

Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Videotron SIP Trunking with Avaya Aura[®] Communication Manager 6.3, Avaya Aura[®] Session Manager 6.3 and Avaya Session Border Controller for Enterprise 6.2.1 – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Videotron SIP Trunking and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura[®] Session Manager 6.3, Avaya Aura[®] Communication Manager 6.3, Avaya Session Border Controller for Enterprise 6.2.1 Q16 and various Avaya endpoints.

Videotron 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.	INT	RODUCTION	4
2.	GEN	ERAL TEST APPROACH AND TEST RESULTS	4
	2.1.	INTEROPERABILITY COMPLIANCE TESTING	4
	2.2.	TEST RESULTS	5
	2.3.	SUPPORT	5
3.	REF	ERENCE CONFIGURATION	6
4.	EQU	IPMENT AND SOFTWARE VALIDATED	7
5.		IFIGURE AVAYA AURA [®] COMMUNICATION MANAGER	
	5.1.	LICENSING AND CAPACITY	8
	5.2.	System Features	
	5.3.	IP NODE NAMES	
	5.4.	CODECS	
	5.5.	IP NETWORK REGION	
	5.6.	CONFIGURE IP INTERFACE FOR PROCR	14
	5.7.	SIGNALING GROUP	14
	5.8.	TRUNK GROUP	16
	5.9.	CALLING PARTY INFORMATION	20
	5.10.	OUTBOUND ROUTING	
	5.11.	INCOMING CALL HANDLING TREATMENT	
	5.12.	AVAYA AURA® COMMUNICATION MANAGER STATIONS	24
	5.13.	SAVE AVAYA AURA® COMMUNICATION MANAGER CONFIGURATION CHANGES	24
6.	CON	FIGURE AVAYA AURA [®] SESSION MANAGER	25
	6.1.	AVAYA AURA® SYSTEM MANAGER LOGIN AND NAVIGATION	26
	6.2.	SPECIFY SIP DOMAIN	
	6.3.	ADD LOCATION	
	6.4.	ADD SIP ENTITIES	
	6.4.1	. Configure Session Manager SIP Entity	
		. Configure Communication Manager SIP Entity	
		. Configure Avaya Session Border Controller for Enterprise SIP Entity	
	6.5.	ADD ENTITY LINKS	
	6.6.	CONFIGURE TIME RANGES	
	6.7.	ADD ROUTING POLICIES	
	6.8.	ADD DIAL PATTERNS	
7.	CON	FIGURE AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE	42
	7.1.	LOG IN AVAYA SESSION BORDER CONTROLLER FOR ENTERPRISE	
	7.2.	GLOBAL PROFILES	
		. Configure Server Interworking Profile - Avaya site	
		. Configure Server Interworking Profile – Videotron site	
		. Configure URI Groups	
		. Configure Routing – Avaya site	
		. Configure Routing – Videotron site	
		. Configure Signaling Manipulation	
		. Configure Server – Session Manager	
		. Configure Server – Videotron	
		. Configure Topology Hiding – Avaya site	
	7.2.1	0. Configure Topology Hiding – Videotron site	
	7.3.	DOMAIN POLICIES	53

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	2 of 108
SPOC 11/6/2014	©2014 Avaya Inc. All Rights Reserved.	VTCM63SM63SBCE

