



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring IntelPeer CoreCloud SIP Trunk with Avaya Aura[®] Communication Manager 7.0, Avaya Aura[®] Session Manager 7.0 and Avaya Session Border Controller for Enterprise 7.0 – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between IntelPeer CoreCloud SIP Trunk and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura[®] Session Manager 7.0, Avaya Aura[®] Communication Manager 7.0, Avaya Session Border Controller for Enterprise 7.0 and various Avaya endpoints.

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

Table of Contents

1.	INTRODUCTION.....	4
2.	GENERAL TEST APPROACH AND TEST RESULTS	4
2.1.	INTEROPERABILITY COMPLIANCE TESTING	4
2.2.	TEST RESULTS	5
2.3.	SUPPORT.....	6
3.	REFERENCE CONFIGURATION	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	15
5.6.	CONFIGURE IP INTERFACE FOR PROCR	16
5.7.	SIGNALING GROUP	16
5.8.	TRUNK GROUP	18
5.9.	CALLING PARTY INFORMATION.....	22
5.10.	OUTBOUND ROUTING	23
5.11.	INCOMING CALL HANDLING TREATMENT	27
5.12.	AVAYA AURA® COMMUNICATION MANAGER STATIONS	28
5.13.	SAVE AVAYA AURA® COMMUNICATION MANAGER CONFIGURATION CHANGES.....	28
6.	CONFIGURE AVAYA AURA® SESSION MANAGER	29
6.1.	AVAYA AURA® SYSTEM MANAGER LOGIN AND NAVIGATION	30
6.2.	SPECIFY SIP DOMAIN	32
6.3.	ADD LOCATION	33
6.4.	ADD SIP ENTITIES	34
6.4.1.	<i>Configure Session Manager SIP Entity.....</i>	<i>35</i>
6.4.2.	<i>Configure Communication Manager SIP Entity</i>	<i>37</i>
6.4.3.	<i>Configure Avaya Session Border Controller for Enterprise SIP Entity.....</i>	<i>38</i>
6.5.	ADD ENTITY LINKS	38
6.6.	CONFIGURE TIME RANGES	40
6.7.	ADD ROUTING POLICIES.....	40
6.8.	ADD DIAL PATTERNS	42
7.	CONFIGURE AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE	46
7.1.	LOG IN AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE	47
7.2.	GLOBAL PROFILES.....	50
7.2.1.	<i>Configure Server Interworking Profile - Avaya site.....</i>	<i>50</i>
7.2.2.	<i>Configure Server Interworking Profile – IntelPeer CoreCloud SIP Trunk site.....</i>	<i>51</i>
7.2.3.	<i>Configure Signaling Manipulation.....</i>	<i>52</i>
7.2.4.	<i>Configure Server – Avaya site.....</i>	<i>53</i>
7.2.5.	<i>Configure Server – IntelPeer CoreCloud SIP Trunk.....</i>	<i>55</i>
7.2.6.	<i>Configure Routing – Avaya site</i>	<i>57</i>
7.2.7.	<i>Configure Routing – IntelPeer CoreCloud SIP Trunk site</i>	<i>58</i>
7.2.8.	<i>Configure Topology Hiding – Avaya site</i>	<i>59</i>
7.2.9.	<i>Configure Topology Hiding – IntelPeer CoreCloud SIP Trunk site.....</i>	<i>60</i>
7.3.	CREATE ENDPOINT POLICY GROUPS	61
7.4.	DEVICE SPECIFIC SETTINGS.....	63

7.4.1. Manage Network Settings.....	63
7.4.2. Create Media Interfaces.....	66
7.4.3. Create Signaling Interfaces.....	67
7.4.4. Configuration Server Flows	68
7.4.4.1 Create End Point Flows – SMVM Flow.....	68
7.4.4.2 Create End Point Flows – IntelPeer CoreCloud SIP Trunk Flow	69
8. INTELEPEER CORECLOUD SIP TRUNK CONFIGURATION.....	69
9. VERIFICATION STEPS.....	70
10. CONCLUSION.....	71
11. REFERENCES.....	72
12. APPENDIX A – REMOTE WORKER CONFIGURATION	74
12.1. NETWORK MANAGEMENT ON AVAYA SBCE	76
12.2. MEDIA INTERFACE ON AVAYA SBCE	78
12.3. SIGNALING INTERFACE ON AVAYA SBCE.....	79
12.4. SERVER INTERWORKING CONFIGURATION ON AVAYA SBCE	80
12.5. SERVER CONFIGURATION ON AVAYA SBCE	81
12.6. ROUTING PROFILE ON AVAYA SBCE	83
12.7. USER AGENT ON AVAYA SBCE	85
12.8. RELAY SERVICES ON AVAYA SBCE.....	87
12.9. MAPPING PROFILES ON AVAYA SBCE	89
12.10. APPLICATION RULES ON AVAYA SBCE	90
12.11. MEDIA RULES ON AVAYA SBCE.....	91
12.12. END POINT POLICY GROUPS ON AVAYA SBCE	92
12.13. END POINT FLOWS ON AVAYA SBCE.....	94
12.13.1. Subscriber Flow	94
12.13.2. Server Flow on Avaya SBCE.....	97
12.13.2.1 Remote Worker Server Flow	97
12.13.2.2 Trunking Server Flow on Avaya SBCE.....	98
12.14. SYSTEM MANAGER.....	99
12.14.1. Modify Session Manager Firewall: Elements → Session Manager → Network Configuration → SIP Firewall.....	99
12.14.2. Disable PPM Limiting: Elements → Session Manager → Session Manager Administration	101
12.15. REMOTE WORKER CLIENT CONFIGURATION	102
SIP Global Settings Screen	102
13. APPENDIX B: SIGMA SCRIPT	103

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between IntelPeer CoreCloud SIP Trunk and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager 7.0, Avaya Aura® Communication Manager 7.0, Avaya Session Border Controller for Enterprise (Avaya SBCE) 7.0 and various Avaya endpoints.

Customers using this Avaya SIP-enabled enterprise solution with IntelPeer CoreCloud 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 IntelPeer CoreCloud 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.

2.1. Interoperability Compliance Testing

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

- Response to SIP OPTIONS queries.
- Incoming PSTN calls to various phone types including H.323, SIP, digital, and analog telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types including H.323, SIP, digital, and analog telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from softphones. Two Avaya soft phones were used in testing: Avaya one-X® Communicator (1XC) and Avaya Communicator 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 Communicator for Windows was used in testing as a simple SIP endpoint for basic inbound/outbound calls.

- SIP transport using UDP and port 5060 as supported.
- 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.
- Various call types including: local call, long distance, international, outbound toll-free, inbound toll-free, and 911 services.
- Codec G.711MU and G.729A.
- 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).
- Use of SIP re-Invite for call transfer.
- Use of the Diversion Header for call forward.
- Call Center scenarios.
- Fax using G.711 pass-through mode.
- Mobility EC500.
- DTMF - RFC2833.
- Remote Worker.

Items not supported included the following:

- Operator Assisted Calls.
- Local Directory Assistance Calls (e.g. 411 in US).

2.2. Test Results

Interoperability testing of IntelPeer CoreCloud SIP Trunk was completed with successful results for all test cases with the exception of the observations described below.

- **IntelPeer CoreCloud supported the SIP REFER, however the call was not established successfully between PSTN phones after completing off-net blind/attended call transfer using SIP REFER Method** – For this call scenario, IntelPeer expected Avaya CM to release the trunks and shuffle media after completing off-net call transfer using SIP REFER. However, as design intend of Avaya CM, Avaya CM did not release the trunks and shuffle media unless Avaya CM received 180 ringing or 200 OK sipfrag NOTIFY from IntelPeer CoreCloud. As the result, IntelPeer CoreCloud could not establish the call between PSTN phones after completing off-net call transfer using SIP REFER. This issue is under investigation by IntelPeer CoreCloud.

- **Dynamic match of Payload Type was in failure of out-band DTMF - RFC2833 tone transmission** - IntelPeer CoreCloud could not configure the capable of dynamically matching to different RFC2833 payload types at the same time from the enterprise site. Therefore, administrator makes sure to use either Payload Type 101 or 120 for RFC2833 DTMF but not both at the same time. All endpoints must support the same DTMF Payload type.

2.3. Support

For technical support on the IntelPeer CoreCloud SIP Trunk Service, please contact customer service at 1-866-780-8639 or visit: <http://www.intelepeer.com/SIPTrunking>.

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

3. Reference Configuration

Figure 1 illustrates a sample Avaya SIP-enabled enterprise solution connected to IntelPeer CoreCloud SIP Trunk. This was 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.

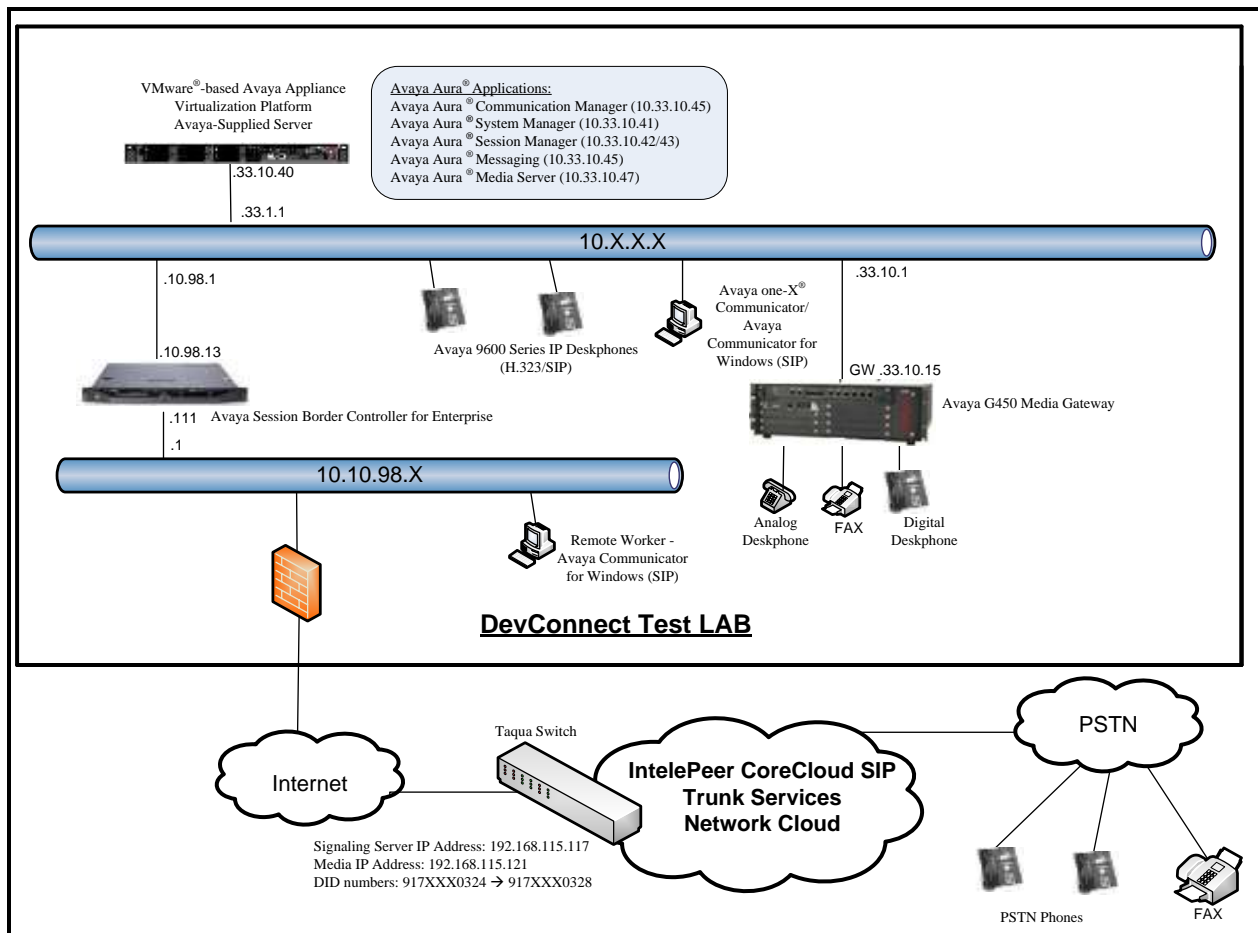


Figure 1: Avaya IP Telephony Network and IntelPeer CoreCloud SIP Trunk

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	7.0.0.1.0-SP1 (Patch-00.0.441.0-22477)
Avaya G450 Media Gateway <ul style="list-style-type: none"> – MM711AP Analog – MM712AP Digital – MM710AP 	FW 37.19.0 HW46 FW096 HW10 FW014 HW05 FW020
Avaya Aura [®] Session Manager running on VMware [®] -based Avaya appliance	7.0.0.0 Build No: 7.0.0.0.700001-7.0.0.0
Avaya Aura [®] System Manager running on VMware [®] -based Avaya appliance	7.0.0.0 Build No: 7.0.0.0.16266-7.0.9.912 Software Update Revision No: 7.0.0.0.3929
Avaya Aura [®] Messaging running on VMware [®] -based Avaya appliance	N6.3-69.0 - 335
Avaya Aura [®] Media Server running on VMware [®] -based Avaya appliance	7.7.0.226
Avaya Session Border Controller for Enterprise running on Dell R210 V2 Server	7.0.0-21-6602
Avaya 9621G IP Deskphone (SIP)	7.0.0.39
Avaya 9621G IP Deskphone (H.323)	6.6029
Avaya 9641 IP Deskphone (H.323)	6.6029
Avaya Digital Deskphones (1408D)	R40
Avaya Communicator for Windows	2.1.2.75 SP2
Avaya one-X [®] Communicator (H.323 & SIP)	6.2.6-03-FP6
Nortel Symphony 2000 Analog telephone	N/A
HP Officejet 4500 Fax	N/A
IntelPeer CoreCloud SIP Trunk Components	
Equipment/Software	Release/Version
Taqua	3.1.1.7

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: From Release 7.0, Avaya uses the VMware®-based Avaya Appliance Virtualization Platform to provide virtualization for Avaya Aura® applications in Avaya appliance offer. Avaya-appliance offer includes:

- Common Servers: Dell™ PowerEdge™ R610, Dell™ PowerEdge™ R620, HP ProLiant DL360 G7 (It was used for this compliance testing), and HP ProLiant DL360p G8
- S8300D and S8300E

Appliance Virtualization Platform is the customized OEM version of VMware® ESXi 5.5. With Appliance Virtualization Platform, customers can run any combination of supported applications such as Avaya Aura® Communication Manager, Avaya Aura® System Manager, Avaya Aura® Session Manager, Avaya Aura® Messaging, and Avaya Aura® Media Server on Avaya-supplied servers. Appliance Virtualization Platform provides greater flexibility in scaling customer solutions to individual requirements. Appliance Virtualization Platform is available only in an Avaya-appliance offer. Avaya-appliance offer does not support VMware tools, such as vCenter and vSphere Client. You can configure and manage Appliance Virtualization Platform by using Solution Deployment Manager that is part of System Manager, or by installing the Solution Deployment Manager client.

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 IntelPeer CoreCloud 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 4000 SIP trunks are available and 100 are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity.

display system-parameters customer-options		Page	2 of 11
OPTIONAL FEATURES			
IP PORT CAPACITIES		USED	
Maximum Administered H.323 Trunks:		4000	0
Maximum Concurrently Registered IP Stations:		2400	2
Maximum Administered Remote Office Trunks:		4000	0
Maximum Concurrently Registered Remote Office Stations:		2400	0
Maximum Concurrently Registered IP eCons:		68	0
Max Concur Registered Unauthenticated H.323 Stations:		100	0
Maximum Video Capable Stations:		2400	0
Maximum Video Capable IP Softphones:		2400	5
Maximum Administered SIP Trunks:		4000	100
Maximum Administered Ad-hoc Video Conferencing Ports:		4000	0
Maximum Number of DS1 Boards with Echo Cancellation:		80	0

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 11
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 11
OPTIONAL FEATURES		
Multinational Locations? n	Station and Trunk MSP? y	
Multiple Level Precedence & Preemption? n	Station as Virtual Extension? y	
Multiple Locations? n	System Management Data Transfer? n	
Personal Station Access (PSA)? y	Tenant Partitioning? y	
PNC Duplication? n	Terminal Trans. Init. (TTI)? y	
Port Network Support? n	Time of Day Routing? y	
Posted Messages? y	TN2501 VAL Maximum Capacity? y	
Private Networking? y	Uniform Dialing Plan? y	
Processor and System MSP? y	Usage Allocation Enhancements? y	
Processor Ethernet? y	Wideband Switching? y	
Remote Office? y	Wireless? n	
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 20
      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 of Communication Manager (**procr**) and Session Manager (**bwasm2**). 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	
bwasm2	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. For the compliance test, ip-codec-set 1 was used for this purpose. IntelPeer CoreCloud SIP Trunk supports the **G.711MU** and **G.729** codecs. Default values can be used for all other fields.

change ip-codec-set 1

Page1 of2

IP CODEC SET

Codec Set: 1

Audio	Silence	Frames	Packet
Codec	Suppression	Per Pkt	Size(ms)
1: G.711MU	n	2	20
2: G.729	n	2	20

Figure 8: IP-Codec-Set Form – Page 1

On **Page 2**, set the **FAX Mode** to **off**. IntelPeer CoreCloud supports Fax using G.711 pass-through mode.

change ip-codec-set 1

Page2 of 2

IP CODEC SET

Allow Direct-IP Multimedia? n

	Mode	Redundancy	Packet Size (ms)
FAX	off	0	
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 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 **bvwdev.com**. This name appears in the From header of SIP messages originating from this IP region.
- Enter a descriptive name in the **Name** field.
- Enable IP-IP Direct Audio (shuffling) to allow audio traffic to be sent directly between IP endpoints without using media resources in the Avaya Media Gateway. 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: bvwdev.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

5.6. Configure IP Interface for procr

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

change ip-interface procr	
IP INTERFACES	
Type: PROCR	Target socket load: 4800
Enable Interface? y	Allow H.323 Endpoints? y
Network Region: 1	Allow H.248 Gateways? y
	Gatekeeper Priority: 5
IPV4 PARAMETERS	
Node Name: procr	IP Address: 10.33.10.44
Subnet Mask: /24	

