMVM_RW** (not shown)

- **Load Balancing: Priority**
- **Check Next Hop Priority**
- Click **Add** button to add a Next-Hop Address
- **Priority/Weight: 1**
- **Server Configuration: SMVM**
- **Next Hop Address: 10.33.10.43:5061 (TLS)** (IP Address of Session Manager)
- Click **Finish**

The Routing Profile **To_SMVM_RW** is used in the Subscriber Flows (**Section 12.8.1**).

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left-hand navigation menu is expanded, showing the path: **Global Profiles → Routing → Add**. The main content area is titled "Routing Profiles: To_SMVM_RW" and includes an "Add" button. Below this, a "Routing Profile" configuration window is open, showing the following settings:

URI Group	Time of Day	Load Balancing	Next Hop Address	Transport
*	default	Priority	10.33.10.43:5061 (TLS)	None

The "Load Balancing" section is set to "Priority" with a weight of "1". The "Next Hop Address" is "10.33.10.43:5061 (TLS)" and the "Transport" is "None". The "Next Hop Priority" checkbox is checked. The "ENUM" and "Ignore Route Header" checkboxes are unchecked. The "Add" button is visible at the bottom right of the configuration window.

Figure 83: Remote Worker Routing to Session Manager

The Routing Profile **default_RW** is created for routing SIP traffic from Session Manager to Remote Worker via Avaya SBCE.

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

- Check **Load Balancing: DNS/SRV**
- **NAPTR** box is checked
- Click **Finish**

The Routing Profile **default_RW** is used in the Remote Worker Server Flow in **Section 12.8.2.1**.

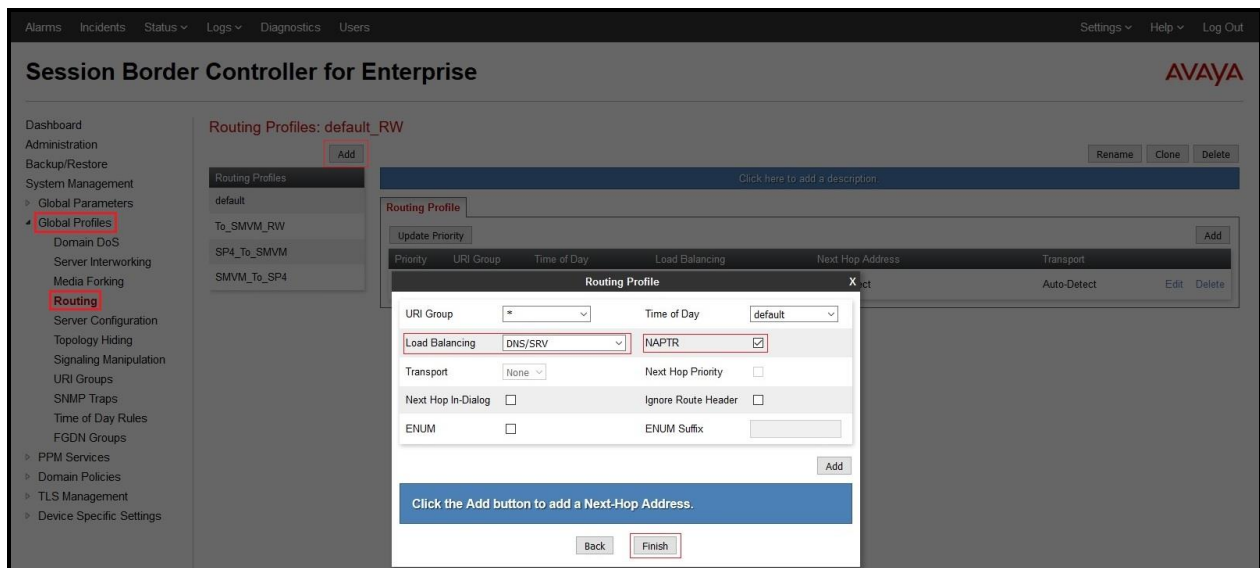


Figure 84: Remote Worker Default Routing

12.5. User Agent on Avaya SBCE

User Agents are created for each type of endpoints tested. In this compliance testing, Avaya one-X Communicator is used as the User Agent.

From the menu on the left-hand side, select **Global Parameters** → **User Agents**

Click **Add** button to add the user agent:

- Enter **Name: one-X Communicator**
- Enter **Regular Expression: Avaya one-X Communicator.***
- Click on **Finish** (not shown)



Figure 85: User Agents for Remote Worker

The following abridged output of Session Manager trace shows the details of an INVITE from an Avaya one-X Communicator. The User-Agent shown in this trace will match User Agent **one-X Communicator** shown above with a **Regular Expression** of “**Avaya one-X Communicator.***”. In this expression, “**.***” will match anything listed after the user agent name.

```
INVITE sip: 61613XXX7497@bvwddev.com SIP/2.0
From: sip:6581@bvwddev.com;tag=-59f03c7f529fb7c152aa3fd4_F0950710.10.98.79
To: sip: 61613XXX7497@bvwddev.com
CSeq: 24 INVITE
Call-ID: 18_a7e80-49279ea452aa365c_I@10.10.98.79
Contact: <sip:6581@10.10.98.79:5061;transport=tls;subid_ipcs=3784557512>;+avaya-cm-line=1
Allow: INVITE, CANCEL, BYE, ACK, SUBSCRIBE, NOTIFY, MESSAGE, INFO, PUBLISH, REFER, UPDATE, PRA
CK
Supported: eventlist, 100rel, replaces, vnd.avaya.ipo
User-Agent: Avaya one-X Communicator/6.2.12.23 (Engine GA-2.2.0.175; Windows NT 6.2, 32-bit)
Max-Forwards: 69
Via: SIP/2.0/TLS 10.10.98.79:62151;branch=z9hG4bK18_a7e80-312c149e52aa3fe8_I09507
Accept-Language: en
Content-Type: application/sdp
Content-Length: 440
```

Figure 86: Output of trace for User Agent

Note: The User Agent is defined in its associated **Subscriber Flows** in **Section 12.8.1**.