	7.3.1.	. Create Application Rules	54
	7.3.2.	. Create Border Rules	54
	7.3.3.	. Create Media Rules	55
	7.3.4.	. Create Security Rules	57
	7.3.5.	. Create Signaling Rules	58
		. Create Time of Day Rules	
	7.3.7.	Create Endpoint Policy Groups	61
	7.3.8.	. Create Session Policy	64
7.	4.	DEVICE SPECIFIC SETTINGS	
	7.4.1.	. Manage Network Settings	65
		. Create Media Interfaces	
		. Create Signaling Interfaces	
		. Configuration Server Flows	
		4.4.1 Create End Point Flows – SM63 Flow	
		4.4.2 Create End Point Flows – Videotron Flow	
		. Create Session Flows	
8.	VIDE	EOTRON SIP TRUNKING CONFIGURATION	71
9.	VER	IFICATION STEPS	71
10.	CON	ICLUSION	72
11.		ERENCES	
12. CON		ENDIX A – REMOTE WORKER CONFIGURATION ON THE AVAYA SESSION BORI LLER FOR ENTERPRISE (AVAYA SBCE)	
13	2.1.	NETWORK MANAGEMENT	77
	2.2.	MEDIA INTERFACE	
	2.3.	SIGNALING INTERFACE	
	2.4.	CREATE REMOTE WORKER URI GROUP	
12	2.5.	ROUTING PROFILE	
12	2.6.	CONFIGURE SERVER INTERWORKING PROFILE - AVAYA SITE	
	2.7.	SERVER CONFIGURATION	
12	2.8.	USER AGENTS	
12	2.9.	RELAY SERVICES	85
12	2.10.	Cluster Proxy	86
12	2.11.	APPLICATION RULES	
12	2.12.	Media Rules	90
12	2.13.	END POINT POLICY GROUPS	93
12	2.14.	END POINT FLOWS	96
	12.14	4.1. Subscriber Flow	
	12.14	4.2. Server Flow	
		2.14.2.1 Remote Worker Server Flow	
	12.	2.14.2.2 Trunking Server Flow	
12	2.15.	System Manager	
		5.1. Modify Session Manager Firewall: Elements \rightarrow Session Manager \rightarrow Network Configuration	
		vall	
		5.2. Disable PPM Limiting: Elements \rightarrow Session Manager \rightarrow Session Manager Administration	
12	2.16.	REMOTE WORKER IP TELEPHONE (9630 SIP) CONFIGURATION	
		5.1. ADDR Screen	
		5.2. SIP Global Settings Screen	•
		5.3. SIP Proxy Settings Screen	
12	2.17.	AVAYA IP TELEPHONE 46XXSETTINGS CONFIGURATION FILE	106

Solution & Interoperability Test Lab Application Notes ©2014 Avaya Inc. All Rights Reserved.

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Videotron SIP Trunking and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura[®] Session Manager 6.3, Avaya Aura[®] Communication Manager 6.3, Avaya Session Border Controller for Enterprise (Avaya SBCE) 6.2.1 Q16 and various Avaya endpoints.

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

2. General Test Approach and Test Results

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

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

2.1. Interoperability Compliance Testing

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

- Response to SIP OPTIONS queries.
- Incoming PSTN calls to various phone types including H.323, SIP, digital, and analog telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types including H.323, SIP, digital, and analog telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from softphones. Two Avaya soft phones were used in testing: Avaya one-X[®] Communicator and Avaya Flare[®] Experience for Windows. Avaya one-X[®] Communicator supports two work modes (Computer and Other Phone). Each supported mode was tested. Avaya one-X[®] Communicator also supports two Voice over IP (VoIP) protocols: H.323 and SIP. Both protocols were tested. Avaya Flare[®] Experience for Windows was used in testing as a simple SIP endpoint for basic inbound/outbound calls.

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	4 of 108
SPOC 11/6/2014	©2014 Avaya Inc. All Rights Reserved.	VTCM63SM63SBCE

- SIP transport using UDP, TCP or TLS 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, long distance, international, outbound toll-free, 411, and 911 services.
- Codec G.711MU.
- 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 SIP RE-INVITE for call transfer.
- Use Diversion Header for call forward.
- Call Center scenarios.
- Fax G.711 pass-through.

Items not supported or not tested included the following:

- Inbound toll-free.
- Registration and Authentication.

2.2. Test Results

Interoperability testing of Videotron SIP Trunking was completed with successful results for all test cases.

2.3. Support

For technical support on the Videotron system, please use the support link at <u>http://affaires.videotron.com/web/ge/telephonie/sip-pbx/index-en.jsp</u>, or call the customer support number at 1-877-380-4667.

Avaya customers may obtain documentation and support for Avaya products by visiting <u>http://support.avaya.com</u>. 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 Videotron SIP Trunking. This is the configuration used for compliance testing.

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

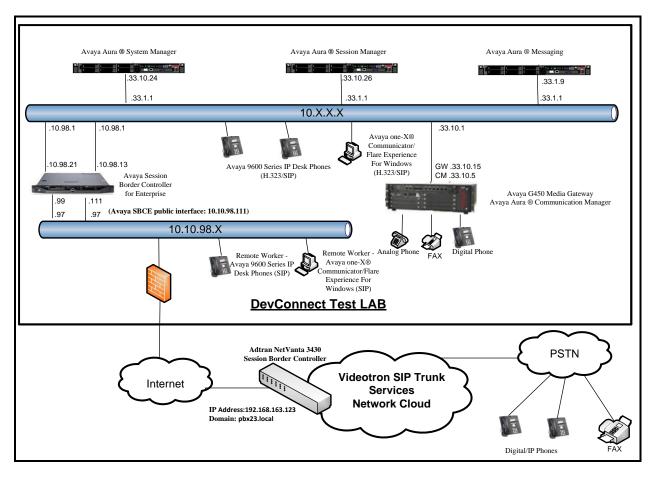


Figure 1: Avaya IP Telephony Network and Videotron SIP Trunking

Solution & Interoperability Test Lab Application Notes ©2014 Avaya Inc. All Rights Reserved.