Figure 11: IP-Interface Form

5.7. Signaling Group

Use the **add signaling-group** command to create signaling groups between Communication Manager and Session Manager. The signaling groups are used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group **20** was used for both outbound and inbound calls. It was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- Set the **IMS Enabled** field to **n**. This specifies the Communication Manager will serve as an Evolution Server for Session Manager.
- Set the **Transport Method** to the value of **tcp** (Transmission Control Protocol). The transport method specified here is used between Communication Manager and Session Manager. TLS (Transport Layer Security) is the recommended setting, but TCP was used during testing to aid in debugging.
- 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 TCP, as **5060**.
- Set the **Far-end Network Region** to the IP network region defined for the service provider in **Section 5.5**.
- Set the **Far-end Domain** to **bwvdev.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 Media Gateway will not remain in the media path of all calls between the SIP trunk and the endpoint.
- Set the **Alternate Route Timer** to **6**. This defines the number of seconds the Communication Manager will wait for a response (other than 100 Trying) to an outbound INVITE before selecting another route. If an alternate route is not defined, then the call is cancelled after this interval.
- Default values may be used for all other fields.

```

add signaling-group 20                                     Page 1 of 2
                                     SIGNALING GROUP

Group Number: 20                      Group Type: sip
IMS Enabled? n                      Transport Method: tcp
    Q-SIP? n
    IP Video? n                      Enforce SIPS URI for SRTP? y
Peer Detection Enabled? y Peer Server: SM
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: bwvasm2
Near-end Listen Port: 5060             Far-end Listen Port: 5060
                                     Far-end Network Region: 1
                                     Far-end Secondary Node Name:

Far-end Domain: bwvdev.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 12: Signaling-Group

5.8. Trunk Group

Use the **add trunk-group** command to create trunk groups for the signaling groups created in **Section 5.7**. For the compliance test, trunk group **20** was used for both outbound and inbound calls. 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. (i.e. ***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 21	
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	Auth Code? n		
Service Type: public-ntwrk	Member Assignment Method: auto		
	Signaling Group: 20		
	Number of Members: 50		

Figure 13: 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 SIP UPDATES must be sent to keep the active session alive. For the compliance test, the value of **600** seconds was used.

add trunk-group 20		Page 2 of 21
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): 600		
Disconnect Supervision - In? y Out? y		
XOIP Treatment: auto Delay Call Setup When Accessed Via IGAR? n		

Figure 14: 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 11 digit numbering format. Thus, **Numbering Format** was set to **public** and the **Numbering Format** field in the route pattern was set to **pub-unk** (see **Section 5.10**).

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

add trunk-group 20		Page 3 of 21
TRUNK FEATURES		
ACA Assignment? n	Measured: none	Maintenance Tests? y
Numbering Format: public		
UI Treatment: service-provider		
Replace Restricted Numbers? y		
Replace Unavailable Numbers? y		
Hold/Unhold Notifications? y		
Modify Tandem Calling Number: no		
Show ANSWERED BY on Display? y		

Figure 15: Trunk-Group – Page 3

On **Page 4**, the **Network Call Redirection** field can be set to **n** (default setting) so that the SIP REFER is not sent. Note: IntelPeer CoreCloud supported the SIP REFER, however the call was not established successfully between PSTN phones after completing off-net call transfer using a Blind/Attended Transfer REFER Method (see **Section 2.1**).

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 re-directed. These settings are needed to support call forwarding of inbound calls back to the PSTN and some Extension to Cellular (EC500) call scenarios.

add trunk-group 20	Page 4 of 21
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 16: Trunk-Group – Page 4

5.9. Calling Party Information

The calling party number is sent in the SIP “From”, “Contact” and “PAI” headers. Since public numbering was selected to define the format of this number (**Section 5.8**), use the **change public-unknown-numbering** command to create an entry for each extension which has a DID assigned. The DID numbers are provided by the SIP 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 this compliance testing, all stations with a 4-digit extension beginning with **03** will send the calling party number as the **CPN Prefix** plus the extension number.

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	03	20	917999	10	Total Administered: 1

Figure 17: 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 **6** is used as the ARS access code. Enterprise callers will dial **6** to reach an “outside line”. This common configuration is illustrated below. Use the **change dialplan analysis** command to define the **Dialed String** as followings:

- **Dialed String** beginning with **03** for creating the local stations in **Section 5.12**.
- **Dialed String** beginning with **181** and **800** for Voicemail testing purpose.
- **Dialed String** beginning with **6** for feature access code (**fac**).
- **Dialed String** beginning with ***** 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	
03	4	ext							
181	4	ext							
6	1	fac							
800	4	ext							
*	4	dac							

Figure 18: Dialplan–Analysis Form

Use the **change feature-access-codes** command to configure **6** 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: 6		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 19: Feature–Access-Codes Form

Use the **change ars analysis** command to configure the routing of dialed digits following the first digit **6**. 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 to the service provider (as defined in next section).

change ars analysis 0							Page 1 of 2
ARS DIGIT ANALYSIS TABLE							
Location: all							Percent Full: 1
Dialed String	Total Min	Total Max	Route Pattern	Call Type	Node Num	ANI Req'd	
1416	11	11	20	pubu		n	
1613	11	11	20	pubu		n	
1800	11	11	20	pubu		n	
4420	4	12	20	pubu		n	
911	3	3	20	pubu		n	
917	10	10	20	pubu		n	

Figure 20: 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 21: 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 to use feature access code (fac) 6 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 22: 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 DID number sent by Service Provider is unchanged by Session Manager, then 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 followings:

- The incoming DID number **+1855XXX2970** to **0324** by deleting **12** of incoming digits for inbound toll-free testing purpose.
- The incoming DID number **+1917XXX0328** to **8000** by deleting **12** of incoming digits for voicemail testing purpose.
- The incoming DID number **+1917XXXYYYY** to 4 digit extension **YYYY** by deleting **8** of the incoming digits for inbound call testing purpose.
- The incoming DID number **+917XXXYYYY** to 4 digit extension **YYYY** by deleting **7** of the incoming digits for inbound local call testing purpose.

change inc-call-handling-trmt trunk-group 20				Page 1 of 3	
INCOMING CALL HANDLING TREATMENT					
Service/ Feature	Number Len	Number Digits	Del	Insert	
public-ntwrk	12	+1855XXX2970	12	0324	
public-ntwrk	12	+1917XXX0328	12	8000	
public-ntwrk	12	+1917XXX	8		
public-ntwrk	11	+917XXX	7		

Figure 23: Inc-Call-Handling-Trmt Form