12.6. Application Rules on Avaya SBCE

The following section describes Application Rule **RW_AR**, used in this Remote Worker setting. In a typical customer installation, set the **Maximum Concurrent Sessions** for the **Voice** application to a value slightly larger than the licensed sessions.

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

- Select **default** from **Application Rules** and click **Clone** button:
- Enter **Clone Name** (e.g., **RW_AR**) and click **Finish** (not shown)
- Click on **RW_AR** from **Application Rules**, then click **Edit** button:
- In the **Audio** field:
 - Check **In** and **Out**
 - Enter an appropriate value in the **Maximum Concurrent Sessions** field (e.g., **2000**), and the same value in the **Maximum Session Per Endpoint** field
 - Leave the **CDR Support** field at **None** and the **RTCP Keep-Alive** field unchecked (**No**)
 - Click on **Finish** (not shown)

Alarms
Incidents
Status
Logs
Diagnostics
Users

Settings
Help
Log Out

Session Border Controller for Enterprise

Dashboard
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
PPM Services
Domain Policies
Application Rules
Border Rules
Media Rules
Security Rules
Signaling Rules
End Point Policy Groups
Session Policies

Application Rules: RW_AR

Add
Filter By Device...
Rename
Clone
Delete

Click here to add a description

Application Rule

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	2000	2000
Video	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	100	10

Miscellaneous

CDR Support	Off
RTCP Keep-Alive	No

Edit

Figure 87: Remote Worker Application Rule

Note: The rule **RW_AR** is assigned to the End Point Policy Groups in **Section 12.7**.

12.7. End Point Policy Groups on Avaya SBCE

A new End Point Policy Groups is defined for Remote Worker: **SMVM_RW**.

To create the new **SMVM_RW** group, click on **Add**. Enter the following:

- Enter a name (e.g., **SMVM_RW**), and click on **Next** (not shown)
- The **Policy Group** window will open. Enter the following:
 - **Application Rule** = **RW_AR** (see Section 12.6)
 - **Border Rule** = **default**
 - **Media Rule** = **SMVM_SP4** (see Section 7.3.1)
 - **Security Rule** = **default-low**
 - **Signaling Rule** = **default**
- Click on **Finish** (not shown)

The End Point Policy Group **SMVM_RW** is used in the Subscriber Flow **one-X Communicator** in Section 12.8.1 and Remote Worker Server Flow in Section 12.8.2.1.

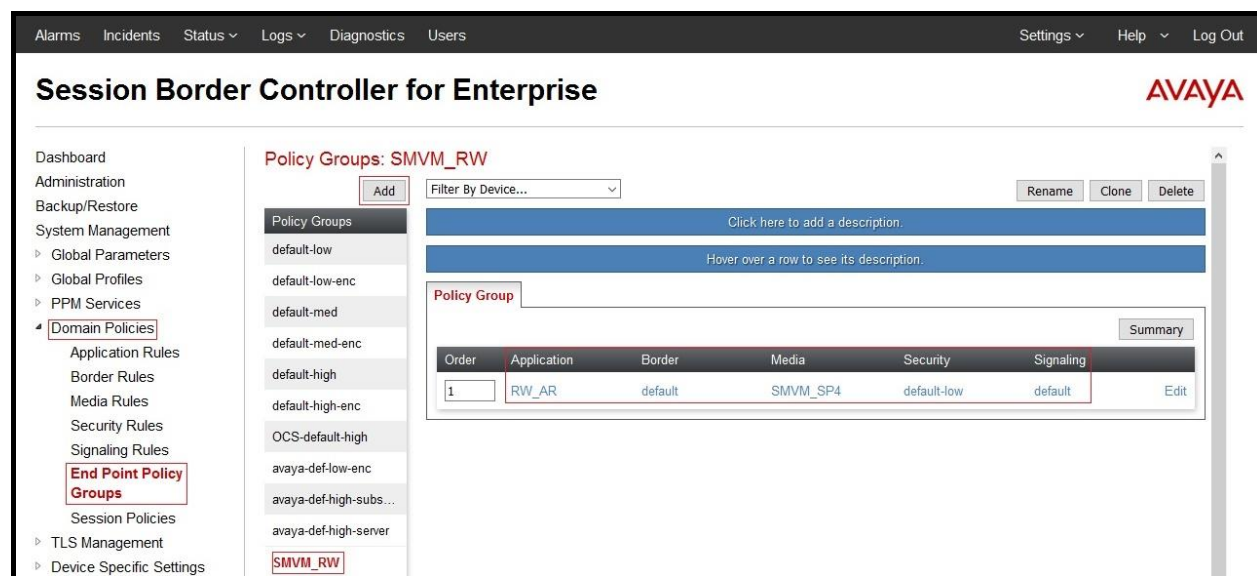


Figure 88: Remote Worker End Point Policy

12.8. End Point Flows on Avaya SBCE

12.8.1. Subscriber Flow

The **Subscriber Flow** is defined for Remote Workers associated with the **User Agent one-X Communicator** that was created in Section 12.5. The below subscriber flow is configured for Remote Worker to access Session Manager via Avaya SBCE.