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	6.3.5			
running on Avaya S8300 Server	(R016x.03.0.124.0-21591)			
Avaya G450 Media Gateway				
– MM711AP Analog	HW46 FW096			
 MM712AP Digital 	HW10 FW014			
– MM710AP	HW05 FW020			
Avaya Aura [®] Session Manager	6.3.7			
running on Avaya S8800 Server	(6.3.7.0.637008)			
Avaya Aura [®] System Manager	6.3.7			
running on Avaya S8800 Server	(Build no 6.3.0.8.5682 – 6.3.8.3204)			
Avaya Aura [®] Messaging	6.2 SP2			
running on Avaya S8800 Server				
Avaya Session Border Controller for Enterprise	6.2.1 Q16			
running on Dell R210 V2 Server				
Avaya 9630 IP Deskphone (SIP)	Avaya one-X [®] Deskphone SIP Edition 2.6.6.0			
Avaya 9640 IP Deskphone (H.323)	Avaya one-X [®] Deskphone Edition			
	3.2			
Avaya 9630 IP Deskphone (H.323)	Avaya one-X [®] Deskphone Edition			
	3.2			
Avaya Flare [®] Experience for Windows	1.1.4.23			
Avaya one-X [®] Communicator (H.323 & SIP)	6.2.3.05 FP3			
Avaya Digital Telephones (1408D)	N/A			
Nortel Symphony 2000 Analog telephone	N/A			
HP Officejet 4500 Fax	N/A			
Videotron SIP Tru				
Equipment/Software	Release/Version			
Adtran NetVanta 3430 Session Border	R10.3.0.V			
Controller				

Table 1: Equipment and Software Tested

The specific configuration above was used for the compliance testing. Note that this solution will be compatible with other Avaya Server and Media Gateway platforms running similar versions of Communication Manager and Session Manager.

5. Configure Avaya Aura[®] Communication Manager

This section describes the procedure for configuring Communication Manager for Videotron SIP Trunking. It is assumed the general installation of Communication Manager, Avaya Media Gateway and Session Manager has been previously completed and is not discussed here.

The Communication Manager configuration was performed using the System Access Terminal (SAT). Some screens in this section have been abridged and highlighted for brevity and clarity in presentation.

5.1. Licensing and Capacity

Use the **display system-parameters customer-options** command to verify that the **Maximum Administered SIP Trunks** value on **Page 2** is sufficient to support the desired number of simultaneous SIP calls across all SIP trunks at the enterprise including any trunks to the service provider. The example shows that 24000 SIP trunks are available and 248 are in use. The license file installed on the system controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity.

display system-parameters customer-options	Page 2 of 11
OPTIONAL FEATURES	
IP PORT CAPACITIES	USED
Maximum Administered H.323 Trunks:	12000 0
Maximum Concurrently Registered IP Stations:	18000 4
Maximum Administered Remote Office Trunks:	12000 0
Maximum Concurrently Registered Remote Office Stations:	18000 0
Maximum Concurrently Registered IP eCons:	414 0
Max Concur Registered Unauthenticated H.323 Stations:	
Maximum Video Capable Stations:	
Maximum Video Capable IP Softphones:	
Maximum Administered SIP Trunks:	
Maximum Administered Ad-hoc Video Conferencing Ports:	
Maximum Number of DS1 Boards with Echo Cancellation:	
Maximum TN2501 VAL Boards:	
Maximum Media Gateway VAL Sources:	
Maximum TN2602 Boards with 80 VoIP Channels:	
Maximum TN2602 Boards with 320 VoIP Channels:	
Maximum Number of Expanded Meet-me Conference Ports:	300 0
(NOTE: You must logoff & login to effect the per	rmission changes.)