5.12. Avaya Aura® Communication Manager Stations

In the sample configuration, a four-digit station extension was used with the format 03XX. Use the **add station 0324** command to add an Avaya H.323 IP Deskphone.

- Enter **Type: 9641, Name: 0324, Security Code: 1234, Coverage Path 1: 1, COR: 1, IP SoftPhone: y** (if this extension is used for a Softphone such as Avaya one-X® Communicator)
- Leave other values as default.

add station 0324		Page 1 of 5
STATION		
Extension: 0324	Lock Messages? n	BCC: 0
Type: 9641	Security Code: 1234	TN: 1
Port: S00002	Coverage Path 1: 1	COR: 1
Name: 0324	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: 0324	
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 24: Add-Station Form

5.13. Save Avaya Aura® Communication Manager Configuration Changes

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

6. Configure Avaya Aura[®] Session Manager

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

- SIP Domain.
- Logical/physical Location that can be occupied by SIP Entities.
- SIP Entities corresponding to Communication Manager, Avaya SBCE and Session Manager.
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities.
- Routing Policies, which 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 been defined already 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 System Manager home screen is shown below.

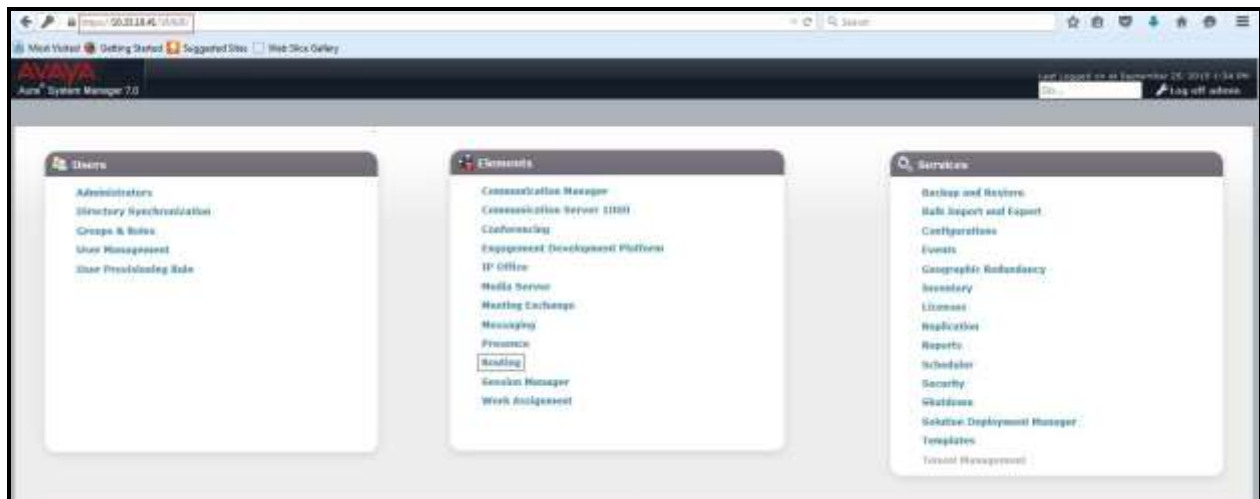


Figure 25: System Manager Home Screen

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

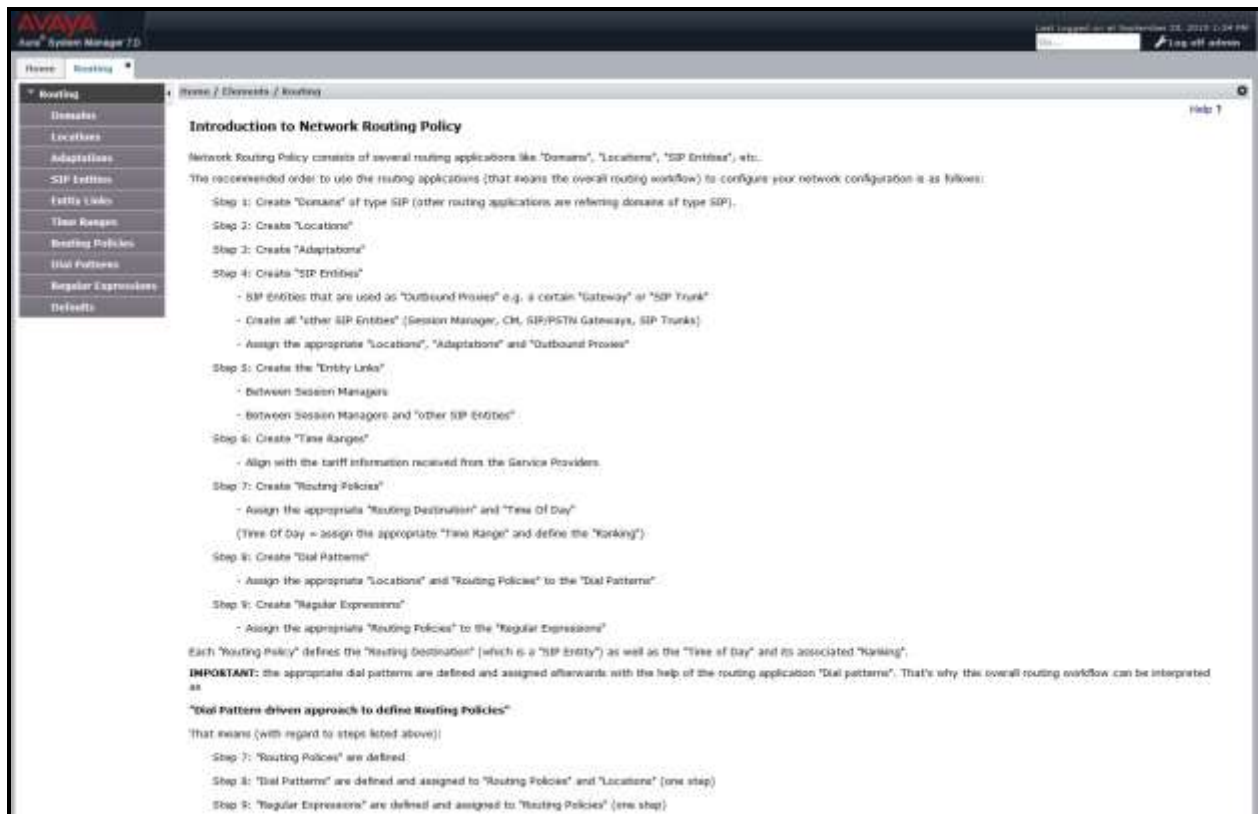


Figure 26: Network Routing Policy

6.2. Specify SIP Domain

Create a SIP Domain for each domain of which Session Manager will need to be aware in order to route calls. For the compliance test, this includes the enterprise domain **bwvdev.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 27: 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 System Manager 7.0 interface. The left-hand navigation pane is open, showing the 'Routing' section with 'Locations' selected. The main pane displays the 'Location Details' configuration page. The 'General' tab is active. The 'Name' field is populated with 'Belleville-GSSCP'. The 'Notes' field is empty. The 'Dial Plan Transparency in Survivable Mode' section has an 'Enabled' checkbox. The 'Overall Managed Bandwidth' section has fields for 'Managed Bandwidth Units' (set to Kbit/sec), 'Total Bandwidth', and 'Multimedia Bandwidth'. The 'Per-Call Bandwidth Parameters' section has fields for 'Maximum Multimedia Bandwidth (Intra-Location)', 'Maximum Multimedia Bandwidth (Inter-Location)', 'Minimum Multimedia Bandwidth', and 'Default Audio Bandwidth'.

Figure 28: 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 29: 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 **Other** for Avaya SBCE.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. Adaptation module was not used in this configuration.
- **Location:** Select the Location that applies to the SIP Entity being created. For the compliance test, all components were located in Location **Belleville-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**.

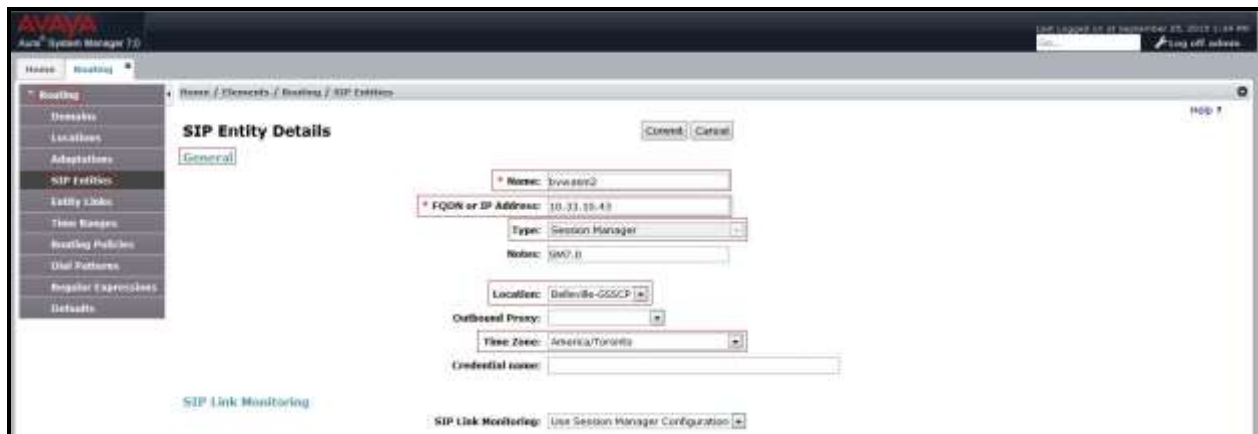


Figure 30: Session Manager SIP Entity

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 **5060** with **TCP** for connecting to Communication Manager, port **5070** with **TCP** for connecting Avaya SIP phones and SIP soft clients, port **5060** with **UDP** for connecting to Avaya SBCE.



Figure 31: 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 **CM7**. 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 System Manager 7.0 web interface. The left-hand navigation pane includes links for Home, Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, URI Patterns, Regular Expressions, and Defaults. The 'SIP Entities' link is selected, leading to the 'SIP Entity Details' page for an entity named 'CM7'. The page has a breadcrumb trail: Home / Elements / Routing / SIP Entities. The 'General' tab is active. The configuration fields are as follows: Name: CM7; FQDN or IP Address: 10.33.10.44; Type: CM; Notes: (empty); Adaptation: (dropdown menu); Location: Dallas-OSGCP; Time Zone: America/Toronto; SIP Timer B/F (in seconds): 4; Credential name: (empty); Securable: (checkbox, unchecked); Call Detail Recording: none; Loop Detection: (checkbox, unchecked); Loop Detection Mode: Off; SIP Link Monitoring: Link Monitoring Enabled; Proactive Monitoring Interval (in seconds): 900; Reactive Monitoring Interval (in seconds): 120; Number of Retries: 1; Supports Call Admission Control: (checkbox, unchecked); Shared Bandwidth Manager: (checkbox, unchecked); Primary Session Manager Bandwidth Association: (dropdown menu); Backup Session Manager Bandwidth Association: (dropdown menu). Buttons for 'Cancel' and 'Cancel' are at the top right, and a 'Help ?' link is in the top right corner.

Figure 32: 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 **Other** was selected for **Type**. The user will need to select the specific values for the **Location** and **Time Zone**.

The screenshot shows the Avaya System Manager 7.0 interface. The left-hand navigation pane is open, showing a tree structure with 'Routing' selected. Under 'Routing', 'SIP Entity' is highlighted. The main pane displays the 'SIP Entity Details' configuration page for an entity named 'SBCE'. The 'General' tab is active. The 'FQDN or IP Address' field is set to '10.10.98.13' and the 'Type' is set to 'Other'. The 'Location' is set to 'Default' and the 'Time Zone' is set to 'America/Toronto'. Other fields include 'SIP Timer B/F (in seconds)' set to '0', 'Credential name', 'Securable', 'Call Detail Recording' set to 'none', 'CoreProfile Type Preference', 'Loop Detection Mode' set to 'Off', 'SIP Link Monitoring' set to 'Link Monitoring Enabled', 'Proactive Monitoring Interval (in seconds)' set to '600', 'Reactive Monitoring Interval (in seconds)' set to '120', 'Number of Entries' set to '1', 'Supports Call Admission Control', 'Shared Bandwidth Manager', 'Primary Session Manager Bandwidth Association', and 'Backup Session Manager Bandwidth Association'.

Figure 33: Avaya SBCE SIP Entity

6.5. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created: one to Communication Manager for use only by service provider traffic and one to the Avaya SBCE.

To add an Entity Link, navigate to **Routing → Entity Links** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown 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. (Ex: For the Communication Manager Entity Link, this must

match the **Far-end Listen Port** defined on the Communication Manager signaling group in **Section 5.7**).

- **SIP Entity 2:** Select the name of the other system as defined in **Section 6.4**.
- **Port:** Port number on which the other system receives SIP requests from the Session Manager. (Ex: For the Communication Manager Entity Link, this must match the **Near-end Listen Port** defined on the Communication Manager signaling group in **Section 5.7**).
- **Trusted:** Check this box. **Note:** If this box is not checked, calls from the associated SIP Entity specified in **Section 6.4** will be denied.

Click **Commit** to save.

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



Figure 34: Communication Manager Entity Link

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



Figure 35: Avaya SBCE Entity Link

6.6. Configure Time Ranges

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



Figure 36: 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 **IntelePeer_Inbound_To_CM** associated with incoming PSTN calls from IntelePeer CoreCloud SIP Trunk to Communication Manager. Observe the **SIP Entity as Destination** is the entity named **CM7**.



Figure 37: Routing to Communication Manager

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