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

On the **Subscriber Flows** tab, click on the **Add** button and enter the following:

- Enter a **Flow Name** (e.g., **one-X Communicator**)

- **URI Group** = * (default)
- **User Agent** = **one-X Communicator** (see **Section 12.5**)
- **Source Subnet** = * (default)
- **Via Host** = * (default)
- **Contact Host** = * (default)
- **Signaling Interface** = **OutsideSIGRW** (see **Section 12.3**)

Click on **Next** (not shown) and the Profile window will open (not shown). Enter the following:

- **Source** = **Subscriber**
- **Methods Allowed Before REGISTER** = Leave as default
- **Media Interface** = **OutsideMedRW** (see **Section 12.2**)
- **Received Interface** = **None**.
- **End Point Policy Group** = **SMVM_RW** (see **Section 12.7**)
- **Routing Profile** = **To_SMVM_RW** (see **Section 12.4**)
- **TLS Client Profile** = **None**
- **Signaling Manipulation Script** = **None**
- **Presence Server Address** = Leave as blank

Click on **Finish** (not shown).

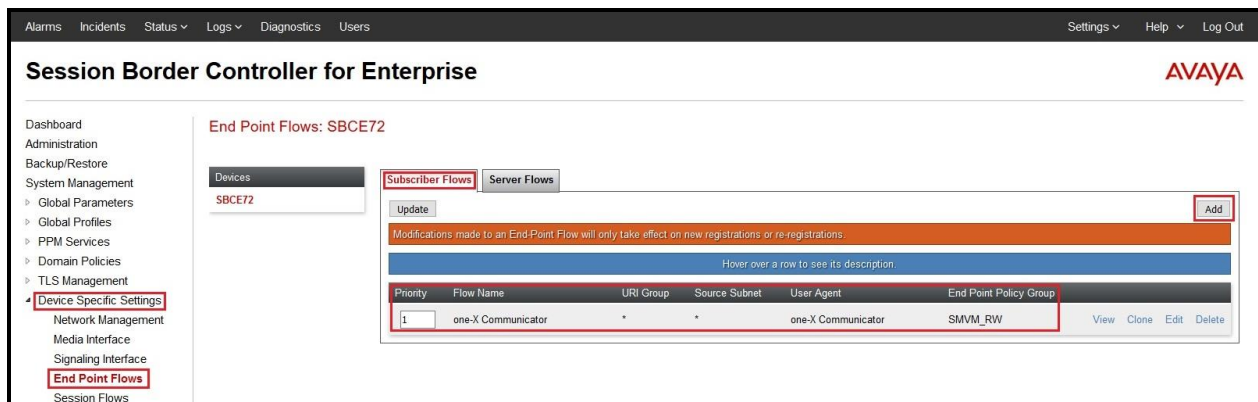


Figure 89: Remote Worker Subscriber Flows – 1

View Flow: one-X Communicator

X

Criteria

Flow Name	one-X Communicator
URI Group	*
User Agent	one-X Communicator
Source Subnet	*
Via Host	*
Contact Host	*
Signaling Interface	OutsideSIGRW

Optional Settings

TLS Client Profile	None
Signaling Manipulation Script	None

Profile

Source	Subscriber
Methods Allowed Before REGISTER	
User Agent	one-X Communicator
Media Interface	OutsideMedRW
Secondary Media Interface	None
End Point Policy Group	SMVM_RW
Routing Profile	To_SMVM_RW
Presence Server Address	---

Figure 90: Remote Worker Subscriber Flows – 2

12.8.2. Server Flow on Avaya SBCE

The new Remote Worker Server Flow (**SMVM_RemoteWorker**) is configured for the SIP traffic flow from Session Manager to Remote Worker via Avaya SBCE. Two existing Trunking Server Flows (SMVM Flow in **Section 7.4.4.1** and SP4 Flow in **Section 7.4.4.2**) are also used for Remote Worker.

12.8.2.1 Remote Worker Server Flow

From the menu on the left-hand side, select **Device Specific Settings → Endpoint Flows**. Select the **Server Flows** tab and click the **Add** button (not shown) to enter the following:

- **Name** = **SMVM_RemoteWorker**
- **Server Configuration** = **SMVM** (see **Section 7.2.4**)
- **URI Group** = * (default)
- **Transport** = * (default)
- **Remote Subnet** = * (default)
- **Received Interface** = **OutsideSIGRW** (see **Section 12.3**)
- **Signaling Interface** = **InsideSIGRW** (see **Section 12.3**)
- **Media Interface** = **InsideMedRW** (see **Section 12.2**)
- **Secondary Media Interface** = **None**
- **End Point Policy Group** = **SMVM_RW** (see **Section 12.7**)
- **Routing Profile** = **default_RW** (see **Section 12.4**)
- **Topology Hiding Profile** = **None** (default)
- **Signaling Manipulation Script** = **None** (default)
- **Remote Branch Office** = **Any** (default)

Click **Finish** (not shown).