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

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

display system-parameters customer-optic	ons Page 3 of 11
OPTIONA	L FEATURES
Abbreviated Dialing Enhanced List? 1	n Audible Message Waiting? y
Access Security Gateway (ASG)?	n Authorization Codes? n
Analog Trunk Incoming Call ID?	n CAS Branch? n
A/D Grp/Sys List Dialing Start at 01?	n CAS Main? n
Answer Supervision by Call Classifier?	n Change COR by FAC? n
ARS?	Y Computer Telephony Adjunct Links? n
ARS/AAR Partitioning?	y Cvg Of Calls Redirected Off-net? y
ARS/AAR Dialing without FAC?	DCS (Basic)? y
ASAI Link Core Capabilities?	y DCS Call Coverage? y
ASAI Link Plus Capabilities?	y DCS with Rerouting? y
Async. Transfer Mode (ATM) PNC?	n
Async. Transfer Mode (ATM) Trunking?	n Digital Loss Plan Modification? y
ATM WAN Spare Processor?	n DS1 MSP? y
ATMS?	y DS1 Echo Cancellation? y
Attendant Vectoring?	·

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

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

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

Figure 4: System-Parameters Customer-Options Form – Page 5

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 featuresPage1 of19FEATURE-RELATED SYSTEM PARAMETERS<br/>Self Station Display Enabled? yTrunk-to-Trunk Transfer: allAutomatic Callback with Called Party Queuing? nAutomatic Callback - No Answer Timeout Interval (rings): 3<br/>Call Park Timeout Interval (minutes): 10Off-Premises Tone Detect Timeout Interval (seconds): 20<br/>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.

```
9 of 19
change system-parameters features
                                                                Page
                        FEATURE-RELATED SYSTEM PARAMETERS
CPN/ANI/ICLID PARAMETERS
  CPN/ANI/ICLID Replacement for Restricted Calls: anonymous
  CPN/ANI/ICLID Replacement for Unavailable Calls: anonymous
DISPLAY TEXT
                                       Identity When Bridging: principal
                                       User Guidance Display? n
Extension only label for Team button on 96xx H.323 terminals? n
INTERNATIONAL CALL ROUTING PARAMETERS
               Local Country Code: 1
          International Access Code: 011
SCCAN PARAMETERS
  Enable Enbloc Dialing without ARS FAC? n
CALLER ID ON CALL WAITING PARAMETERS
     Caller ID on Call Waiting Delay Timer (msec): 200
```

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 (**SM63**). These node names will be needed for defining the service provider signaling group in **Section 0**.

```
Page
                                                                           2
change node-names ip
                                                                    1 of
                                IP NODE NAMES
                    IP Address
   Name
DevAAM
                 10.33.10.9
SM63
                  10.33.10.26
default
                  0.0.0.0
procr
                  10.33.10.5
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. Videotron SIP Trunking supports the **G.711MU** codec. Default values can be used for all other fields.

```
change ip-codec-set 1 Page 1 of 2

IP Codec Set:

Codec Set: 1

Audio Silence Frames Packet

Codec Suppression Per Pkt Size(ms)

1: G.711MU n 2
```

Figure 8: IP-Codec-Set Form – Page 1

On **Page 2**, to enable fax G.711 pass-through, set the **Fax Mode** to **off**. Note: Use of G.711 pass-through fax on SIP trunks is performed using "best effort" and success is not guaranteed. Avaya Aura[®] Communication Manager does not officially support G.711 pass-through fax on SIP trunks except in the case of T.38 fallback.

change ip-codec-set 1	Page 2 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 O	20

Figure 9: IP-Codec-Set Form – Page 2

5.5. IP Network Region

Create a separate IP network region for the service provider trunk. This allows for separate codec or quality of service settings to be used (if necessary) for calls between the enterprise and the service provider versus calls within the enterprise or elsewhere. For the compliance test, IP network region 1 was chosen for the service provider trunk. Use the **change ip-network-region** 1 command to configure region 1 with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In this configuration, the domain name is **bvwdev7.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** 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 0**.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.4**.
- Default values can be used for all other fields.

```
Page 1 of 20
change ip-network-region 1
                              IP NETWORK REGION
 Region: 1
             Authoritative Domain: bvwdev7.com
Location: 1
  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
                                   AUDIO RESOURCE RESERVATION PARAMETERS
H.323 IP ENDPOINTS
                                                      RSVP Enabled? n
 H.323 Link Bounce Recovery? y
 Idle Traffic Interval (sec): 20
  Keep-Alive Interval (sec): 5
           Keep-Alive Count: 5
```

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

Enable Interface? y

Network Region: 1

IPV4 PARAMETERS

Node Name: procr

Subnet Mask: /24

IPV4 PARAMETERS
```

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 outbound calls and signaling group **21** was used for inbound calls. They were configured using the parameters highlighted below.

Set the Group Type field to sip.