Figure 38: Routing to IntelPeer CoreCloud 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 IntelPeer CoreCloud 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 **IntelPeer_Outbound_To_SBCE** as defined in **Section 6.7**.

The screenshot displays the Avaya System Manager 7.0 interface for configuring a Dial Pattern. The 'Dial Pattern Details' window is open, showing the 'General' tab. The 'Pattern' field is set to '1613', 'Min' is '1', and 'Max' is '11'. The 'SIP Domain' is 'bwvdev.com'. The 'Notes' field contains 'IntelPeer Outbound Calls'. Below the main form, the 'Originating Locations and Routing Policies' section shows a table with one entry. The table has columns for Originating Location Name, Originating Location Rate, Routing Policy Name, Rank, Routing Policy (Modified), Routing Policy Destination, and Routing Policy Notes. The entry shows '-4U-' for Originating Location Name, 0 for Originating Location Rate, IntelPeer_Outbound_To_SBCE for Routing Policy Name, 0 for Rank, SBCE for Routing Policy (Modified), and SBCE for Routing Policy Destination.

Originating Location Name	Originating Location Rate	Routing Policy Name	Rank	Routing Policy (Modified)	Routing Policy Destination	Routing Policy Notes
-4U-	0	IntelPeer_Outbound_To_SBCE	0	SBCE	SBCE	

Figure 39: Dial Pattern_1613

Note that with the above Dial Pattern, IntelPeer 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 12-digit numbers that start with +1917 use Routing Policy Name **IntelPeer_Inbound_To_CM** as defined in **Section 6.7**. This Dial Pattern matches the DID numbers assigned to the enterprise by IntelPeer CoreCloud SIP Trunk.

Avaya Aura System Manager 7.0

Home / Routing / Dial Patterns

Dial Pattern Details

General

Pattern: +1917

Min: 6

Max: 12

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: sip-dev.com

Notes: IntelPeer Inbound Calls

Originating Location and Routing Policies

Originating Location Name	Originating Location Notes	Routing Policy Name	Route	Routing Policy Enabled	Routing Policy Destination	Routing Policy Notes
All		IntelPeer_Inbound_To_CM	1	<input checked="" type="checkbox"/>	CM7	

Select: All, None

Figure 40: Dial Pattern_+1917

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	Rules
00	2	6	<input type="checkbox"/>			brnlev.com	IntelPeer Local SIP Phones
1416	4	11	<input type="checkbox"/>			brnlev.com	IntelPeer Outbound Calls
1612	3	11	<input type="checkbox"/>			brnlev.com	IntelPeer Outbound Calls
1800	4	11	<input type="checkbox"/>			brnlev.com	IntelPeer Outbound Calls
1810	4	6	<input type="checkbox"/>			brnlev.com	For AMN/MI
1855	3	12	<input type="checkbox"/>			brnlev.com	IntelPeer Inbound Toll Free Calls
1917	3	12	<input type="checkbox"/>			brnlev.com	IntelPeer Inbound Calls
4420	4	12	<input type="checkbox"/>			brnlev.com	IntelPeer International Outbound Calls
811	3	3	<input type="checkbox"/>			brnlev.com	IntelPeer Outbound Calls
917	3	18	<input type="checkbox"/>			brnlev.com	IntelPeer Local Calls

Figure 41: 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 IntelPeer CoreCloud SIP Trunk system.

In this testing, according to the configuration reference **Figure 1**, the Avaya elements reside on the Private side and the IntelPeer CoreCloud SIP Trunk 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 about Avaya SBCE, refer to the documentation listed in **Section 11** of these Application Notes.

7.1. Log in Avaya Session Border Controller for Enterprise

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

Enter the **Username** and **Password** and click on **Log In** button.



Figure 42: Avaya SBCE Login

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

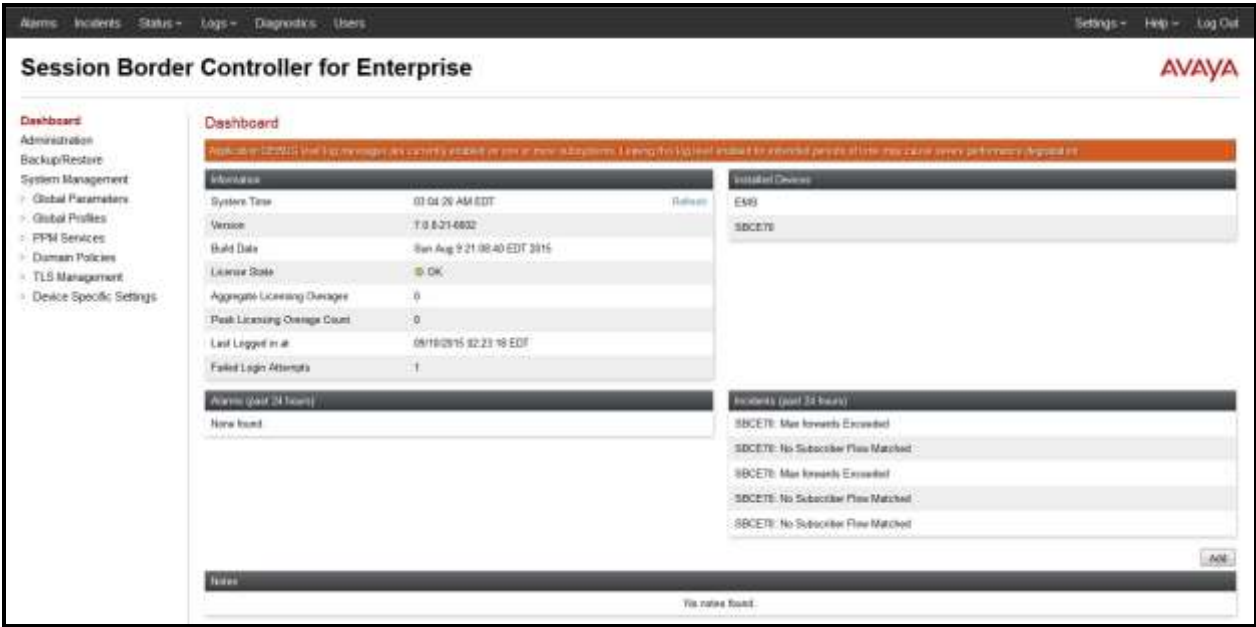


Figure 43: Avaya SBCE Dashboard

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 **SBCE70** was already added. To view the configuration of this device, click **View** as shown in the screenshot below.



Figure 44: 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 corresponded to **Figure 1**. The **Box Type** was set to **SIP** and the **Deployment Mode** was set to **Proxy**.

System Information: SBCE70

General Configuration

Appliance Name SBCE70
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
Encryption ☒

Network Configuration

IP	Public IP	Netmask	Gateway	Interface
10.10.98.13	10.10.98.13	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
10.10.98.99	10.10.98.99	255.255.255.224	10.10.98.97	B1
10.10.98.21	10.10.98.21	255.255.255.192	10.10.98.1	A1

DNS Configuration

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

Management IP(s)

IP 10.33.10.29

Figure 45: Avaya SBCE System Information

7.2. Global Profiles

When selected, Global Profiles allow configuring 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.

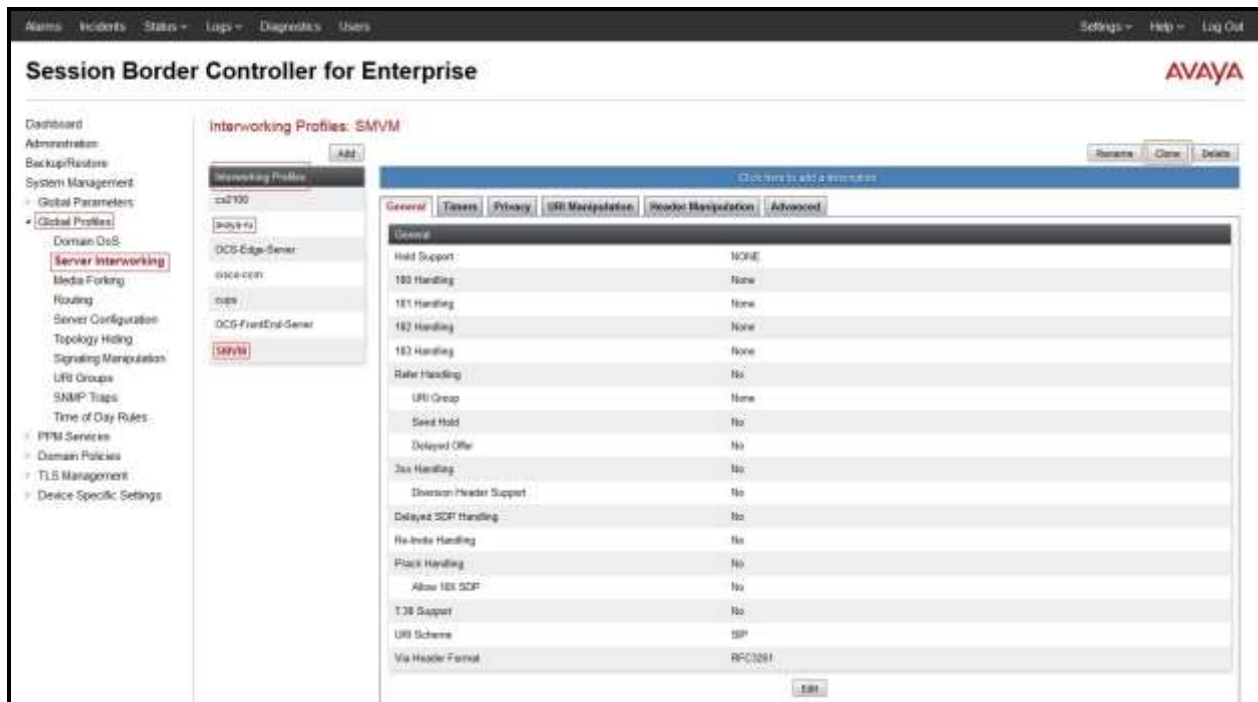


Figure 46: Server Interworking – Avaya site

7.2.2. Configure Server Interworking Profile – IntelPeer CoreCloud 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 IntelPeer CoreCloud SIP Trunk server interworking profile (named: **SP4**) was added.

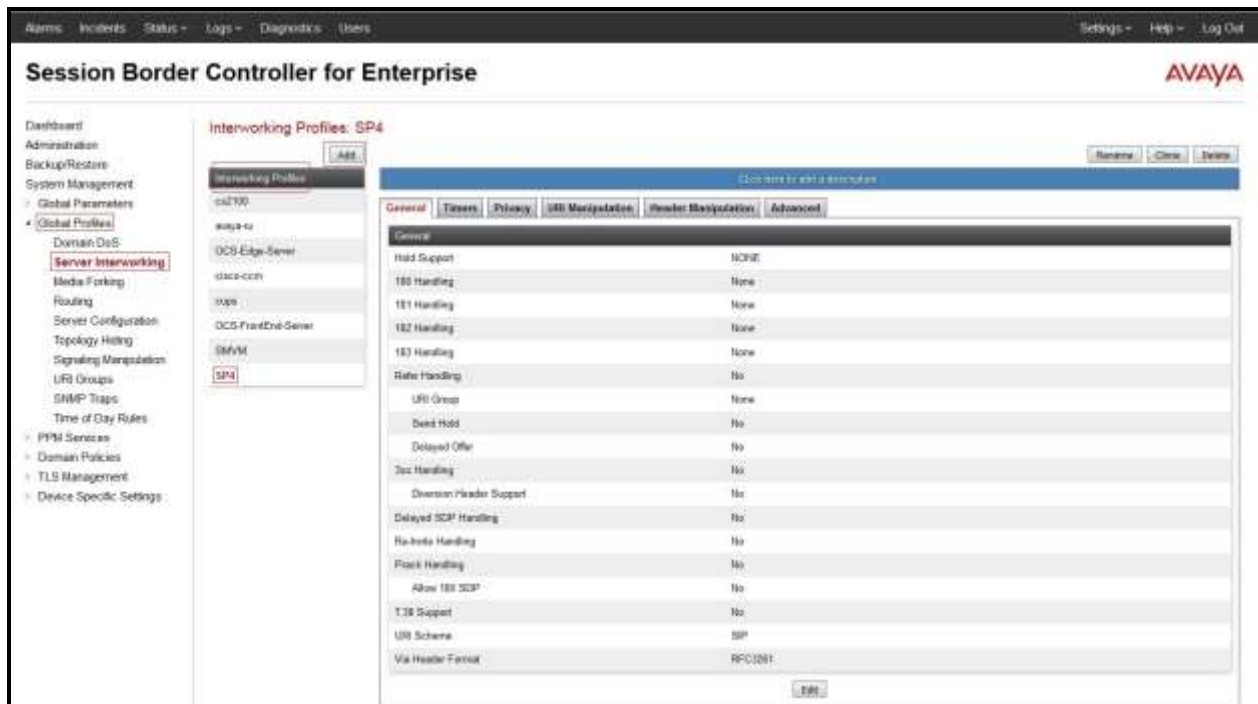


Figure 47: Server Interworking – IntelPeer CoreCloud SIP Trunk site

From the list of **Interworking Profiles**, click on **SP4** to edit.

- On the **URI Manipulation** tab, click **Add** button to create the URI manipulation to add the prefix “+” sign in front of user number for any outbound calls. When a URI [user@domain] matches the following: **Domain Regex** as **bvwddev.com**, do this with the user section: **User Action** → **Add prefix[Value]**, enter **User Values 1: +** (Not shown).

Note: IntelPeer CoreCloud SIP Trunk requires numbers to be given in E.164 with leading plus for all fields. This applies for both Request-URI, To- and From-header as well as for example the Diversion-header.

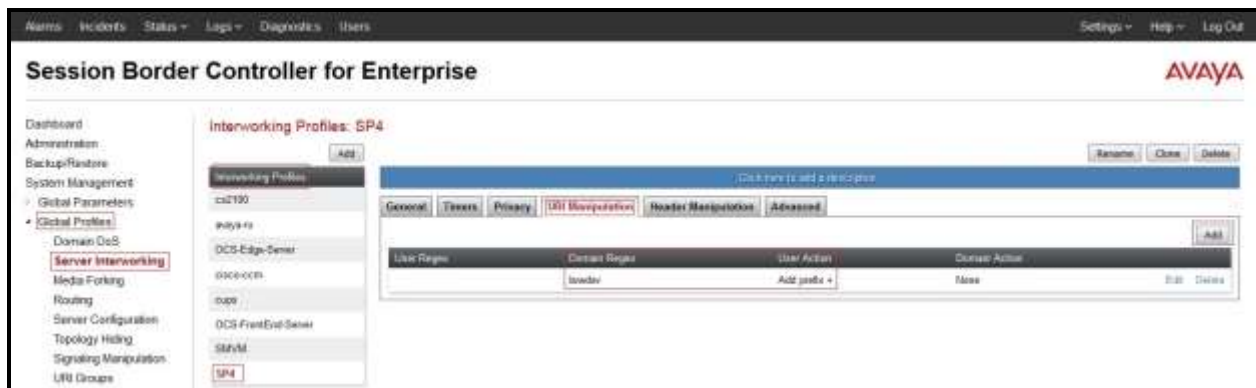


Figure 48: Server Interworking – IntelPeer CoreCloud SIP Trunk site - URI Manipulation

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 screenshot on the next page to perform the following:
 - Remove user of SIP URI in Request-Line header of the SIP OPTIONS coming from IntelPeer.
 - Click **Save** (not shown).

Note: See **Appendix B** in **Section 13** for the reference of this sigma script.

On the **Advanced** tab:

- Select **SMVM** for **Interworking Profile** (see Section 7.2.1).
- Click **Finish** (not shown).

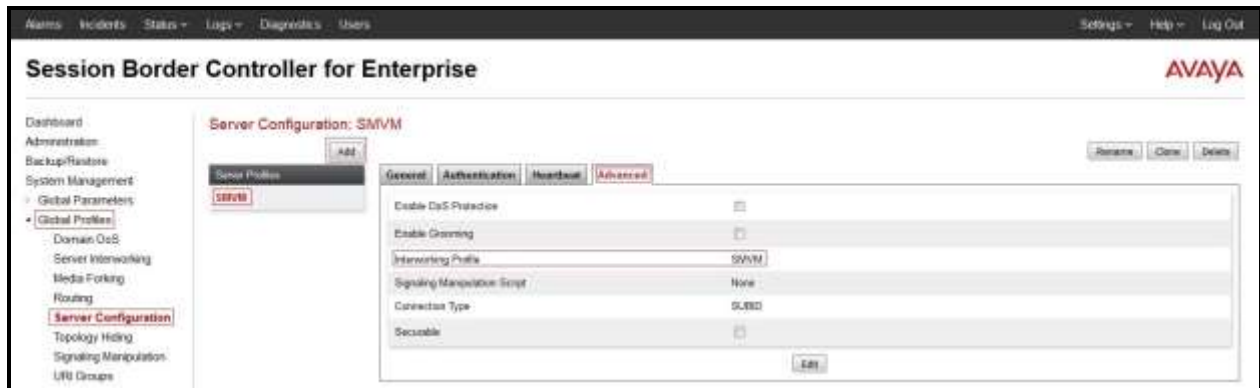


Figure 51: Server Configuration – Advanced - Avaya site

7.2.5. Configure Server – IntelPeer CoreCloud 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**: **192.168.115.117** (IntelPeer CoreCloud SIP Trunk Signaling Server IP Address).
- **Port**: **5060**.
- **Transport**: **UDP**.
- Click **Finish** (not shown).



Figure 52: Server Configuration – General - IntelPeer site

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

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

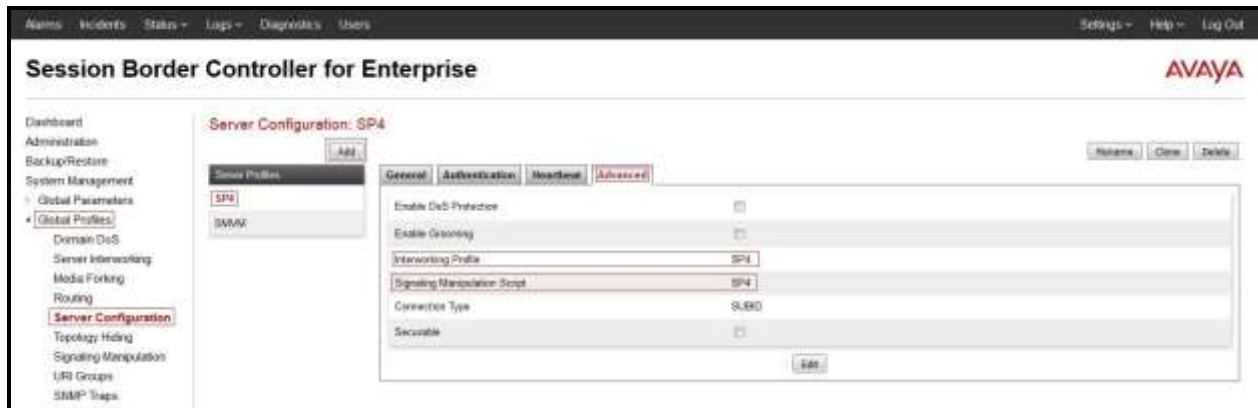


Figure 53: Server Configuration – Advanced - IntelPeer site

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: 10.33.10.43:5060 (UDP)** (Avaya Aura® Session Manager IP address).
- Click **Finish**.

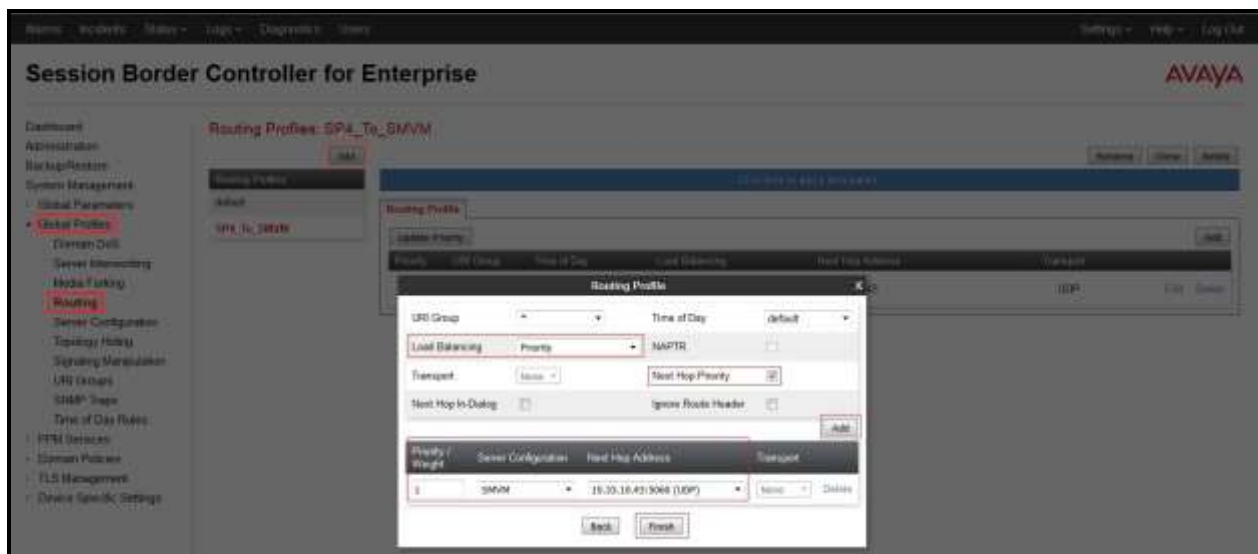


Figure 54: Routing to Session Manager

7.2.7. Configure Routing – IntelPeer CoreCloud 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: 192.168.115.117:5060 (UDP)** (IntelPeer CoreCloud Signaling Server IP address).
- Click **Finish.**

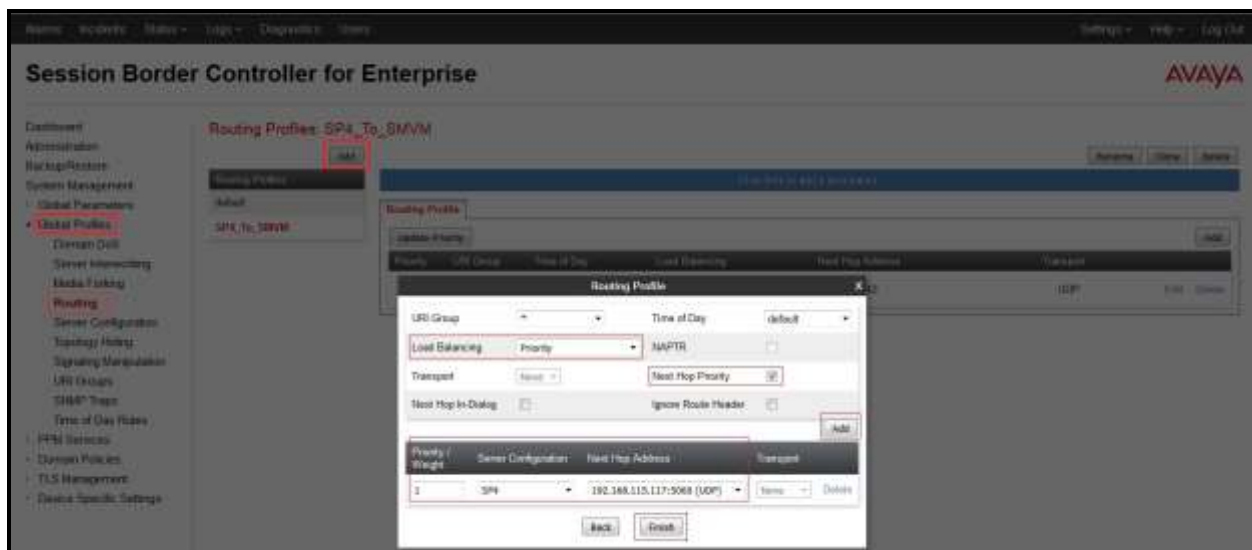


Figure 55: Routing to IntelPeer CoreCloud SIP Trunk

7.2.8. Configure Topology Hiding – Avaya site

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

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

Select **Add** button to enter **Profile Name: SP4_To_SMVM**.

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

Click **Finish** (not shown).

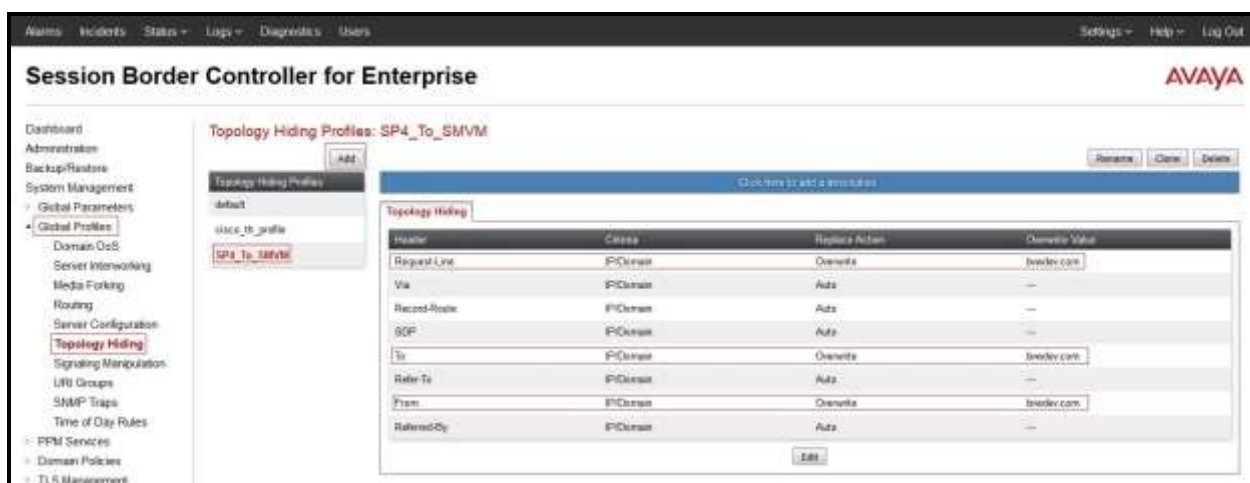


Figure 56: Topology Hiding Session Manager

7.2.9. Configure Topology Hiding – IntelPeer CoreCloud SIP Trunk site

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

Select **Add** button to enter **Profile Name: SMVM_To_SP4**.