View Flow: SMVM_RemoteWorker

X

Criteria	
Flow Name	SMVM_RemoteWorker
Server Configuration	SMVM
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	OutsideSIGRW

Profile	
Signaling Interface	InsideSIGRW
Media Interface	InsideMedRW
Secondary Media Interface	None
End Point Policy Group	SMVM_RW
Routing Profile	default_RW
Topology Hiding Profile	None
Signaling Manipulation Script	None
Remote Branch Office	Any

Figure 91: Remote Worker Server Flow

12.8.2.2 Trunking Server Flow

Two existing Trunking Server Flows (SMVM Flow in **Section 7.4.4.1** and SP4 Flow in **Section 7.4.4.2**) are also used for Remote Worker.

View Flow: SP4 Flow

X

Criteria	
Flow Name	SP4 Flow
Server Configuration	SP4
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	InsideTLS

Profile	
Signaling Interface	OutsideUDP
Media Interface	OutsideMedia1
Secondary Media Interface	None
End Point Policy Group	SMVM_SP4
Routing Profile	SP4_To_SMVM
Topology Hiding Profile	SMVM_To_SP4
Signaling Manipulation Script	None
Remote Branch Office	Any

Figure 92: Trunking Server Flow – SP4 Flow

View Flow: SMVM Flow

X

Criteria	
Flow Name	SMVM Flow
Server Configuration	SMVM
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	OutsideUDP

Profile	
Signaling Interface	InsideTLS
Media Interface	InsideMedia1
Secondary Media Interface	None
End Point Policy Group	SMVM_SP4
Routing Profile	SMVM_To_SP4
Topology Hiding Profile	SP4_To_SMVM
Signaling Manipulation Script	None
Remote Branch Office	Any

Figure 93: Trunking Server Flow – SMVM Flow

12.9. System Manager

12.9.1. Modify Session Manager Firewall: Elements → Session Manager → Network Configuration → SIP Firewall

Select **Rule Sets** as **Rule Set for SMVM**, click **Edit** button

The screenshot displays the Avaya Aura System Manager 8.0 interface. The top navigation bar includes 'Users', 'Elements', 'Services', 'Widgets', and 'Shortcuts'. The left sidebar shows a tree view with 'Session Manager' and 'SIP Firewall' highlighted. The main content area is titled 'SIP Firewall Configuration' and contains a table of 'Rule Sets'. The table has columns for 'Rule Sets', 'Type', 'Assigned Count', 'Avaya Provided', and 'Description'. The 'Rule Set for SMVM' row is selected, and the 'Edit' button is highlighted.

Rule Sets	Type	Assigned Count	Avaya Provided	Description
<input type="checkbox"/> BSM 6.3.2.0	BSM	0	Yes	Avaya provided Rule Set for BSM
<input type="checkbox"/> BSM 6.3.8.0	BSM	0	Default	Avaya provided Rule Set for BSM
<input type="checkbox"/> BSM 6.3.4.0	BSM	0	Yes	Avaya provided Rule Set for BSM
<input type="checkbox"/> SM 6.3.2.0	SM	0	Yes	Avaya provided Rule Set for SM
<input type="checkbox"/> SM 6.3.8.0	SM	0	Default	Avaya provided Rule Set for SM
<input type="checkbox"/> SM 6.3.4.0	SM	0	Yes	Avaya provided Rule Set for SM
<input checked="" type="checkbox"/> Rule Set for SMVM	SM	1	No	

Figure 94: Session Manager – SIP Firewall Configuration - Rules

On **Whitelist** tab, select **New**

- In the **Key** field, select **Remote IP Address**
- In the **Value** field, enter internal Avaya SBCE IP Address used for Remote Worker (**10.10.98.34** as defined in **Section 12.1**)
- In the **Mask** field, enter the appropriate mask (e.g., **255.255.255.255**)
- **Enabled** box is checked
- Select **Commit**

The screenshot shows the Avaya Aura System Manager 8.0 interface. The left sidebar contains navigation links: Session Manager, Dashboard, Session Manager Admin..., Global Settings, Communication Profile..., Network Configuration (highlighted), Failover Groups, Local Host Name R..., and Remote Access. The main content area is titled 'Rule Set' and shows the configuration for a SIP Firewall Rule Set. The 'Whitelist' tab is selected. The 'Name' field is 'Rule Set for SMVM', the 'Description' field is empty, and the 'SM Type' is 'SM'. The 'Enabled' checkbox is checked. A table lists the rules, with one rule highlighted: 'Remote IP Address' with value '10.10.98.34' and mask '255.255.255.255'. The 'Commit' button is highlighted in the top right corner.