Set the **IMS Enabled** field to **n**. This specifies the Communication Manager will serve as an Evolution Server for Session Manager.

Set the **Transport Method** to the value of **tcp** (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 for testing to aid 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 **SM63**. This node name maps to the IP address of Session Manager as defined in **Section 5.3**.

Set the **Near-end Listen Port** and **Far-end Listen Port** to a valid used port for TCP as **5060**.

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	14 of 108
SPOC 11/6/2014	©2014 Avaya Inc. All Rights Reserved.	VTCM63SM63SBCE

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 **bvwdev7.com** of the enterprise domain for signaling group **20** and blank value for signaling group **21**.

Set **Direct IP-IP Audio Connections** to **y**. This setting will enable media shuffling on the SIP trunk so that Communication Manager will redirect media traffic directly between the SIP trunk and the enterprise endpoint. Note that 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.

Page 1 of 2 add signaling-group 20 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: SM63 Near-end Listen Port: 5060 Far-end Listen Port: 5060 Far-end Network Region: 1 Far-end Secondary Node Name: Far-end Domain: bvwdev7.com Bypass If IP Threshold Exceeded? n RFC 3389 Comfort Noise? n Incoming Dialog Loopbacks: eliminate DTMF over IP: rtp-payload Direct IP-IP Audio Connections? y Session Establishment Timer(min): 3 IP Audio Hairpinning? n Enable Layer 3 Test? y Initial IP-IP Direct Media? n H.323 Station Outgoing Direct Media? n Alternate Route Timer(sec): 6

Figure 12: Signaling-Group for Outbound Call Form

```
Page 1 of
                                                                                2
add signaling-group 21
                                SIGNALING GROUP
Group Number: 21
IMS Enabled? n
                               Group Type: sip
                        Transport Method: tcp
       O-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: SM63
Near-end Listen Port: 5060
                                           Far-end Listen Port: 5060
                                       Far-end Network Region: 1
                                  Far-end Secondary Node Name:
Far-end Domain:
                                             Bypass If IP Threshold Exceeded? n
DTMF over IP: rtp-payload
Session Establishment Timer(min): 3
Incoming Dialog Loopbacks: eliminate
                                               RFC 3389 Comfort Noise? n
                                             Direct IP-IP Audio Connections? y
                                                       IP Audio Hairpinning? n
       Enable Layer 3 Test? y
                                                  Initial IP-IP Direct Media? n
H.323 Station Outgoing Direct Media? n
                                                  Alternate Route Timer(sec): 6
```

Figure 13: Signaling-Group for Inbound Call Form

5.8. Trunk Group

Use the **add trunk-group** command to create trunk groups for the signaling groups created in **Section 0**. For the compliance test, trunk group **20** was used for outbound calls and trunk group **21** was used for inbound calls. They were configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- Enter a descriptive name for the **Group Name**.
- Enter an available trunk access code (TAC) that is consistent with the existing dial plan in the **TAC** field. (i.e. ***020**, ***021**).
- Set **Direction** to **outgoing** for trunk group **20** and **incoming** for trunk group **21**.
- 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 0**. Trunk group **20** was associated to signaling group **20** and trunk group **21** was associated to signaling group **21**.
- 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	: у
Group Name:	Outbound	COR: 1	TN: 1	TAC:	*020
Direction:	outgoing	Outgoing Display? n			
Dial Access?	n	Nie	ght Servio	ce:	
Queue Length:	0		-		
Service Type:	public-ntwrk	Auth Code? n			
		Member	Signali	nt Method: a ing Group: 2 f Members: 5	0

Figure 14: Trunk-Group for Outbound Call Form – Page 1

add trunk-group 21	TRUNK GROUP	Page 1 of 21
Group Number: 21 Group Name: Inbound Direction: incoming Dial Access? n	Group Type: sip COR: 1 TN: 1 Outgoing Display? n Night Serv:	
Service Type: public-ntwrk	Signal	ent Method: auto Ling Group: 21 of Members: 50

Figure 15: Trunk-Group for Inbound Call Form

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 0. Note that the Redirect On OPTIM Failure timer is defined in milliseconds. Verify that the Preferred Minimum Session Refresh Interval is set to a value acceptable to the service provider. This value defines the interval that re-INVITEs must be sent to keep the active session alive. For the compliance test, the value of 600 seconds was used.

```
add trunk-group 20

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 - Out? y

XOIP Treatment: auto Delay Call Setup When Accessed Via IGAR? n
```

Figure 16: Trunk-Group for Outbound Call Form – Page 2

On **Page 3**, set the **Numbering Format** field to **private**. This field specifies the format of the calling party number (CPN) sent to the far-end. Beginning with Communication Manager 6.0, public numbers are automatically preceded with a + sign (E.164 numbering format) when passed in the SIP From, Contact and P-Asserted Identity headers. The compliance test used 10 digit numbering format. Thus, **Numbering Format** was set to **private** and the **Numbering Format** field in the route pattern was set to **unk-unk** (see **Section 5.10**).