- For the Header **Request-Line**,
 - In the **Criteria** column select **IP/Domain**
 - In the **Replace Action** column select: **Overwrite**
 - In the **Overwrite Value** column: **192.168.115.117**
- For the Header **To**,
 - In the **Criteria** column select **IP/Domain**
 - In the **Replace Action** column select: **Overwrite**
 - In the **Overwrite Value** column: **192.168.115.117**
- For the Header **From**,
 - In the **Criteria** column select **IP/Domain**
 - In the **Replace Action** column select: **Overwrite**
 - In the **Overwrite Value** column: **192.168.115.117**

Click **Finish** (not shown).

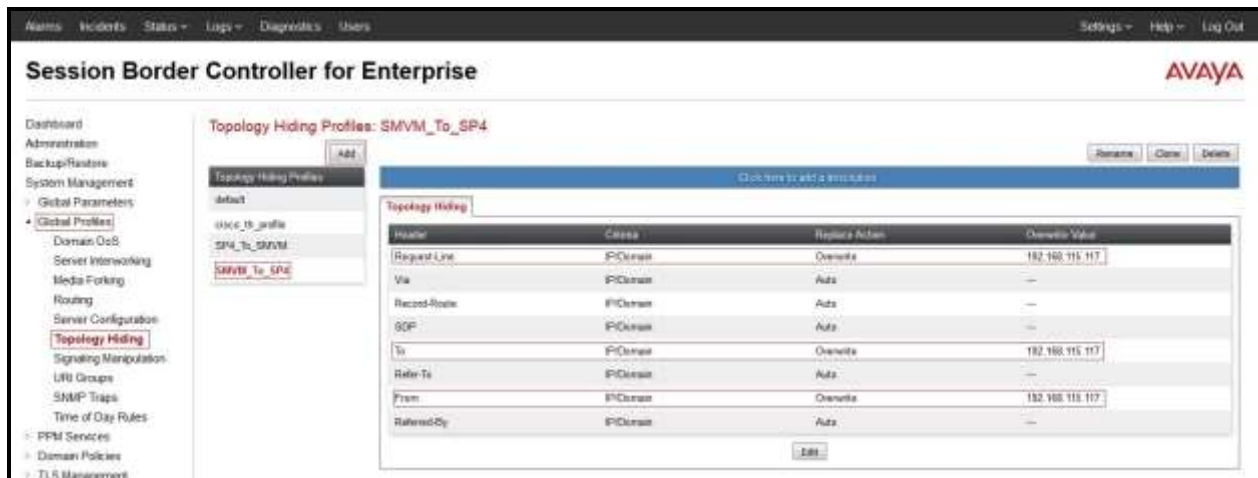


Figure 57: Topology Hiding IntelPeer CoreCloud SIP Trunk

7.3. 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, security, signaling, and ToD, each of which was created using the procedures contained in the previous sections.) A Policy Group is comprised of one or more Policy Sets. The purpose of Policy Sets and Policy Groups is to increasingly aggregate and simplify the application of 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_PolicyG**.
 - **Application Rule: default.**
 - **Border Rule: default.**
 - **Media Rule: default-low-med.**
 - **Security Rule: default-med.**
 - **Signaling Rule: default.**
 - **Time of Day: default.**
- Select **Finish** (not shown).



Figure 58: Endpoint Policy – Avaya site

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

- Select **Add**.
- Enter **Group Name: SP4_PolicyG**.
 - **Application Rule: default.**
 - **Border Rule: default.**
 - **Media Rule: default-low-med.**
 - **Security Rule: default-med.**
 - **Signaling Rule: default.**
 - **Time of Day: default.**
- Select **Finish** (not shown).

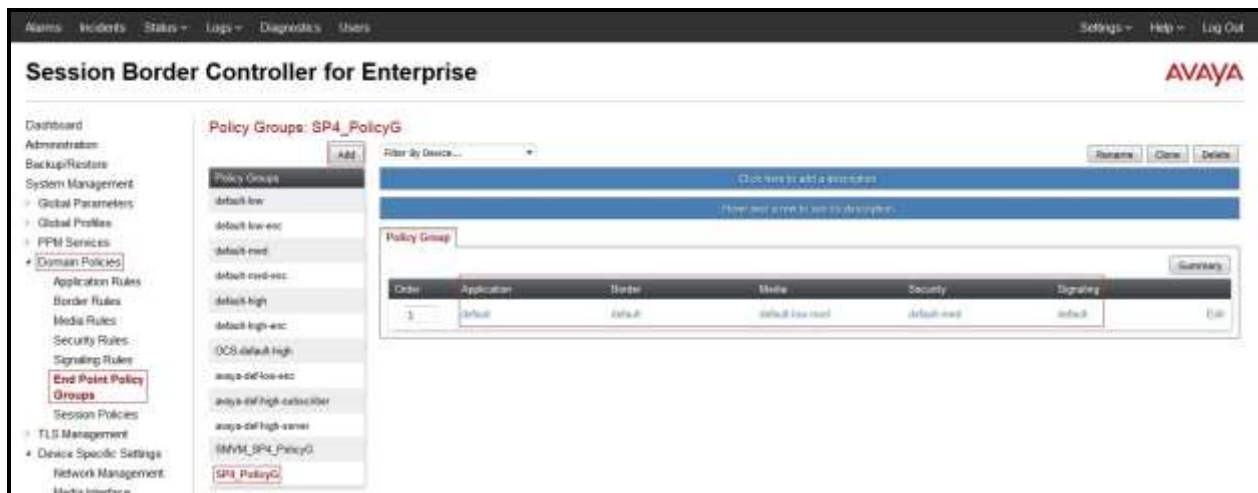


Figure 59: Endpoint Policy – IntelPeer CoreCloud SIP Trunk site

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

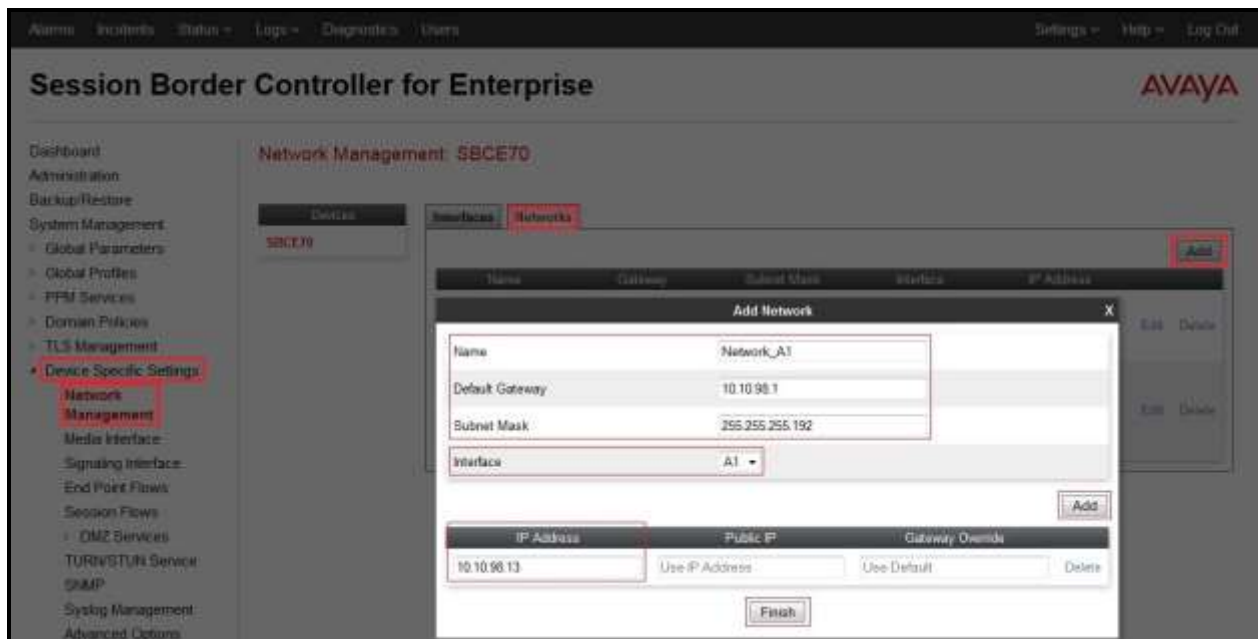


Figure 60: Network Management – Inside Interface

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 of outside interface as followings:
 - **Name: Network_B1.**
 - **Default Gateway: 10.10.98.97.**
 - **Subnet Mask: 255.255.255.224.**
 - **Interface: B1** (This is Avaya SBCE outside interface).
 - Click **Add** button to add **IP Address** for outside interface: **10.10.98.111.**
 - Click **Finish** button to save the changes.

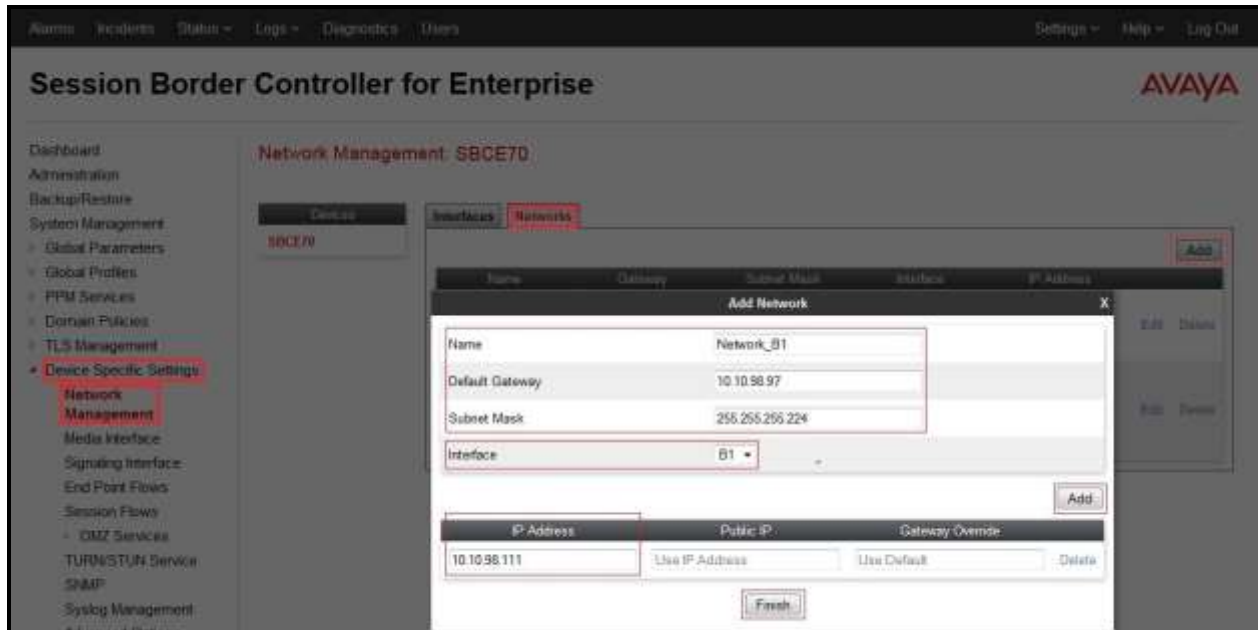


Figure 61: Network Management – Outside Interface

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

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



Figure 62: Network Management – Interface Status

7.4.2. Create Media Interfaces

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

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

- Select **Add** button and enter the following:
 - **Name:** **InsideMedia1**.
 - **IP Address:** Select **Network_A1 (A1,VLAN0)** and **10.10.98.13** (Internal IP Address toward Avaya Aura® Session Manager).
 - **Port Range:** **35000 – 40000**.
 - Click **Finish** (not shown).
- Select **Add** button and enter the following:
 - **Name:** **OutsideMedia1**.
 - **IP Address:** Select **Network_B1 (B1,VLAN0)** and **10.10.98.111** (External IP Address toward IntelPeer CoreCloud SIP Trunk).
 - **Port Range:** **35000 – 40000**.
 - Click **Finish** (not shown).



Figure 63: Media Interface

7.4.3. Create Signaling Interfaces

Signaling Interfaces define the type of signaling on the ports.

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

- Select **Add** button and enter the following:
 - **Name:** **InsideUDP1**.
 - **IP Address:** Select **Network_A1 (A1,VLAN0)** and **10.10.98.13** (Internal IP Address toward Avaya Aura® Session Manager).
 - **UDP Port:** **5060**.
 - Click **Finish** (not shown).

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

- Select **Add** button and enter the following:
 - **Name:** **OutsideUDP1**.
 - **IP Address:** Select **Network_B1 (B1,VLAN0)** and **10.10.98.111** (External IP Address toward IntelPeer CoreCloud SIP trunk).
 - **UDP Port:** **5060**.
 - Click **Finish** (not shown).

Note: For the internal interface, the Avaya SBCE was configured to listen for UDP on port 5060. For the external interface, the Avaya SBCE was configured to listen for UDP on port 5060 as same as IntelPeer CoreCloud SIP Trunk used.



Figure 64: Signaling Interface

7.4.4. Configuration Server Flows

Server Flows allow an administrator to categorize trunk-side signaling and to 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: OutsideUDP1** (see Section 7.4.3).
 - **Signaling Interface: InsideUDP1** (see Section 7.4.3).
 - **Media Interface: InsideMedia1** (see Section 7.4.2).
 - **End Point Policy Group: SMVM_SP4_PolicyG** (see Section 7.3).
 - **Routing Profile: SMVM_To_SP4** (see Section 7.2.7).
 - **Topology Hiding Profile: SP4_To_SMVM** (see Section 7.2.8).
 - Click **Finish**.

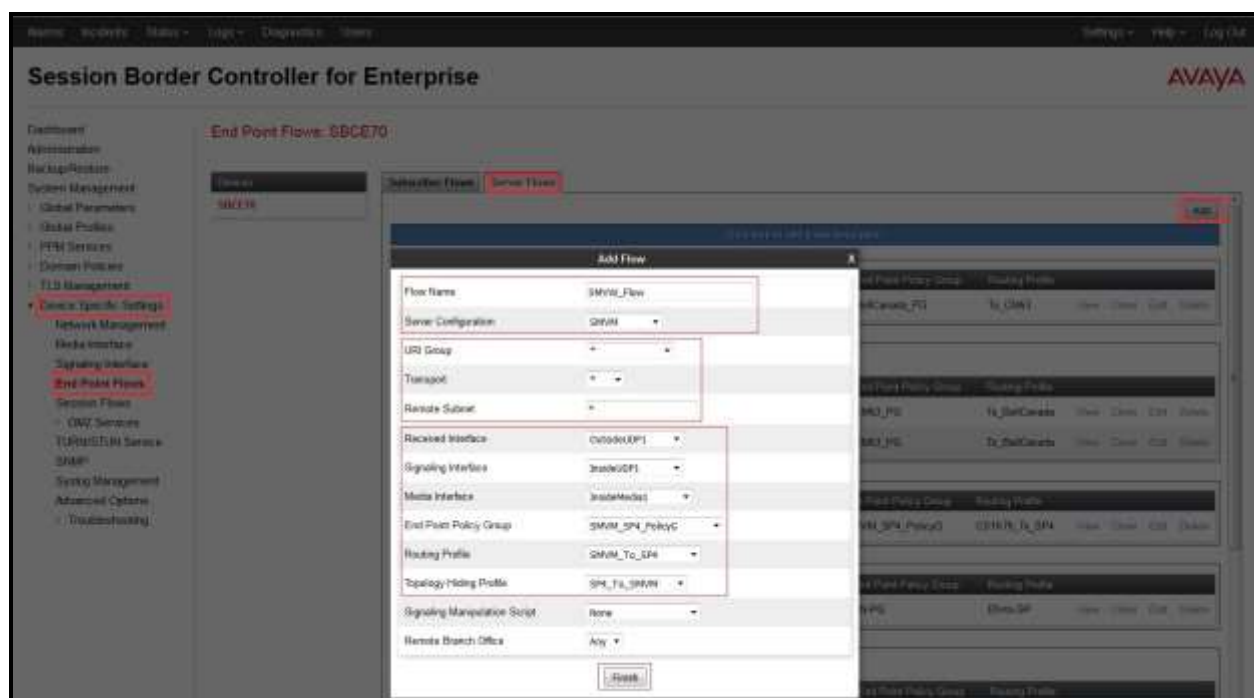


Figure 65: End Point Flow to IntelPeer CoreCloud SIP Trunk

7.4.4.2 Create End Point Flows – IntelPeer CoreCloud 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: InsideUDP1** (see Section 7.4.3).
 - **Signaling Interface: OutsideUDP1** (see Section 7.4.3).
 - **Media Interface: OutsideMedia1** (see Section 7.4.2).
 - **End Point Policy Group: SP4_PolicyG** (see Section 7.3).
 - **Routing Profile: SP4_To_SMVM** (see Section 7.2.6).
 - **Topology Hiding Profile: SMVM_To_SP4** (see Section 7.2.9).
 - Click **Finish**.

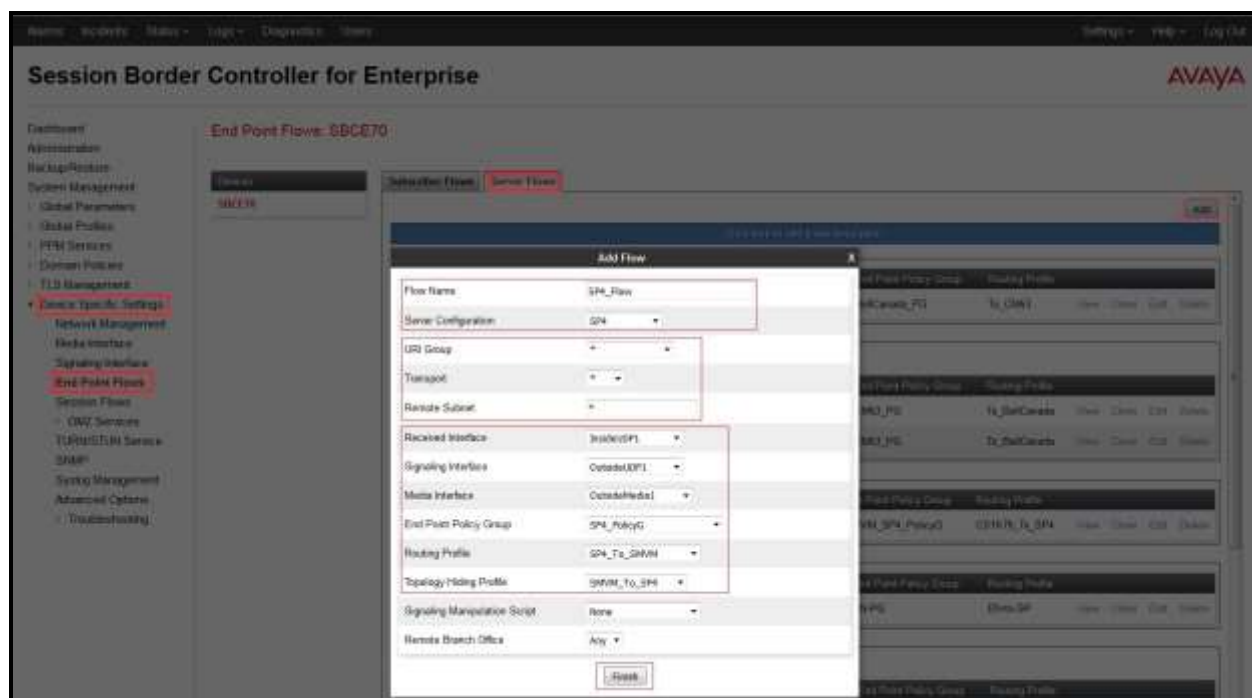


Figure 66: End Point Flow from IntelPeer CoreCloud SIP Trunk

8. IntelPeer CoreCloud SIP Trunk Configuration

IntelPeer CoreCloud SIP Trunk is responsible for the network configuration of the IntelPeer CoreCloud SIP Trunk service. IntelPeer CoreCloud SIP Trunk will require customer to provide the public IP address used to reach the Avaya SBCE public interface at the edge of the enterprise. IntelPeer CoreCloud SIP Trunk will provide the IP address of the IntelPeer CoreCloud SIP Trunk SIP proxy/SBC, IP addresses of media sources and Direct Inward Dialed

(DID) numbers assigned to the enterprise. IntelPeer CoreCloud SIP Trunk also provides the IntelPeer 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 IntelPeer CoreCloud SIP Trunk and the enterprise is a static IP configuration.

9. Verification Steps

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

Troubleshooting:

1. Enter the following commands using Communication Manager System Access Terminal (SAT) interface:
 - **list trace station** <extension number> - Traces calls to and from a specific station.
 - **list trace tac** <trunk access code number> - Trace calls over a specific trunk group.
 - **status station** <extension number> - Displays signaling and media information for an active call on a specific station.
 - **status trunk-group** <trunk-group number> - Displays trunk-group state information.
 - **status signaling-group** <signaling-group number> - Displays signaling-group state information.
2. Session Manager:
 - **Call Routing Test** - The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, navigate to **Elements → Session Manager → System Tools → Call Routing Test**. Enter the requested data to run the test.
 - **traceSM -x** – Session Manager command line tool for traffic analysis. Log into the Session Manager management interface to run this command.
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.
 - **Command Line Interface: /tmp/traceSBC.** The tool updates the database directly based on which trace mode is selected.
 - The first option is recommended when traceSBC is used off-line. These debugs can be enabled by the customers through the GUI, they can send the log files, and traceSBC can parse them off-line.
 - The second option is recommended for live captures. When the tool starts, it checks the database to see if debug logging is already enabled. If yes, the tool automatically starts processing the files.