Key	Value	Mask
Remote IP Address	10.10.98.34	255.255.255.255

Figure 95: Session Manager – SIP Firewall Configuration - Whitelist

12.9.2. Disable PPM Limiting: Elements → Session Manager → Session Manager Administration

Select the **Session Manager Instance** named **bwasm2**, and select **Edit**

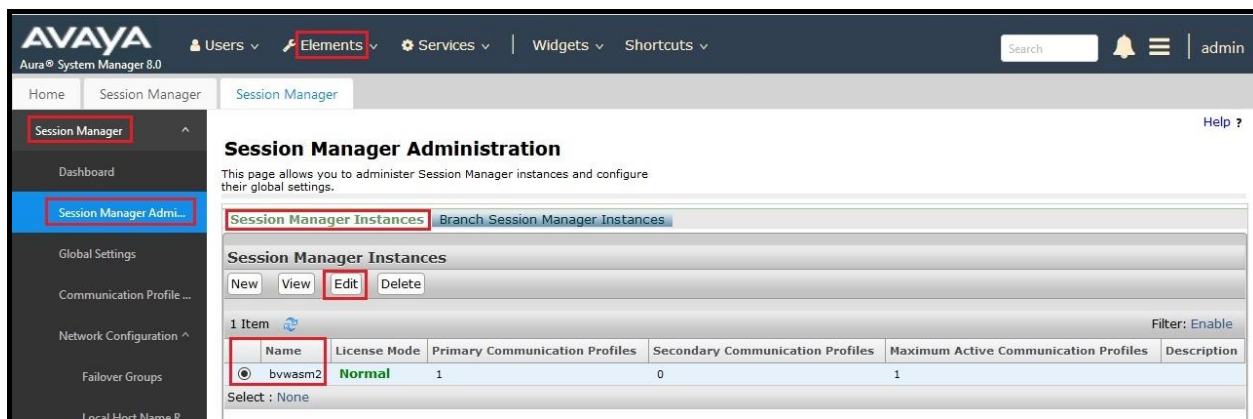


Figure 96: Session Manager – Edit Instance

The **Session Manager View** screen is displayed. Scroll down to the **Personal Profile Manager (PPM) – Connection Settings** section.

- Uncheck the **Limited PPM Client Connection** and **PPM Packet Rate Limiting** options
- Select **Commit** (not shown)

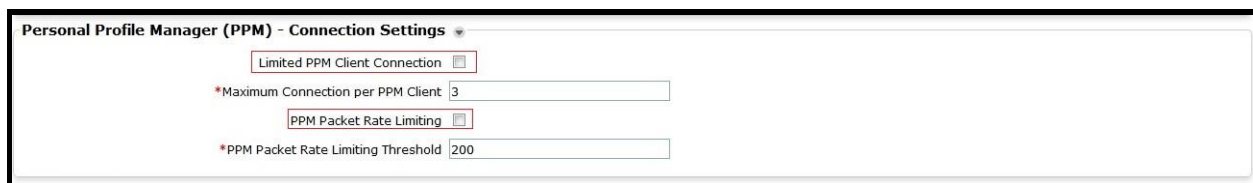


Figure 97: Session Manager – Disable PPM limit

12.10. Remote Worker Client Configuration

The following screen illustrates Avaya one-X® Communicator administration settings for the Remote Worker, used in the reference configuration (note that some screen formats may differ from endpoint to endpoint).

SIP Global Settings Screen

Launch to **Avaya one-X® Communicator** settings and click on **Telephony** under **Accounts**.

Select **Using** as **SIP**

Enter **Extension** and **Password**

Click **Add** button to add a server into **Server List**

Enter **Proxy Server** as **10.10.98.123** (see **Section 12.1**). Set **Transport Type**: **TLS** and **Port**: **5061**. Click **OK** to submit the changes.

Set the **Domain** to **bvwdev.com**.

The other fields are default. Click **OK** to submit the settings.