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

```
add trunk-group 20

TRUNK FEATURES

ACA Assignment? n Measured: none

Numbering Format: private

UUI Treatment: service-provider

Replace Restricted Numbers? y

Replace Unavailable Numbers? y

Modify Tandem Calling Number: no

Show ANSWERED BY on Display? y
```

Figure 17: Trunk-Group for Outbound Call Form – Page 3

```
add trunk-group 21

TRUNK FEATURES

ACA Assignment? n Measured: none

Numbering Format: private

UUI Treatment: service-provider

Replace Restricted Numbers? y

Replace Unavailable Numbers? y

Modify Tandem Calling Number: no

Show ANSWERED BY on Display? y
```

Figure 18: Trunk-Group for Inbound Call Form – 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.

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

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	19 of 108
SPOC 11/6/2014	©2014 Avaya Inc. All Rights Reserved.	VTCM63SM63SBCE

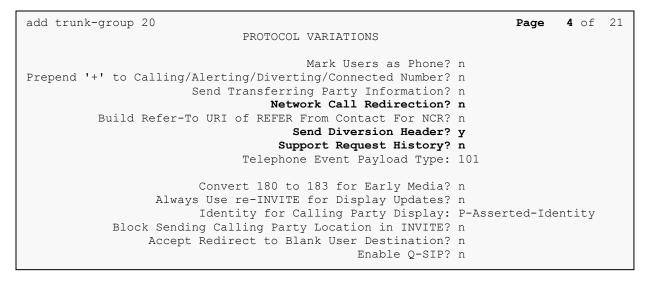


Figure 19: Trunk-Group for Outbound Call Form – Page 4

5.9. Calling Party Information

The calling party number is sent in the SIP "From", "Contact" and "PAI" headers. Since private numbering was selected to define the format of this number (Section 5.8), use the change **private-numbering** command to create an entry for each extension which has a DID assigned. The DID numbers are provided by the SIP service provider. Each DID number is assigned to one enterprise internal extension or Vector Directory Numbers (VDNs). It is used to authenticate the caller.

In a real customer environment, normally the DID number is comprised of the local extension plus a prefix. If this is true, then a single private-numbering entry can be applied for all extensions. In the example below, all stations with a 4-digit extension beginning with **80** will send the calling party number as the **Private Prefix** plus the extension number.

char	nge private-num	bering O	NUMBERING -	PRIVATE	FORMAT	Page	1 of	2
-	Ext Code 80	Trk Grp(s) 20	Private Prefix 514646		Total Len 10	Total Administer Maximum Entries		

Figure 20: Private-Numbering Form

5.10. Outbound Routing

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

change dialplan analysis	DIAL PLAN ANALYSIS TABLE	Page 1 of 12
	Location: all	Percent Full: 2
Dialed Total Call String Length Type	Dialed Total Call String Length Type	Dialed Total Call String Length Type
18 4 ext 8 4 ext 9 1 fac * 4 dac # 4 dac		

Figure 21: Dialplan–Analysis Form

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

```
change feature-access-codes
                                                                  Page 1 of 11
                                FEATURE ACCESS CODE (FAC)
         Abbreviated Dialing List1 Access Code:
         Abbreviated Dialin3g List2 Access Code:
         Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
                      Announcement Access Code: *111
                       Answer Back Access Code:
                         Attendant Access code:
      Auto Alternate Routing (AAR) Access Code: *100
   Auto Route Selection (ARS) - Access Code 1: 9
                                                       Access Code 2:
                 Automatic Callback Activation:
                                                     Deactivation:
Call Forwarding Activation Busy/DA: All:
Call Forwarding Enhanced Status: Act:
                                                     Deactivation:
                                                     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:
                                                        Close Code:
                   Contact Closure Open Code:
```

Figure 22: Feature–Access-Codes Form

HV; Reviewed: SPOC 11/6/2014 Solution & Interoperability Test Lab Application Notes ©2014 Avaya Inc. All Rights Reserved. Use the **change ars analysis** command to configure the routing of dialed digits following the first digit **9**. The example below shows a subset of the dialed strings tested as part of the compliance test. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to **Route Pattern 20** which contains the SIP trunk to the service provider (as defined next).