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 IntelPeer CoreCloud SIP Trunk. This solution successfully passed compliance testing via the Avaya DevConnect Program. Please refer to **Section 2.2** for any exceptions or workarounds.

11. References

This section references the documentation relevant to these Application Notes.

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

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

Avaya Aura[®] Session Manager/System Manager

- [1] *Administering Avaya Aura[®] Session Manager*, Release 7.0, Issue 1, August 2015
- [2] *Administering Avaya Aura[®] System Manager*, Release 7.0, Issue 1, August 2015

Avaya Aura[®] Communication Manager

- [3] *Avaya Aura[®] Communication Manager Product Description*, Document ID 03-300468, Release 7.0, Issue 1, August 2015

Avaya Phones

- [4] *Avaya one-X[®] Deskphone SIP 9621G/9641G User Guide for 9600 Series IP Telephones*, Document ID 16-603596, Issue 1, August 2012
- [5] *Avaya one-X[®] Communicator Overview and Planning*, Release 6.2 FP6, April 2015
- [6] *Administering Avaya Communicator for Android, iPad, and Windows*, Release 2.1, Issue 4, August 2014

Avaya Aura[®] Messaging

- [7] *Administering Avaya Aura[®] Messaging 6.3*, Issue 3, August 2014

Avaya Session Border Controller for Enterprise

[8] *Avaya Session Border Controller for Enterprise Overview and Specification*, Release 7.0 Issue 1, August 2015

[9] *Administering Avaya Session Border Controller for Enterprise*, Release 7.0, Issue 1, August 2015

IETF (Internet Engineering Task Force) SIP Standard Specifications

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

[11] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>

Product documentation for IntelPeer CoreCloud SIP Trunk SIP Trunk may be found at:
<http://www.intelepeer.com/SIPTrunking>.

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 IntelPeer CoreCloud 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 Communicator for Windows SIP softphone. Avaya 96x1 SIP Deskphones support SRTP, while Avaya one-X[®] Communicator and Avaya Communicator for Windows softphones support RTP.

Note: In this compliance testing, only Avaya Communicator for Windows 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.

The figure below illustrates the Remote Worker topology used in the reference configuration.

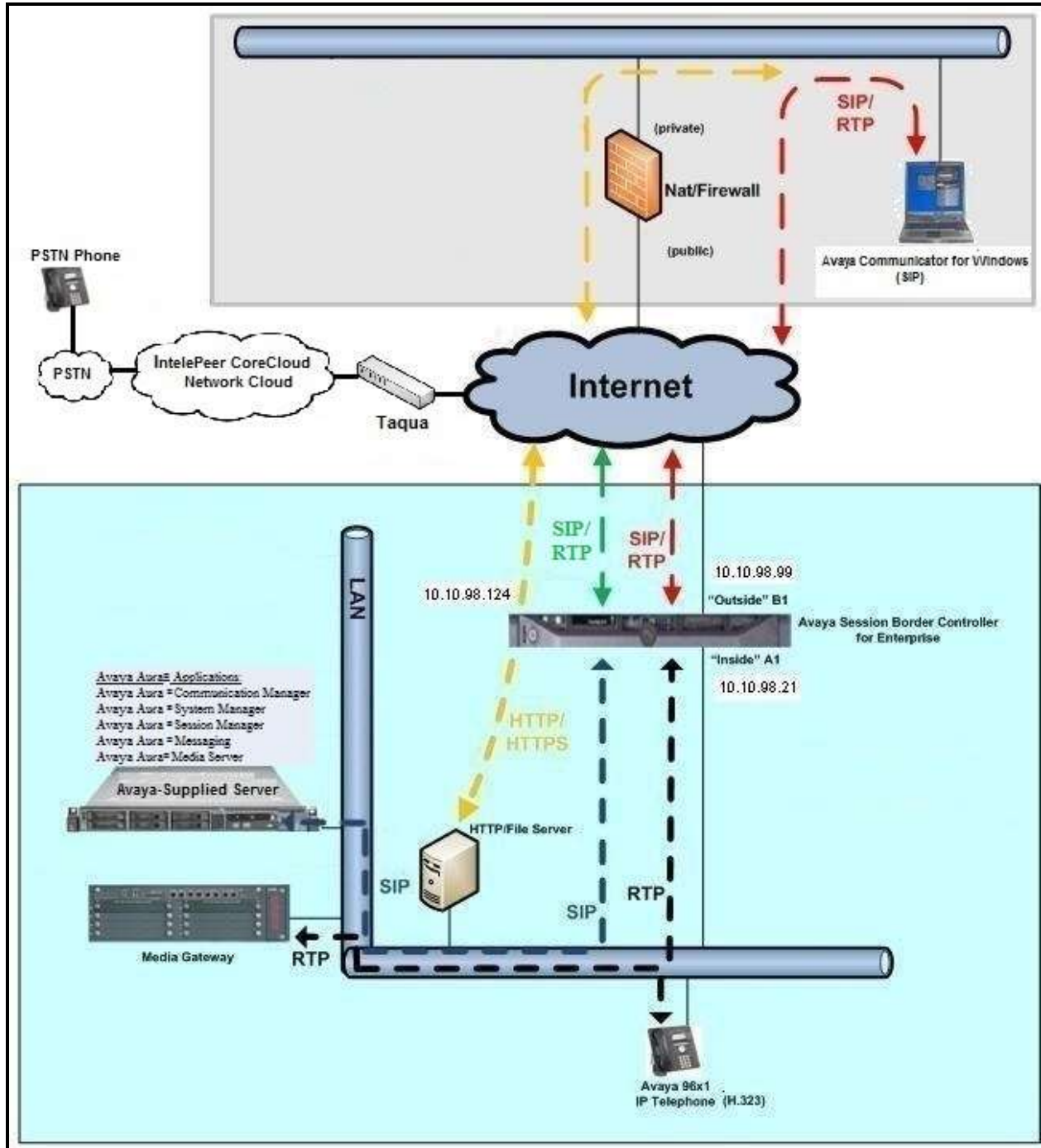


Figure 67: Avaya IP Telephony Network for Remote Worker

12.1. Network Management on Avaya SBCE

The following screen shows the **Network Management** of the Avaya SBCE. The Avaya SBCE is configured with three “outside” IP addresses assigned to physical interface B1, and two “inside” 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” address previously provisioned for SIP Trunking with IntelPeer CoreCloud SIP Trunk (see **Section 7.4.1**).
- **10.10.98.21** is the new Avaya SBCE “inside” address for Remote Worker access to Session Manager.
- **10.10.98.111** is the Avaya SBCE “outside” address previously provisioned for SIP Trunk with IntelPeer CoreCloud SIP Trunk (see **Section 7.4.1**).
- **10.10.98.99** is the new Avaya SBCE “outside” address for Remote Worker access to Session Border Controller.
- **10.10.98.124** is the new Avaya SBCE “outside” address for file transfer access between the Remote Worker phone and the enterprise file server.

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.

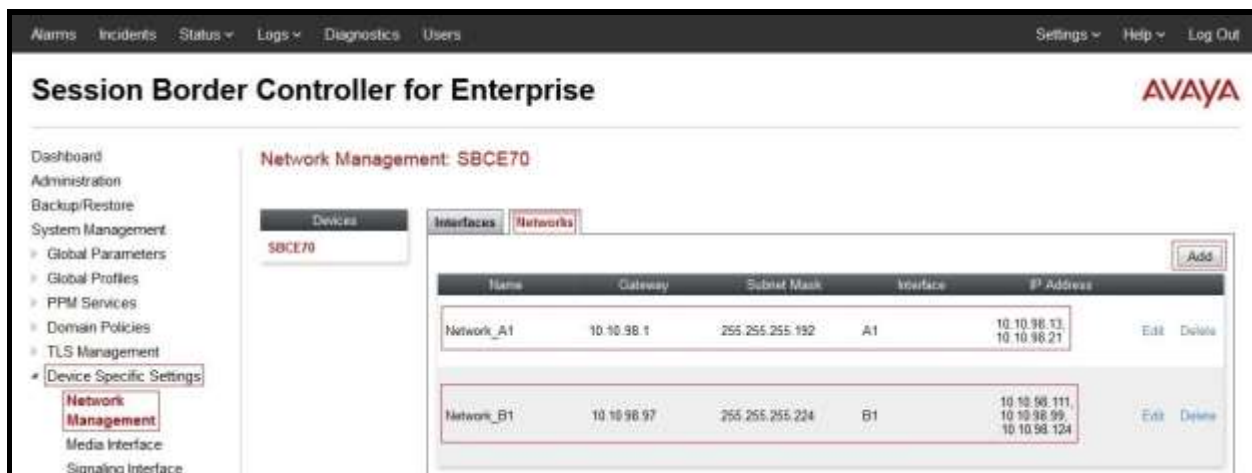


Figure 68: Network Management

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



Figure 69: 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 **Add** button and enter the following:
 - **Name:** **InsideMediaRW**.
 - **IP Address:** Select **Network_A1 (A1, VLAN0)** and **10.10.98.21** (Internal IP Address toward Session Manager).
 - **Port Range:** **35000 – 40000**.
 - Click **Finish** (not shown).
- Select **Add** button and enter the following:
 - **Name:** **OutsideMediaRW**.
 - **IP Address:** Select **Network_B1 (B1, VLAN0)** and **10.10.98.99** (External IP Address toward Remote Worker phones).
 - **Port Range:** **35000 – 40000**.
 - Click **Finish** (not shown).

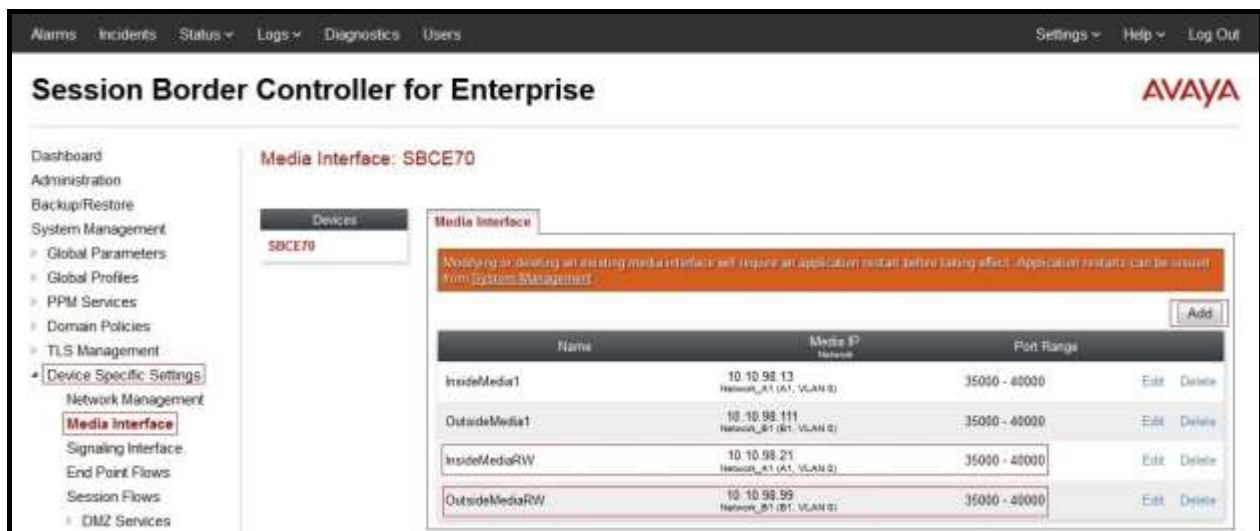


Figure 70: Media Interface

Note: Media Interface **OutsideMediaRW** is used in the Remote Worker Subscriber Flow (Section 12.13.1), and Media Interface **InsideMediaRW** is used in the Remote Worker Server Flow (Section 12.13.2.1).

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 **InsideSIPRW** using the parameters:

- **IP Address:** Select **Network_A1 (A1, VLAN0)** and **10.10.98.21** (Internal IP Address toward Session Manager).
- **TCP Port: 5060.**
- Click on **Finish** (not shown).

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

- **IP Address:** Select **Network_B1 (B1, VLAN0)** and **10.10.98.99** (External IP Address toward Remote Worker phones).
- **TCP Port: 5060.**
- Click on **Finish** (not shown).

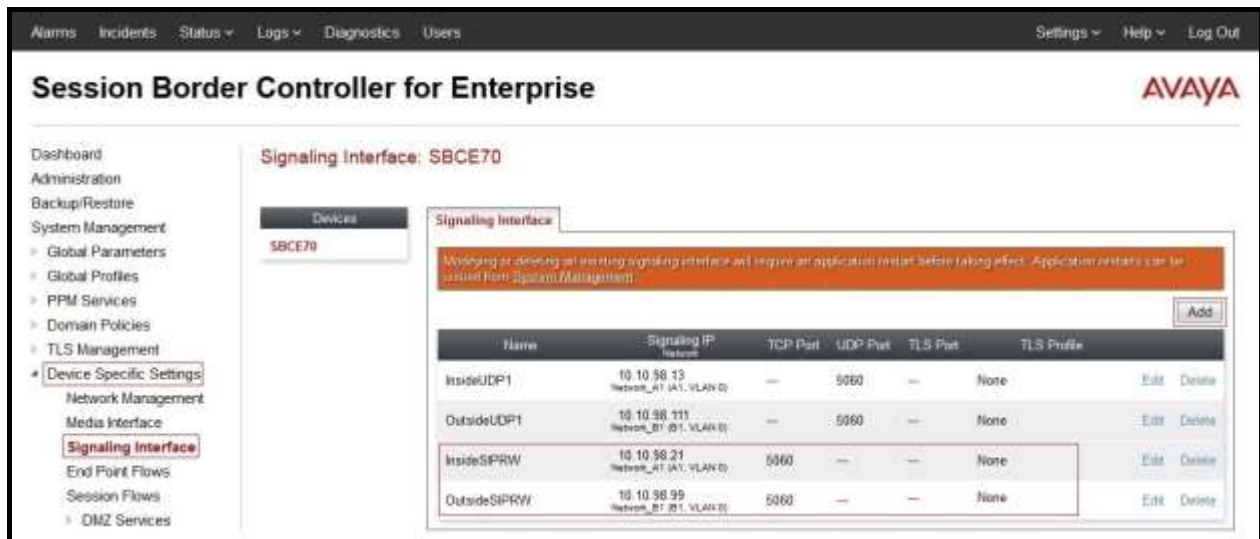


Figure 71: Signaling Interface

Note: Signaling Interface **OutsideSIPRW** is used in the Subscriber Flows (Section 12.13.1), and in the Remote Worker Server Flow (Section 12.13.2.1). Signaling Interface **InsideSIPRW** is used in the Remote Worker Server Flow (Section 12.13.2.1).

12.4. Server Interworking Configuration on Avaya SBCE

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

- Select **Interworking Profiles** as **SMVM**.
- On the **Advanced** tab, click **Edit** button, verify that **Extensions** should be **Avaya**.
- Click **Finish** (not shown).

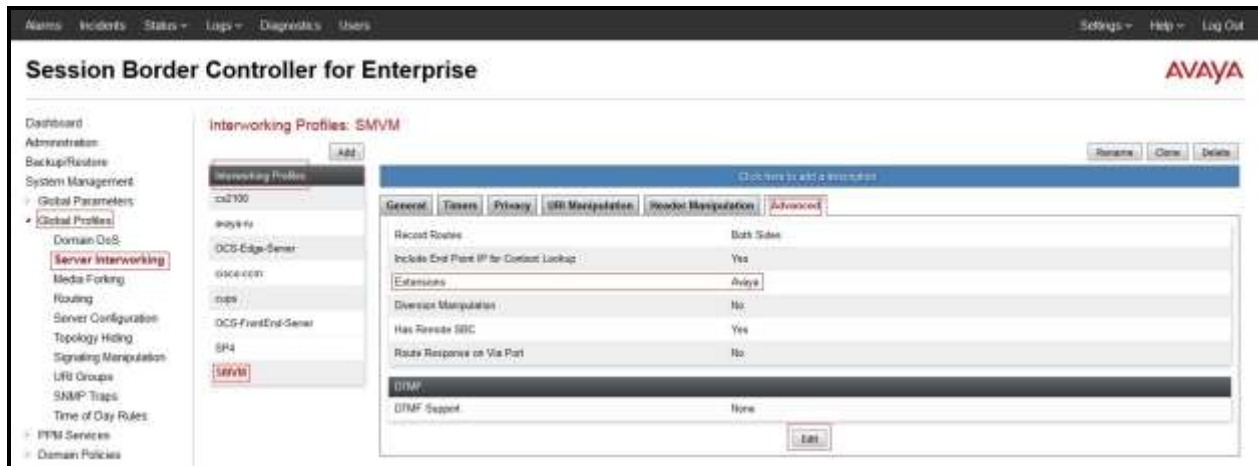


Figure 72: Server Interworking for Remote Worker

12.5. Server Configuration on Avaya SBCE

Note: 10.33.10.43 is the IP address of Session Manager in the reference configuration (see Section 7.2.4).

The following screens show the **Server Configuration** for the Profile **SMVM** created previously for SIP Trunking with IntelPeer CoreCloud SIP Trunk in **Section 7.2.4** for Session Manager. The configuration includes TCP (5060) transport protocol which is used for the Remote Worker configuration.

From the menu on the left-hand side, select **Global Profiles → Server Configuration**. Select **Server Profiles** as **SMVM** to edit the existing Server Configuration SMVM.

- On the **General** tab, click **Edit** button to add the following:
- **IP Address/FQDN:** 10.33.10.43 (Avaya Aura® Session Manager IP Address).
- **Port:** 5060.
- **Transport:** TCP.
- Click **Finish** (not shown).



Figure 73: Server Configuration for Remote Worker

Note: This Server Configuration is used by the Routing Profile defined in **Section 12.6** and the Server Flows defined in **Section 12.13.2.2**.

- On the Advance tab, click **Edit** button to modify the following:
- **Enable Grooming** box is checked.
- Click **Finish** (not shown).

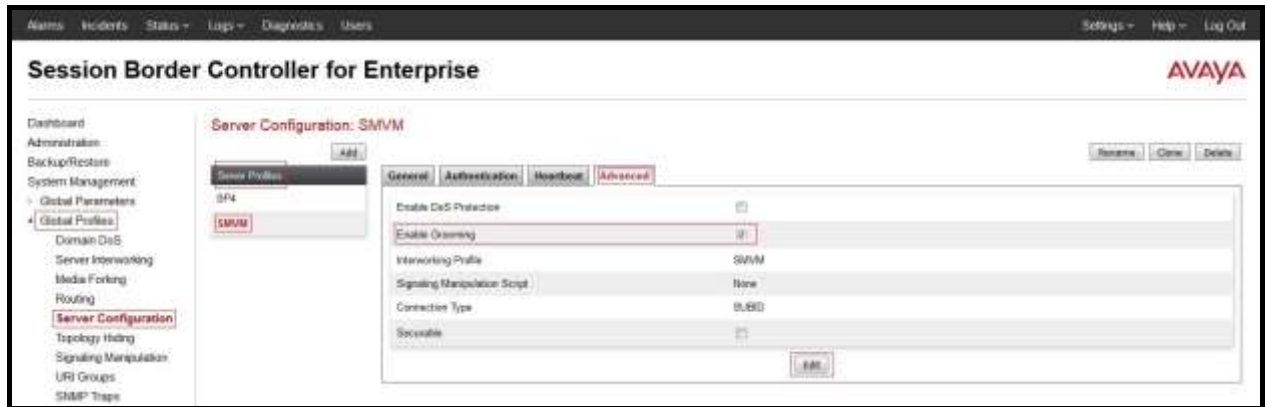


Figure 74: Server Configuration – Advanced for Remote Worker

12.6. Routing Profile on Avaya SBCE

The Routing Profile **To_SMVM_RW** is created for access to Session Manager.

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** (see Section 12.5).
- **Next Hop Address: 10.33.10.43:5060 (TCP)** (IP address of Session Manager).
- Click **Finish.**

The Routing Profile **To_SMVM_RW** is used in the Subscriber Flows (Section 12.13.1).

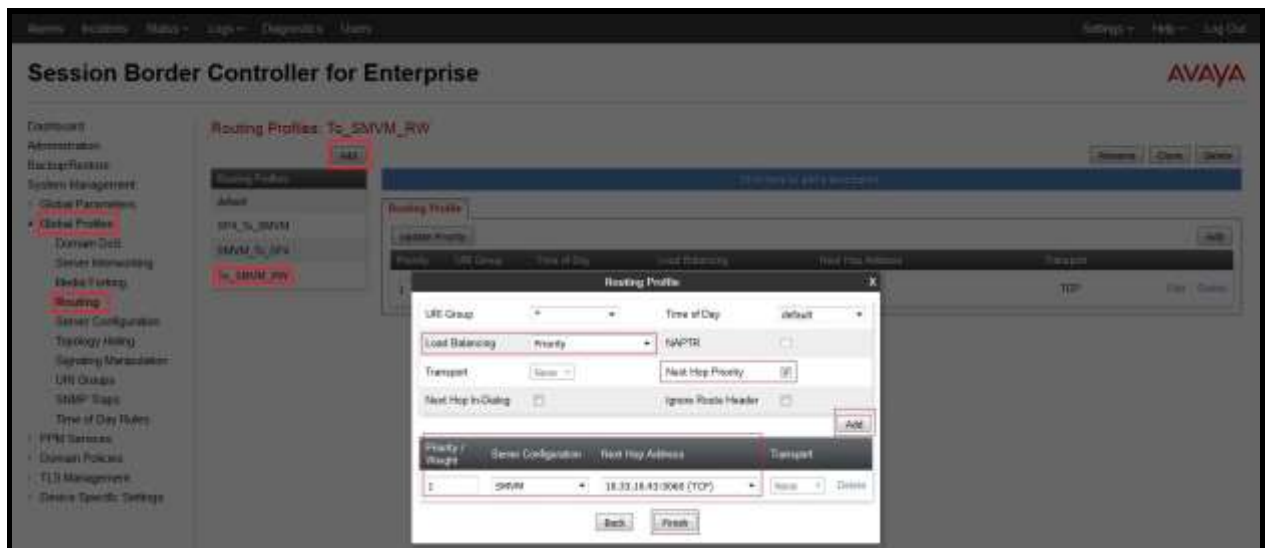


Figure 75: Remote Worker Routing to SM

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 12.13.2.1**.

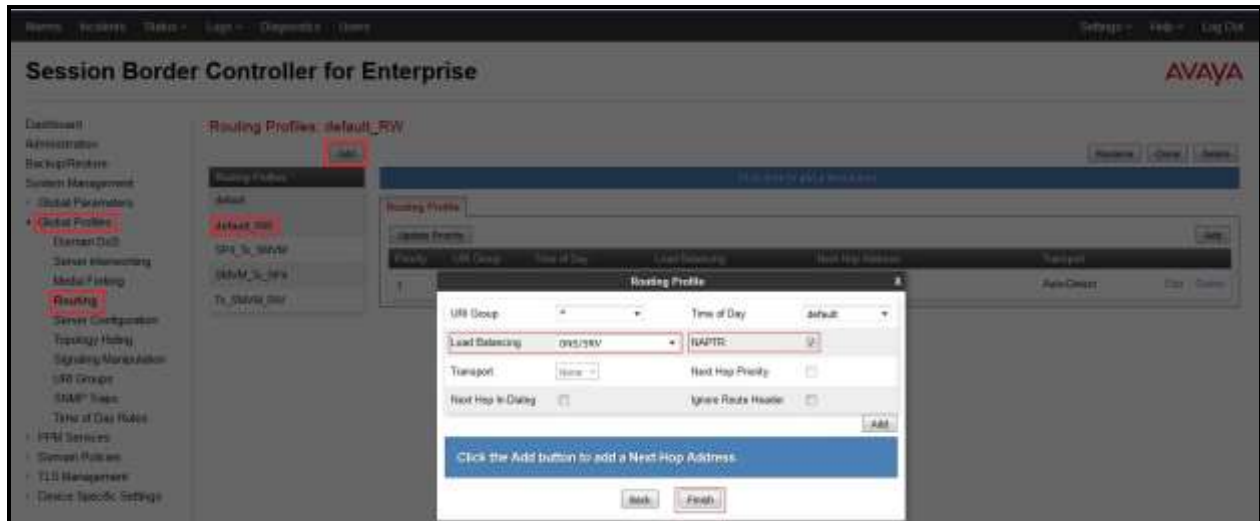


Figure 76: Remote Worker Default Routing

12.7. User Agent on Avaya SBCE

User Agents are created for each type of endpoints tested. In this compliance testing, Avaya Communicator for Windows will be 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: Avaya Communicator**.
- Enter **Regular Expression: Avaya Flare.***.
- Click on **Finish** (not shown).



Figure 77: User Agents for Remote Worker

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