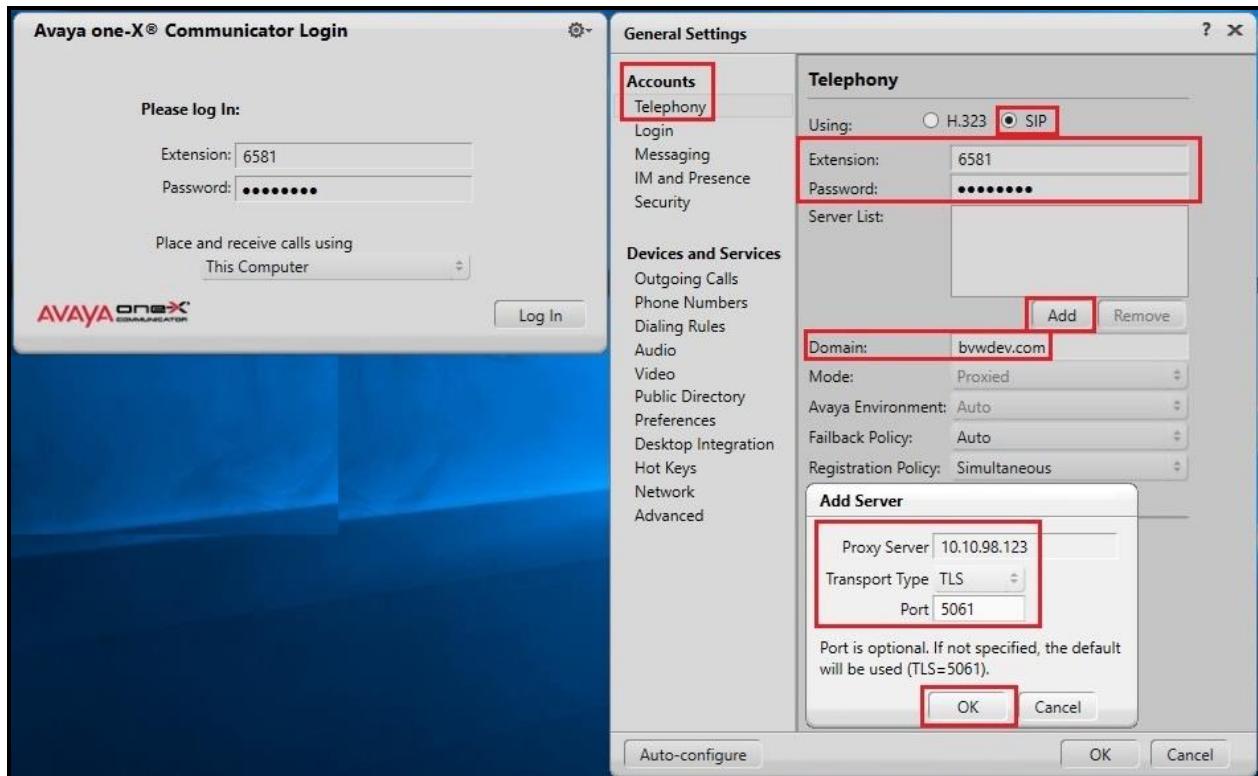


Figure 98: Avaya one-X Communicator - Settings

13. Appendix B - SigMa Script

The following is the Signaling Manipulation script used in the configuration of the SBCE, **Section 7.2.3.**

```
within session "ALL"
{
    act on message where %DIRECTION="OUTBOUND" and
    %ENTRY_POINT="POST_ROUTING"
    {

//Manipulate headers
        %HEADERS["From"][1].URI.USER.regex_replace("\+", "");
        %HEADERS["P-Asserted-Identity"][1].URI.USER.regex_replace("(\\+)", "");
        %HEADERS["Contact"][1].URI.USER.regex_replace("(\\+)", "");
        %HEADERS["Diversion"][1].URI.USER.regex_replace("(\\+)", "");

// Remove unwanted Headers
        remove(%HEADERS["History-Info"][3]);
        remove(%HEADERS["History-Info"][2]);
        remove(%HEADERS["History-Info"][1]);

//Modify user of SIP URI in PAI header on Call Forward Off-net
        if (%HEADERS["Diversion"][1].regex_match("reason")) then
        {
            %HEADERS["P-Asserted-Identity"][1].URI.USER =
%HEADERS["Diversion"][1].URI.USER;
        }
    }
}
```

14. Appendix C - Cox managed CPE Configuration

The Cox managed CPE is configured to manage all SIP signaling and provides voice quality management. All data traffic also traverses the Cox managed CPE. It is part of the Cox Communications SIP trunk service and Cox Communications will provide it to the customer when the customer orders the Cox Communications SIP trunk service. Cox Communications manages it and the end-customer does not manage.

Note: Cox managed CPE is part of Cox Communications SIP trunk service offering and it is Cox Communications's responsibility for all the aspect of the Cox managed CPE (i.e. support, detail configuration, maintenance and etc...). The Cox managed CPE's sample configuration included in this document is used during this compliance testing.

14.1. Cox managed CPE Login

The Cox managed CPE was configured with a local LAN IP Address of 10.10.98.110 and a subnet mask of 255.255.255.224. A personal computer is configured with Ethernet IP Address assigned to any IP Address other than 10.10.98.110 in the same subnet mask, for example 10.10.98.112

Launch a web browser on personal computer and enter the following URL: <http://10.10.98.110> and hit enter.

The following login window should appear:

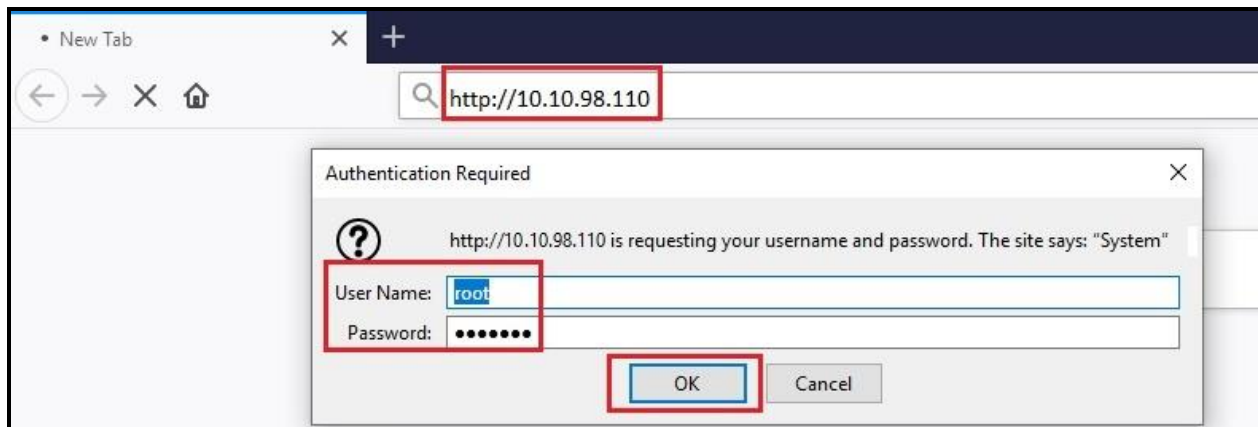


Figure 99 – Cox managed - CPE Login

- Enter **User Name** and **Password** field
- Click **OK** and the system page should be appeared next


14.2. Network Configuration

From the Configuration Menu, select Network menu option.