change ars analysis 0						Page	1 of	2
	I		GIT ANALY: Location:		ΞE	Percent F	ull: 1	
Dialed	Tot	al	Route	Call	Node	ANI		
String	Min	Max	Pattern	Type	Num	Reqd		
0	1	15	20	pubu		n		
1416	11	11	20	pubu		n		
1514	11	11	20	pubu		n		
1613	11	11	20	pubu		n		
1800	11	11	20	pubu		n		
411	3	3	20	svcl		n		
514	10	10	20	pubu		n		
911	3	3	20	svcl		n		

Figure 23: 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 **unk-unk** since private 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 OSIG Intw Dgts 1: 20 0 n user 2: n user 3: user n 4: n user 5: n user 6: user n BCC VALUE TSC CA-TSC ITC BCIE Service/Feature PARM No. Numbering LAR 0 1 2 M 4 W Request Dgts **Format** Subaddress 1: yyyyyn n rest unk-unk none 2: yyyyyn n rest none 3: ууууул п rest none rest. 4: y y y y y n n none

Figure 24: Route–Pattern Form

5.11. Incoming Call Handling Treatment

In general, the incoming call handling treatment for a trunk group can be used to manipulate the digits received for an incoming call if necessary. Since Session Manager is present, Session Manager can be used to perform digit conversion, and digit manipulation via the Communication Manager incoming call handling table may not be necessary. If the DID number sent by Service Provider is unchanged by Session Manager, then the DID number can be mapped to an extension using the incoming call handling treatment of the receiving trunk-group **21**. As an example, use the **change inc-call-handling-trmt trunk-group 21** to convert incoming DID numbers 514646XXX to 4 digit extension XXXX by deleting **6** of the incoming digits. The incoming DID number **5146468011** is converted to **8000** for voicemail testing purpose.

change inc-call-h	andling-trmt		Page	1 of	3		
	INCOMING CALL HANDLING TREATMENT						
Service/	Number	Number	Del	Insert			
Feature	Len	Digits					
public-ntwrk	10	5146468011	10	8000			
public-ntwrk	10	514646	6				

Figure 25: Inc-Call-Handling-Trmt Form

5.12. Avaya Aura[®] Communication Manager Stations

In the sample configuration, four digit station extensions were used with the format 80XX. Use the **add station 8001** command to add an Avaya H.323 IP telephone.

- Enter Type: 9640, Name: 8001, Security Code: 1234, Coverage Path 1: 1, IP SoftPhone: y (if using this extension as a Softphone such as Avaya one-X[®] Communicator)
- Leave other values as default.

add station 8001		Page	1 of	5	
		STATION			
Extension: 8001		Lock Messages? n		BCC:	0
Туре: 9640		Security Code: 1234		TN:	1
Port: S000011		Coverage Path 1: 1		COR:	1
Name: 8001		Coverage Path 2:		COS:	1
		Hunt-to Station:		Tests?	V
STATION OPTIONS					-
		Time of Day Lock Table:			
Loss Group:	19	Personalized Ringing Pattern:	1		
-		Message Lamp Ext:	8001		
Speakerphone:	2-way	Mute Button Enabled?	У		
Display Language:	English	Button Modules:	Ō		
Survivable GK Node Name:	-				
Survivable COR:	internal	Media Complex Ext:			
Survivable Trunk Dest?	У	IP SoftPhone?	у		
	-		-		
		IP Video softpho:	ne? n		
	S	hort/Prefixed Registration Allo	wed: d	efault	
		2			
		Customizable Isbels?	V		

Figure 26: 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 already been defined as part of the initial Session Manager installation. This includes items such as certain SIP Domains, Locations, SIP Entities, and Session Manager itself. However, each item should be reviewed to verify the configuration.

6.1. Avaya Aura[®] System Manager Login and Navigation

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

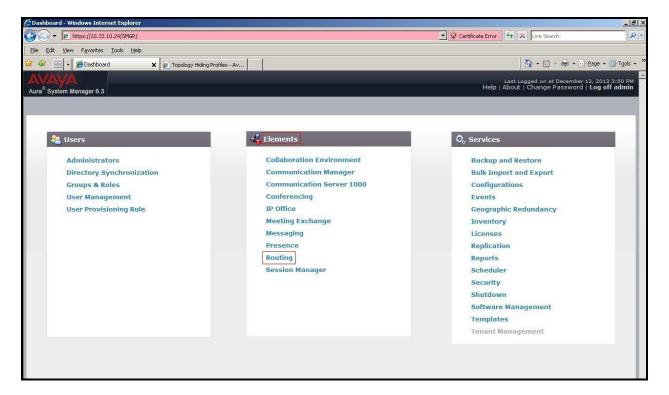


Figure 27 – System Manager Home Screen

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.