```
INVITE sip: 61613XXX5206@bvwddev.com SIP/2.0
From: sip:0326@bvwddev.com;tag=-59f03c7f529fb7c152aa3fd4_F0950710.10.98.136
To: sip: 61613XXX5206@bvwddev.com
CSeq: 24 INVITE
Call-ID: 18_a7e80-49279ea452aa365c_I@10.33.5.58
Contact: <sip:0326@10.10.98.21:5060;transport=tcp;subid_ipcs=592904751>
Record-Route: <sip:10.10.98.21:5060;ipcs-line=3472;lr;transport=tcp>
Record-Route: <sip:10.10.98.99:5060;ipcs-line=3472;lr;transport=tcp>
Allow:
INVITE,CANCEL,BYE,ACK,SUBSCRIBE,NOTIFY,MESSAGE,INFO,PUBLISH,REFER,UPDATE,PRACK
Supported: eventlist, 100rel, replaces
User-Agent: Avaya Flare Engine/ 2.0.0 (Engine GA-2.0.0.25; Windows NT 6.1, 64-bit)
Max-Forwards: 69
Via: SIP/2.0/TCP 10.10.98.21:5060;branch=z9hG4bK-s1632-001362762279-1--s1632-
Via: SIP/2.0/TCP 10.10.98.136:5060;branch=z9hG4bK18_a7e80-312c149e52aa3fe8_I09507
Accept-Language: en
Content-Type: application/sdp
Content-Length: 340
```

Figure 78: Output of trace for User Agent

Note: The User Agent is defined in its associated **Subscriber Flows** in **Section 12.13.1**.

12.8. Relay Services on Avaya SBCE

Relay Services are used to define how file transfers (e.g., phone firmware upgrades and configuration data), are routed to the Remote Worker endpoints. Both HTTP and HTTPS protocols are supported.

In the reference configuration, HTTP protocol is used for file exchanges between the Remote Worker phones and an HTTP file server located in the enterprise. For completeness, HTTP configuration is shown below.

From the menu on the left-hand side, select **Device Specific Settings → DMZ Services → Relay Services**

On the **Application Relay** tab, click on the **Add** button and enter the following:

- Set **Service Type: HTTP**.
- Set the **Remote IP/FQDN** to the IP address of the enterprise file server (e.g., **10.10.98.60**) used to provide the firmware updates and configuration data for the Remote Worker endpoints.
- Set the **Remote Port: 80**.
- Set the **Remote Transport: TCP**.
- Set **Listen IP** to the IP address of the Avaya SBCE's external IP address designated for file transfers (**Network_B1 (B1, VLAN 0)** and **10.10.98.124**).
- Set **Listen Port: 80**.
- Set the **Connect IP** to the internal IP address of the Avaya SBCE used for Remote Worker (**Network_A1 (A1, VLAN 0)** and **10.10.98.21**).
- Set **Listen Transport: TCP**.
- Click on **Finish**.

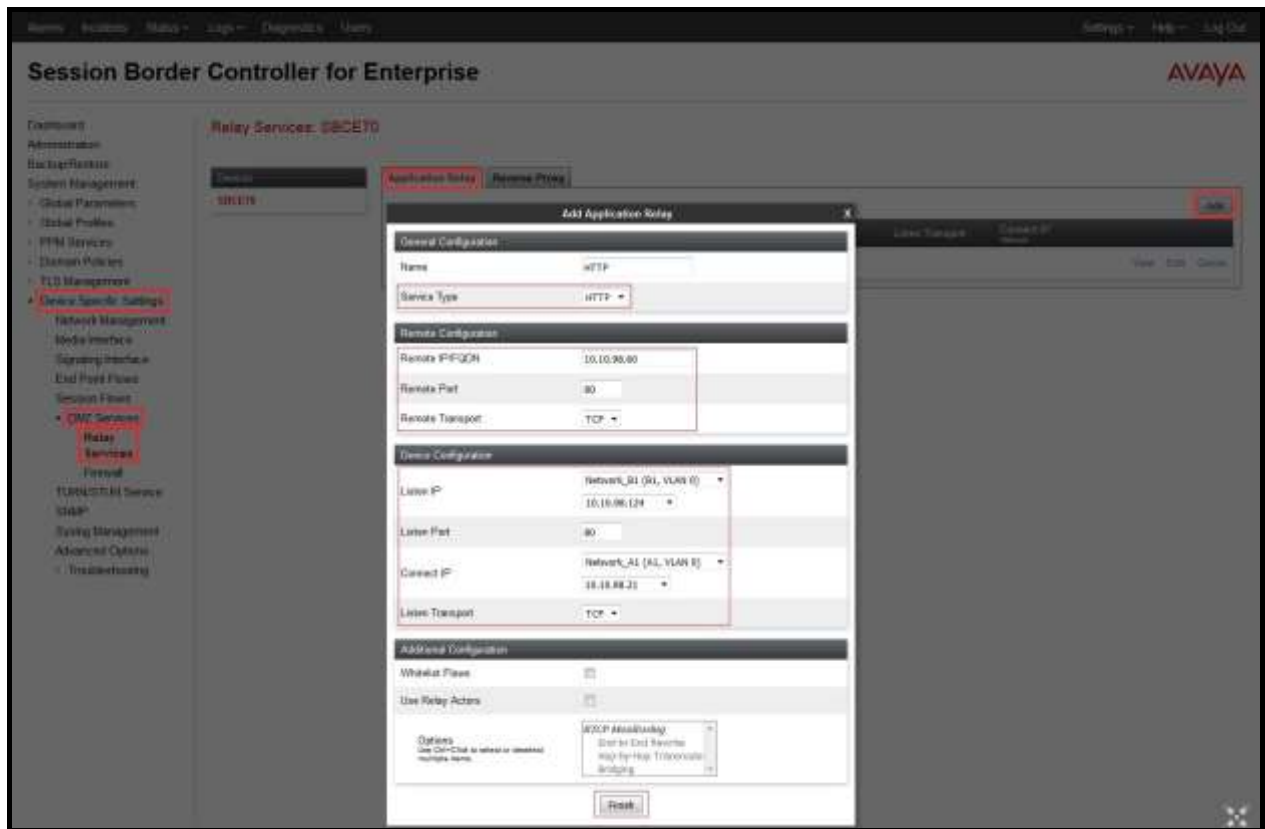


Figure 79: Relay Services Setup

12.9. Mapping Profiles on Avaya SBCE

A Mapping Profile is defined for Personal Profile Manager (PPM) data between the Remote Worker endpoints and Session Manager. The following screen shows the mapping profile **RW** created in the sample configuration. This enables the remote Avaya SIP endpoints to send and receive PPM information to and from Session Manager via the Avaya SBCE.

From the menu on the left-hand side, select **PPM Services → Mapping Profiles**

- Click on the **Add** button and enter the following:
- Enter **Profile Name** (e.g., **RW**), and click on **Next** (not shown).
- Select **Server Type: Session Manager**.
- In **Server Configuration** field, select **SMVM** from the drop down menu and in **Server Address** field, select **10.33.10.43:5060 (TCP)** from the drop down menu (see **Section 12.5**).
- Select **SBCE Device: SBCE70**.
- In **Signaling Interface** field, select **OutsideSIPRW (10.10.98.99)** from the drop down menu (see **Section 12.3**).
- In **Mapped Transport** field, select **TCP (5060)** from the drop down menu.
- Click **Finish**.

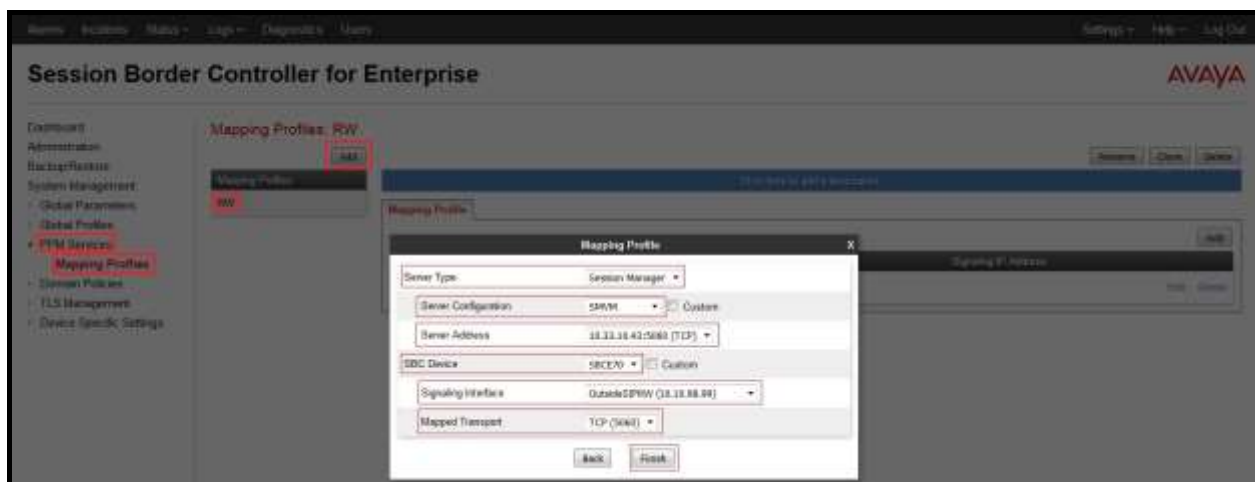


Figure 80: Mapping Profiles - PPM Services Setup

12.10. Application Rules on Avaya SBCE

The following section describes Application Rule **RemoteWorker_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., **RemoteWorker_AR**) and click **Finish** (not shown).
- Click on **RemoteWorker_AR** from **Application Rules**, then click **Edit** button:
- In the **Voice** 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).

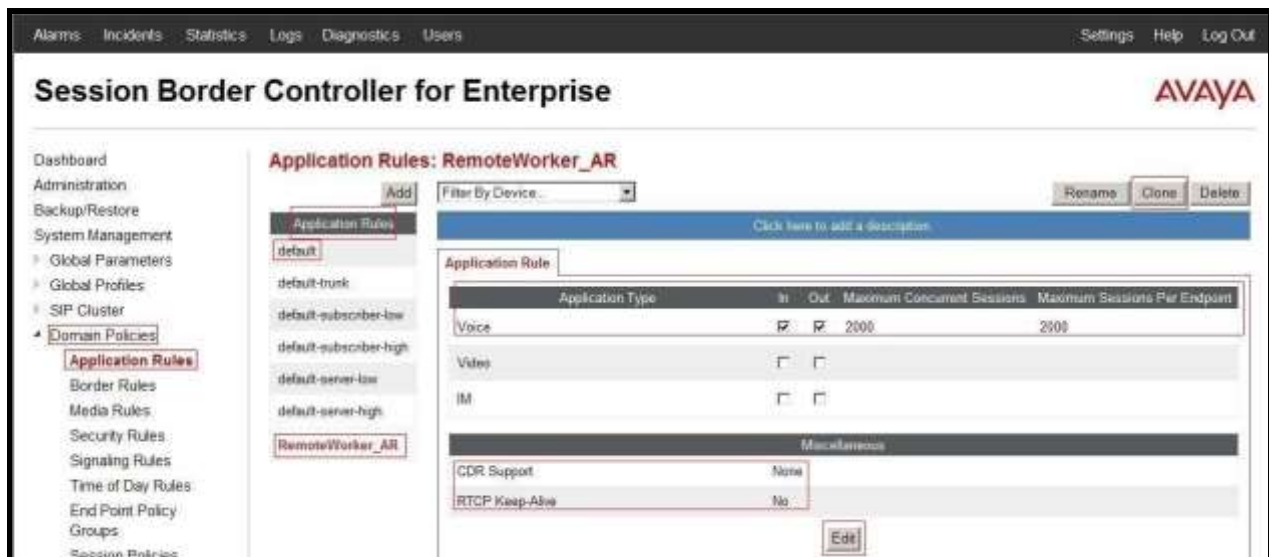


Figure 81: Remote Worker Application Rule

Note: The rule **RemoteWorker_AR** is assigned to the End Point Policy Groups in **Section 12.12**.

12.11. Media Rules on Avaya SBCE

The following section describes **Media Rule**: The existing rule **default-low-med** was used for the Remote Worker. Note that rule has **Interworking** in **Media Encryption** tab checked.

As described above the **default-low-med** rule was previously used and is shown here for completeness.



Figure 82: Default-Low-Med Media Rule

Note: The rule **default-low-med** is assigned to the End Point Policy Groups in **Section 12.12**.

12.12. End Point Policy Groups on Avaya SBCE

Two new End Point Policy Groups are defined for Remote Worker: **SMVM_RW**, and **RemoteUser_RTP**.

In addition, the End Point Policy Group **SP4_PolicyG** was previously created for SIP Trunking with IntelPeer CoreCloud SIP Trunk (see **Section 7.3**) and is shown here for completeness.

The End Point Policy Group **SP4_PolicyG** is used in the Server Flow defined in the **Section 12.13.2.2**.



Figure 83: IntelPeer CoreCloud SIP Trunk End Point Policy

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** = **RemoteWorker_AR** (Section 12.10).
 - **Border Rule** = **default**.
 - **Media Rule** = **default-low-med** (Section 12.11).
 - **Security Rule** = **default-low**.
 - **Signaling Rule** = **default**.
 - **Time of Day Rule** = **default**.
- Click on **Finish** (not shown).

The End Point Policy Group **SMVM_RW** is used in the Subscribe Flows **Flare** in **Section 12.13.1**.

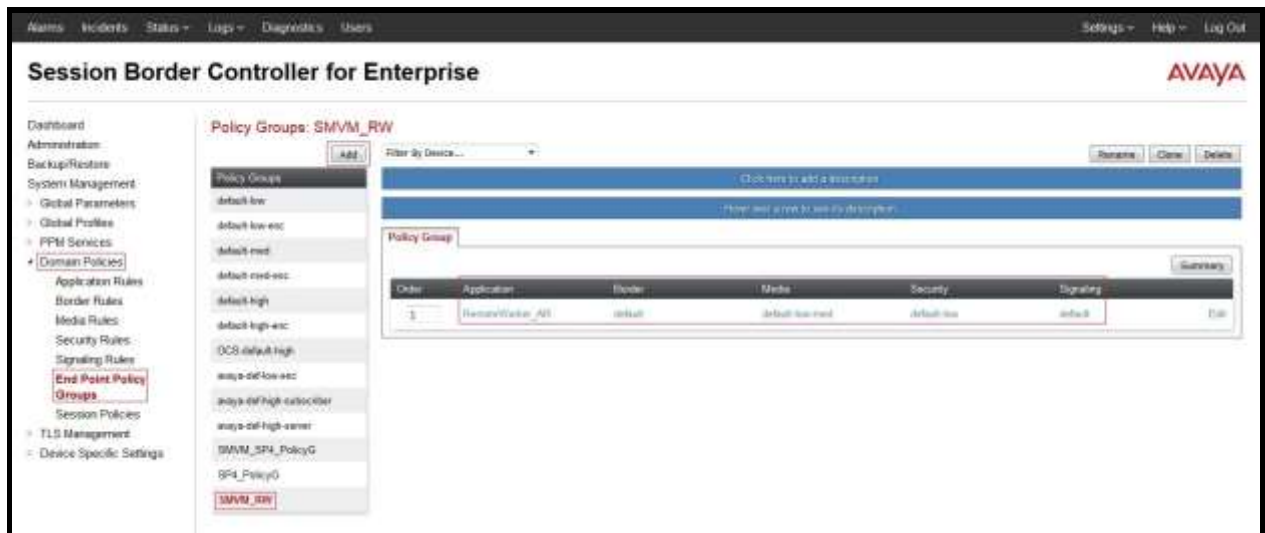


Figure 84: Remote Worker End Point Policy

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

- Enter a name (e.g., **RemoteUserRTP**), and click on **Next** (not shown).
- The **Policy Group** window will open. Enter the following:
 - **Application Rule** = **RemoteWorker_AR** (Section 12.10).
 - **Border Rule** = **default**.