Under Network, input the public and private networks as followings:

- LAN Interface Settings:
 - **IP Address: 10.20.98.110** (Cox managed CPE LAN interface IP Address)
 - **Subnet Mask: 255.255.255.224**
 - Check **Enable VLAN Support**
 - **Default VLAN ID: 1**
- WAN Interface IPv4 Settings:
 - Check **Static IP**
 - **IP Address: 10.10.98.14** (Cox managed CPE WAN interface IP Address)
 - **Subnet Mask: 255.255.255.192**
- Network Settings:
 - **Default Gateway: 10.10.98.1**

Submit the changes.



[Help](#)

Configuration Menu

- + Admin
- **Network**
 - + NAT
 - VLAN
 - WAN VLAN
 - 802.1X Supplicant
 - High Availability
 - + DHCP Relay
 - + DHCP Server
 - + Traffic Shaper
 - Pass-Through Rules
 - Subinterfaces
 - Proxy ARP
 - Switch Ports
 - Static Routes
 - Dynamic DNS
 - Network Information
 - Network Restart
 - Network Test Tools
 - + WAN Failover
 - Router Advertisement
 - IP Multicast
- + Users
- + Security
- + VoIP
- + VPN

Network

Networking configuration information for the public and private networks.

LAN Interface Settings:

IP Address:

Subnet Mask:

IPv6 Address/Prefix:

Enable VLAN support: ☒

Default VLAN ID:

VLAN Configuration

WAN Interface IPv6 Settings:

Select the type of IPv6 WAN Interface to use:

☒ Disabled
☐ Static IP (ethernet)
☐ IPv6 in IPv4 Tunnel
☐ VLAN

WAN Interface IPv4 Settings:

Select the type of IPv4 WAN Interface to use:

☐ Disabled
☐ PPPoE
☐ DHCP
☒ **Static IP**
☐ VLAN

IP Address:

Subnet Mask:

Network Settings:

Default Gateway:

DNS servers:

Note: In case of dynamic links, if the manual override checkbox is not checked the address provided will be used.

Figure 100 – Cox managed CPE - Network Configuration

14.3. VLAN Configuration

There is a VLAN which has been created and configured as shown in capture below. Details how to create the VLAN is not shown.

edgewater NETWORKS **VLAN Configuration** [Help](#)

VLAN Configuration allows the user to configure VLAN support.
Note - Changes to this page may require additional changes to the 'VLAN Membership' and 'VLAN Port' pages.

| [Create/Edit VLAN](#) | [VLAN Membership](#) | [VLAN Port](#) |

VLAN Configuration								
Select: All None Delete								
	VLAN ID	IPv4 Address	Subnet Mask	IPv6 Address	IPv6 Prefix	Virtual IPv4 Address	Virtual IPv6 Address	Isolate VLAN
<input type="checkbox"/>	1	10.10.98.110	255.255.255.224					N

Create a new VLAN

Action: [Add new VLAN](#) v

VLAN ID:

IPv4 Address:

Subnet Mask:

IPv6 Address:

IPv6 Prefix:

Addresses for [High Availability](#)

Virtual IPv4 Address:

Virtual IPv6 Address:

Isolate VLAN from other VLANs ☐

[Add](#) [Reset](#)

Figure 101 – Cox managed CPE - VLAN Configuration

14.4. VoIP SIP Settings

From the **Configuration Menu**, select **VoIP** menu option → **SIP** option.

Under **SIP Settings**, input the parameters as followings:

- **SIP Server Address:** Cox Communications provided this information
- **SIP Server Port:** 5060
- **SIP Server Transport:** Select **Pass Through**
- Check **Use Custom Domain**
- **SIP Server Domain:** Cox Communications provided this information

Submit the changes.

edgewater NETWORKS **SIP Settings** [Help](#)

SIP protocol settings.

The SIP Server settings specify the address and port that all client traffic shall be forwarded to.

SIP Server Address:

SIP Server Port:

SIP Server Transport:

Exclude sips headers for TLS Transport: ☐

Use Custom Domain: ☒

SIP Server Domain:

List of SIP Servers:

Enable Multi-homed Outbound Proxy Mode: ☐

Enable Transparent Proxy Mode: ☐

Limit Outbound to listed SIP Servers: ☒

Limit Inbound to listed SIP Servers: ☒

Include UPDATE In Allow: ☒

PRACK Support: ☒

Allowed SIP Servers

This is the list of SIP Servers or registrars that are allowed when enabling the "Limit Outbound" (for transparent mode only) and "Limit Inbound" (for transparent as well as non-transparent mode) options. The configured SIP Server(s) above are always included and do not have to be in this list.

List of Allowed SIP Servers

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

SIP Server Address/FQDN

The list is currently empty

Add a new Allowed SIP Server

IP Address/FQDN:

Stale Timer

The stale timer, if set, is used to automatically delete SIP clients that have not registered within the given time period.

Stale client time (m):

Figure 102 – Cox managed CPE - VoIP SIP Settings

14.5. VoIP Survivability

From the **Configuration Menu**, select **VoIP → Survivability** to check SIP Server Reachability status. When the SIP Server connectivity is up, the status is **Active**.