 - **Media Rule** = **default_low_med** (Section 12.11).
 - **Security Rule** = **default-low**.
 - **Signaling Rule** = **default**.
 - **Time of Day Rule** = **default**.
- Click on **Finish** (not shown).

The End Point Policy Group **RemoteUserRTP** is used in the Server Flows **SMVM_RemoteWorker** defined in the **Section 12.13.2.1**.

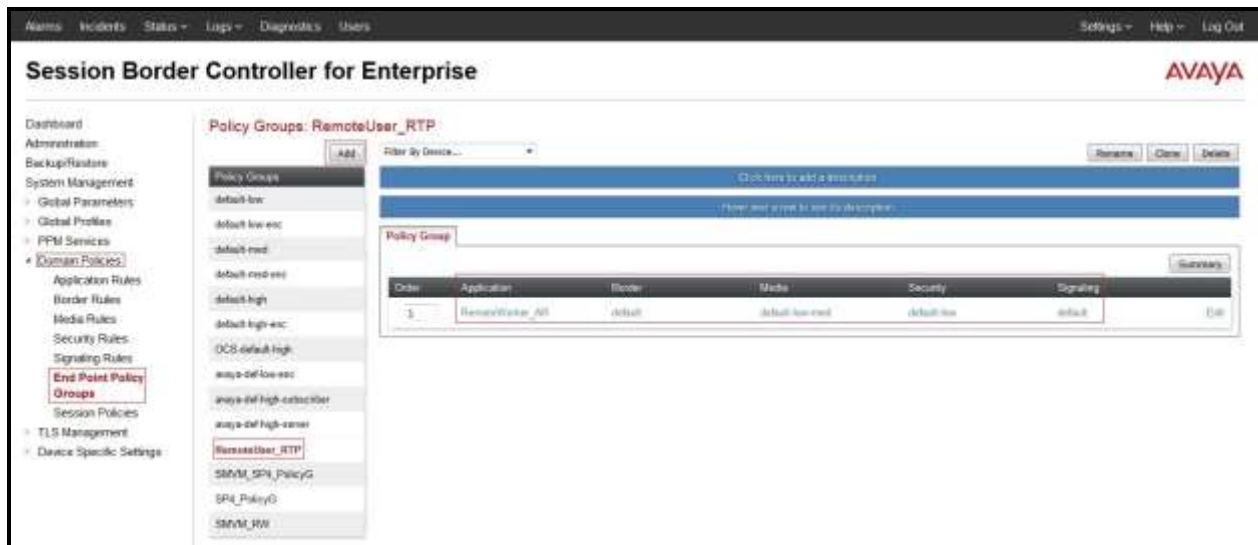


Figure 85: Remote Worker End Point Policy - RTP

12.13. End Point Flows on Avaya SBCE

12.13.1. Subscriber Flow

The **Subscriber Flow** is defined for Remote Workers associated with the **User Agent** previously created: **Avaya Communicator**.

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

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

- Enter a **Flow Name** (e.g., **Communicator**).
- **URI Group** = * (default).
- **User Agent** = **Avaya Communicator** (see **Section 12.7**).
- **Source Subnet** = * (default).
- **Via Host** = * (default).
- **Contact Host** = * (default).
- **Signaling Interface** = **OutsideSIPRW** (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.
- **User Agent** = **Avaya Communicator**.
- **Media Interface** = **OutsideMediaRW** (see **Section 12.2**).
- **End Point Policy Group** = **SMVM_RW** (see **Section 12.12**).
- **Routing Profile** = **To_SMVM_RW** (see **Section 12.6**).
- **Topology Hiding Profile** = **None**.

- **TLS Client Profile = None.**
- **RADIUS Profile = None.**
- **Signaling Manipulation Script = None.**

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



Figure 86: Remote Worker Subscriber Flows – Communicator 1

View Flow: Communicator

X

Criteria

Flow Name	Communicator
URI Group	*
User Agent	Avaya Communicator
Source Subnet	*
Via Host	*
Contact Host	*
Signaling Interface	OutsideSIPRW

Optional Settings

Topology Hiding Profile	None
TLS Client Profile	None
RADIUS Profile	None
Signaling Manipulation Script	None

Profile

Source	Subscriber
Methods Allowed Before REGISTER	
User Agent	Avaya Communicator
Media Interface	OutsideMediaRW
End Point Policy Group	SMVM_RW
Routing Profile	To_SMVM_RW
Presence Server Address	--

Figure 87: Remote Worker Subscriber Flows – Communicator 2

12.13.2. Server Flow on Avaya SBCE

The following screens show the new **Server Flow** settings for Remote Worker access to Session Manager. Two examples of Server Flows are defined for Remote Worker.

12.13.2.1 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 **Add** button (not shown) to enter the following:

- **Name** = **SMVM_RemoteWorker**.
- **Server Configuration** = **SMVM** (see Section 12.5).
- **URI Group** = * (default).
- **Transport** = * (default).
- **Remote Subnet** = * (default).
- **Received Interface** = **OutsideSIPRW** (see Section 12.3).
- **Signaling Interface** = **InsideSIPRW** (see Section 12.3).
- **Media Interface** = **InsideMediaRW** (see Section 12.2).
- **End Point Policy Group** = **RemoteUser_RTP** (see Section 12.12).
- **Routing Profile** = **default_RW** (see Section 12.6).
- **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		Profile		
Flow Name	SMVM_RemoteWorker	Signaling Interface	InsideSIPRW	
Server Configuration	SMVM	Media Interface	InsideMediaRW	
URI Group	*	End Point Policy Group	RemoteUser_RTP	
Transport	*	Routing Profile	default_RW	
Remote Subnet	*	Topology Hiding Profile	None	
Received Interface	OutsideSIPRW	Signaling Manipulation Script	None	
		Remote Branch Office	Any	

Figure 88: Remote Worker Server Flow

12.13.2.2 Trunking Server Flow on Avaya SBCE

The IntelPeer CoreCloud SIP Trunk Server Flow is defined in **Section 7.4.4.2** of this document.

View Flow: SP4_Flow			
Criteria		Profile	
Flow Name	SP4_Flow	Signaling Interface	OutsideUDP1
Server Configuration	SP4	Media Interface	OutsideMedia1
URI Group	*	End Point Policy Group	SP4_PolicyG
Transport	*	Routing Profile	SP4_To_SMVM
Remote Subnet	*	Topology Hiding Profile	SMVM_To_SP4
Received Interface	InsideUDP1	Signaling Manipulation Script	None
		Remote Branch Office	Any

Figure 89: Trunking Server Flow

12.14. System Manager

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

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

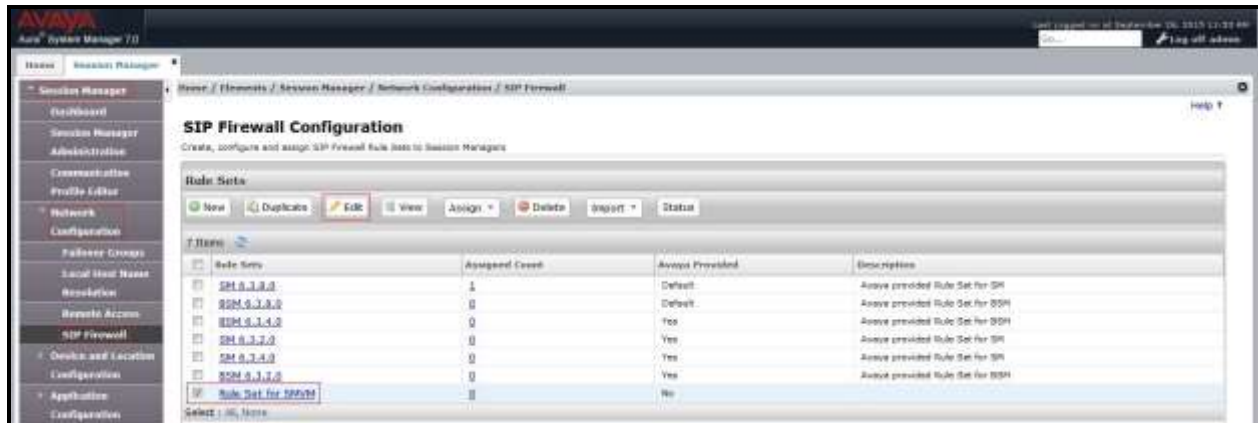


Figure 90: Session Manager – SIP Firewall Configuration - Rules

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 (**10.33.10.21**, see **Section 12.1**).
- In the **Mask** field, enter the appropriate mask (e.g., **255.255.255.255**).
- **Enabled** box is checked.
- Select **Commit**.

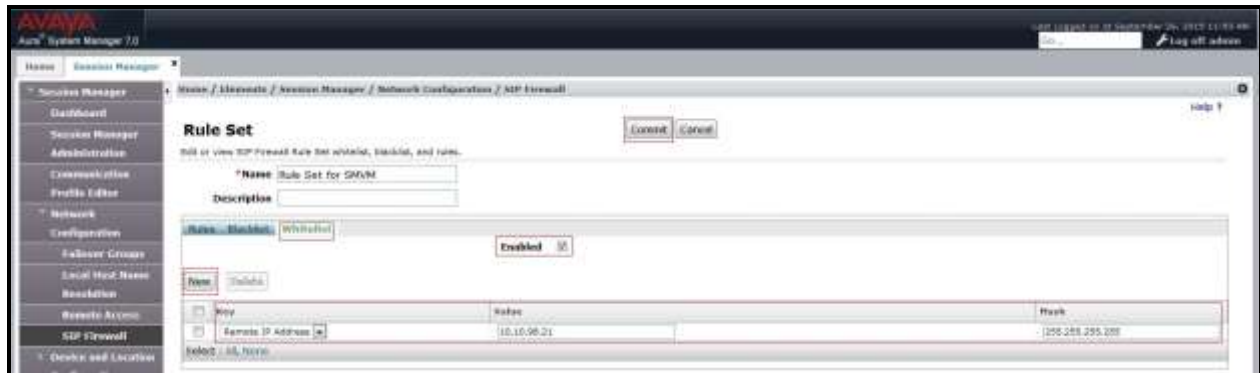


Figure 91: Session Manager – SIP Firewall Configuration - Whitelist

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

Select the **Session Manager Instances** as **bvwas2**, and select **Edit**.

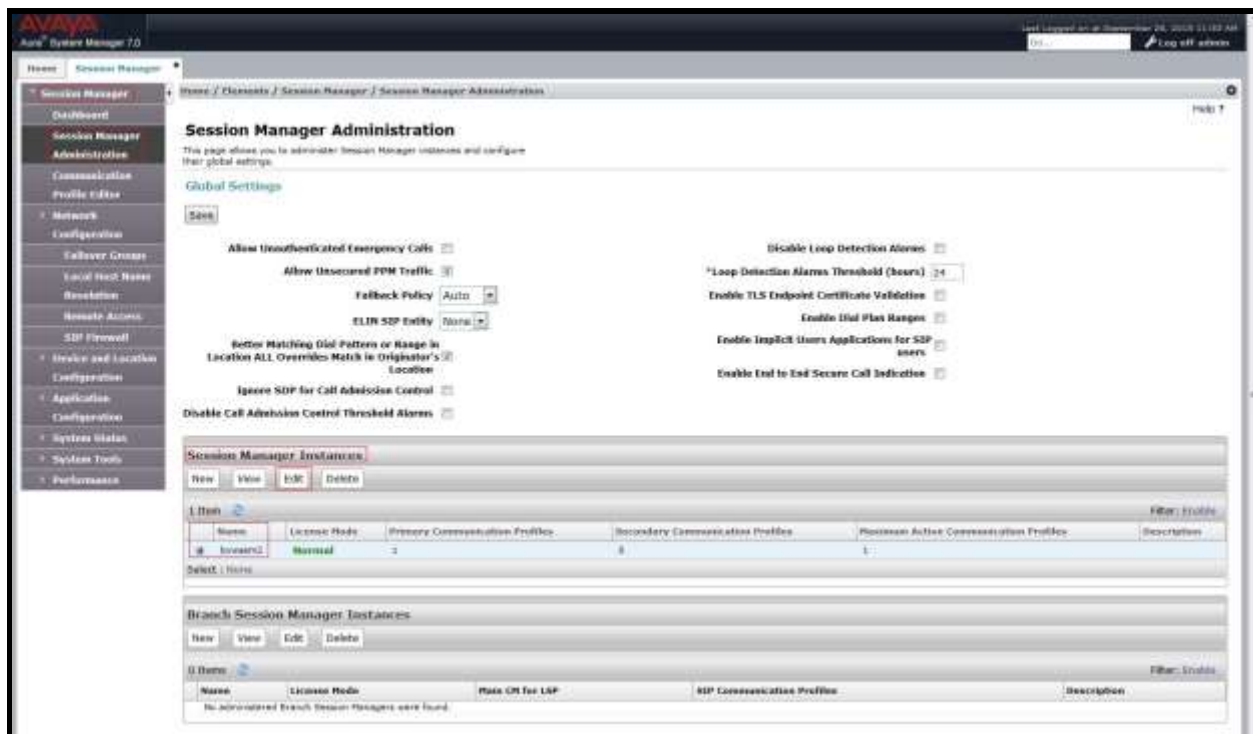


Figure 92: Session Manager – Edit Instance

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

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



Figure 93: Session Manager – Disable PPM limit

12.15. Remote Worker Client Configuration

The following screens illustrate Avaya Communicator for Windows 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 Communicator Settings** and click on **Server**. Set **Server address** parameter to the outside interface of the Avaya SBCE defined for Remote Worker telephony, **10.10.98.99** (see **Section 12.1**). Set **Server port**: **5060** and **Transport type**: **TCP**. The **Domain** is set to **bvwdev.com**. The other fields are default. Click **OK** to submit the settings.

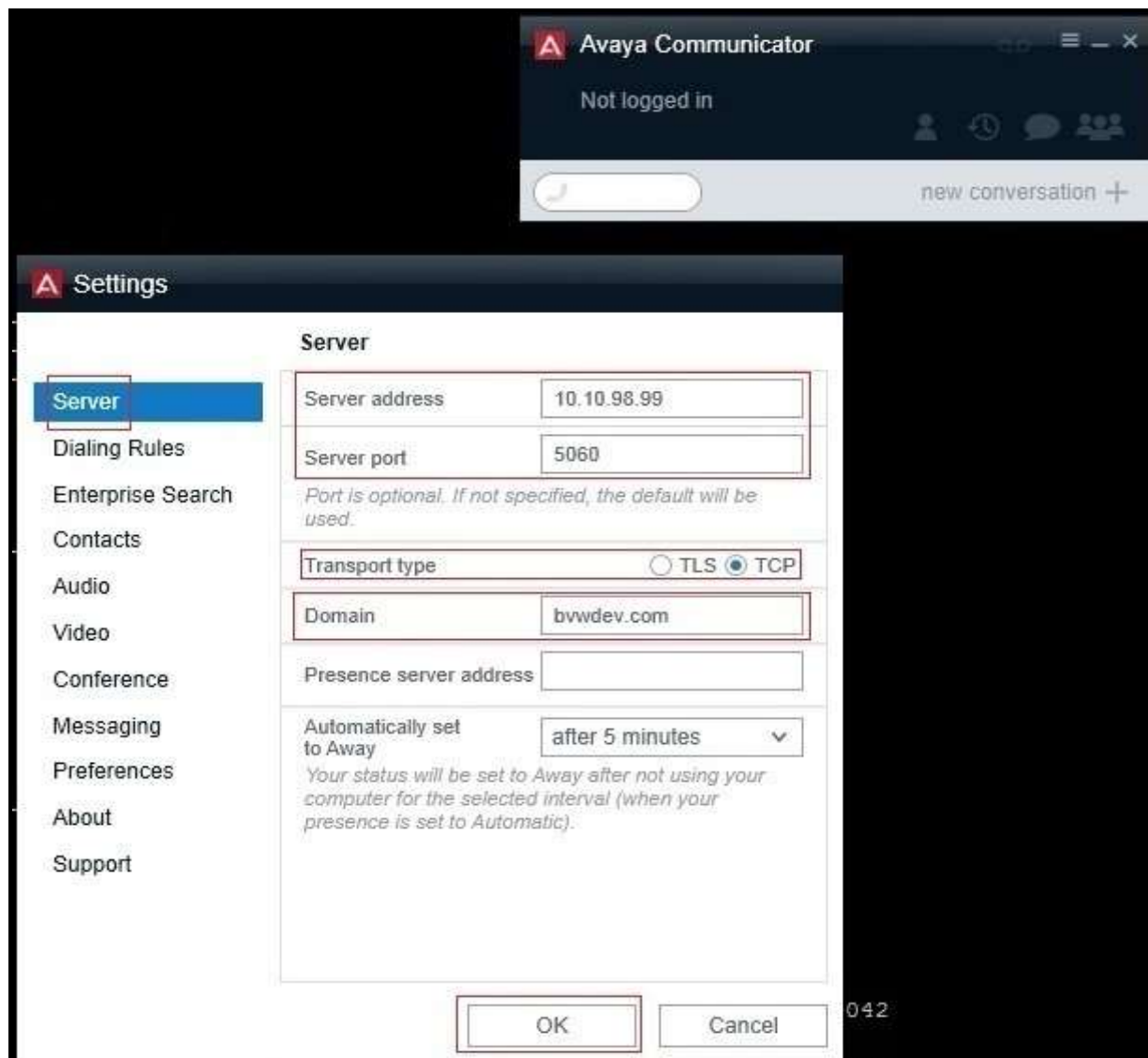


Figure 94: Avaya Communicator for Windows - SIP Global Settings

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="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
  {
    //Remove user in SIP URI in Request-Line header of the OPTIONS coming from IntelPeer

    %HEADERS["Request_Line"][1].URI.USER.regex_replace("(\\DEN43SAOP0002W80001)", "");
  }
}
```

©2015 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.