Configuration Menu

- + Admin
- + Network
- + Users
- + Security
- + VoIP
 - + H.323
 - + SIP
 - + **Survivability**
 - + Clients List
 - + Test UA
- + VPN

Survivability

Survivability is a collection of features that enable the system to extend the availability of VoIP services. These features include support for redundant Softswitches/IP PBX's and local call control in the event of WAN link failure, Softswitch/IP PBX failure, or during periods of network congestion that result in loss of connectivity to a remote Softswitch/IP PBX. [Click here for more.](#)

Current Status

SIP Server Reachability:

Domain	Name	Address	Port	P	W	Transport	Lost	Rcvd	Status
DUKEBWSSCM-MTC1- [REDACTED].NET	DUKEBWSSCM02- [REDACTED].NET	192.168.15.236	5060	10	50	PassThrough	1	30	Active

Current Call Control is: Remote

Common Settings

Survivability: Enabled (auto) ▾

Time (s) between DNS lookups: 30

SIP Server Reachability Configuration

The reachability settings control how often messages are sent to the Softswitch/IP PBX and how quickly a Softswitch/IP PBX will be declared unreachable or reachable. The configuration below is used to determine Softswitch/IP PBX reachability for both redundancy and local or remote call control functions.

SIP Keepalive Messages:

Enable keepalive messages for active server ☒

Time between Keepalive messages (sec.): 60

Number of missed messages to declare alarm: 5

Number of received messages to clear alarm: 10

Interpret error code as success: 403

Figure 103 – Cox managed CPE - SIP Server Survivability

14.6. ALG Trunking Configuration

From the **Configuration Menu**, select **VoIP → SIP → ALG** option.

Under **SIP Trunking Devices**, add a trunking device as followings:

- **Action:** choose **Add new trunking device**
- **Name:** **Avaya Aura**
- **Address:** **10.10.98.111** (Avaya SBCE public interface IP Address)
- **Port:** **5060**

Select **Commit** button

edgewater NETWORKS **ALG Trunking Configuration** [Help](#)

Configuration of SIP trunking devices.

Configuration Menu

- + [Admin](#)
- + [Network](#)
- + [Users](#)
- + [Security](#)
- [VoIP](#)
 - [H.323](#)
 - [SIP](#)
 - [ALG](#)
 - [B2BUA](#)
 - [SIP Routing](#)
 - [Media Server](#)
 - [Survivability](#)
 - [Clients List](#)
 - [Test UA](#)
- + [VPN](#)

SIP Trunking devices

A SIP trunking device can be a PSTN gateway, or similar device, that does not issue REGISTER messages. Calls will be forwarded to the device based on the dial-plan rules below.

If VLANs are enabled, the SIP trunking device needs to be in the same VLAN as defined in the VoIP ALG page.

SIP Trunking Devices				
Select: All None Delete				
	Address	Port	Name	Group
<input type="checkbox"/>	10.10.98.111	5060	Avaya Aura	

Add a trunking device

Action: [Add new trunking device](#)

Name:

Address:

Port:

[Commit](#) [Reset](#)

Figure 104 – Cox managed CPE - SIP ALG Trunk Configuration

The following captured screens show the rest of the ALG Trunking Configuration page, continue from above screen. Detail configuration is not discussed here.

Header Transformation

These header transformation rules are applied to all SIP trunking devices. They define how specified SIP headers should be transformed when forwarding to the SIP Server.

From Header

Select the domain to use in From header when sending requests to the SIP Server:

☒ SIP Server Address (default)

☐ System WAN IP

Rules

Rules are used to forward and/or modify incoming and outgoing calls. There are 3 types of rules:

- Inbound: from server to trunking device
- Outbound: from trunking device to server
- Redirect: from local phone to trunking device (w/o routing to server)

Outbound rules can match against and/or modify either the calling or called number. Inbound and redirect rules operate on the called number only. Stripped and added digits always apply to the left-most digits of the DID.

Dial Rules								
Select: All None								<input type="button" value="Delete"/>
	Type	Mode	Party	PRI0	Pattern-match	Strip	Add	Trunking device
<input type="checkbox"/>	Inbound	BothModes			Default Rule			Avaya Aura (10.10.98.111:5060)

Add a rule

Action:

Type:

Mode:

Call Party:

Default rule: ☐

Priority: ☐

Pattern-match (if not default):

Strip digits:

Add string:

Trunking device:

Note: "Use SIP proxy as secondary target" rule can be configured on the B2BUA page

Figure 105 – Cox managed CPE - Header Transformation and Rules

14.7. SIP Routing Configuration

From the **Configuration Menu**, select **VoIP** → **SIP** → **SIP Routing** option. A new SIP Routing was created as below screenshot.

edgewater NETWORKS **SIP Routing** [Help](#)

Configuration Menu

- + [Admin](#)
- + [Network](#)
- + [Users](#)
- + [Security](#)
- [VoIP](#)
 - [H.323](#)
 - [SIP](#)
 - [ALG](#)
 - [B2BUA](#)
 - [SIP Routing](#)
 - [Media Server](#)
 - [Survivability](#)
 - [Clients List](#)
 - [Test UA](#)
- + [VPN](#)

Create New Routing Group

Name:

Select group members:

	Name	URI
<input type="checkbox"/>	Avaya Aura	sip:10.10.98.111:5060

Existing Routing Groups

Name	Domain	State
No Entries		

Members:

Name	URI	Last Event	State
No Entries			

Keepalives

Interval: From User:

Error Response: To User:

☒ Backoff on No response:

☒ Regular with max. Interval: sec

☐ Random with max. Interval: sec

Figure 106 – Cox managed CPE – SIP Routing Configuration

©2019 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.