Solution & Interoperability Test Lab Application Notes ©2014 Avaya Inc. All Rights Reserved. The navigation tree displayed in the left pane will be referenced in subsequent sections to navigate to items requiring configuration.

AVAYA Aura [®] System Manager 6.3	Last Logged on at December 12 Help About Change Password I	, 2013 3:50 PM . og off admin
Home Routing ×		
* Routing	Home /Elements / Routing	
Domains Locations	Introduction to Network Routing Policy	Help ?
Adaptations	Network Routing Policy consists of several routing applications like "Domains", "Locations", "SIP Entities", etc.	
SIP Entities	The recommended order to use the routing applications (that means the overall routing workflow) to configure your network configuration follows:	is as
Entity Links Time Ranges	Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).	
Routing Policies	Step 2: Create "Locations"	
Dial Patterns	Step 3: Create "Adaptations"	
Regular Expressions Defaults	Step 4: Create "SIP Entities"	
	- SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"	
	- Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)	
	- Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"	
	Step 5: Create the "Entity Links"	
	- Between Session Managers	
	- Between Session Managers and "other SIP Entities"	
	Step 6: Create "Time Ranges"	
	- Align with the tariff information received from the Service Providers	
	Step 7: Create "Routing Policies"	
	- Assign the appropriate "Routing Destination" and "Time Of Day"	
	(Time Of Day = assign the appropriate "Time Range" and define the "Ranking")	
	Step 8: Create "Dial Patterns"	
	- Assign the appropriate "Locations" and "Routing Policies" to the "Dial Patterns"	

Figure 28 – Network Routing Policy

6.2. Specify SIP Domain

Create a SIP Domain for each domain of which Session Manager will need to be aware in order to route calls. For the compliance test, this includes the enterprise domain **bvwdev7.com**.

Navigate to **Routing** \rightarrow **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.

AVAYA Aura [®] System Manager 6.3			Last Help Abou	Logged on at December 12, 2013 3:50 PM It Change Password Log off admin
Home Routing ×				
* Routing	Home / Elements / Routing / Domain	15		
Domains				Help ?
Locations Domain Management				
Adaptations	New Edit Delete Duplica	ate More Actions •		
SIP Entities		20 93 10		
Entity Links	3 Items 🍣			Filter: Enable
Time Ranges	□ Name	Туре	Notes	
Routing Policies	bvwdev7.com	sip		
Dial Patterns				
Regular Expressions				
Defaults	Select : All, None			

Figure 29 – Domain Management

6.3. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. A single Location was defined for the enterprise even though multiple subnets were used. The screens below show the addition of the Location named **Belleville**, which includes all equipment in the enterprise including Communication Manager, Session Manager and Avaya SBCE.

To add a Location, navigate to **Routing** \rightarrow **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.

AVAVA Aura [®] System Manager 6.3			Last Logged on at December 17, 2013 3:18 PM Help About Change Password Log off admin
Home Routing *			
Routing	Home /Elements / Routing / Locations		
Domains			Help ?
Locations	Location Details	Commit Cancel	
Adaptations	General		
SIP Entities	* Name:	Belleville	
Entity Links		GSSCP Belleville	
Time Ranges	Notes:	GSSCP Belleville	
Routing Policies	Dial Plan Transparency in Survivable Mode		
Dial Patterns			
Regular Expressions	Enabled:		
Defaults	Listed Directory Number:		
	Associated CM SIP Entity:	V	
	Overall Managed Bandwidth		
	Managed Bandwidth Units:	Kbit/sec 💌	
	Total Bandwidth:	10000000	
	Multimedia Bandwidth:	10000000	
	Audio Calls Can Take Multimedia Bandwidth:	N	
	Per-Call Bandwidth Parameters		
	Maximum Multimedia Bandwidth (Intra-Location):	2000 Kbit/Sec	
	Maximum Multimedia Bandwidth (Inter-Location):	2000 Kbit/Sec	
	* Minimum Multimedia Bandwidth:	64 Kbit/Sec	
	* Default Audio Bandwidth:	80 Kbit/sec 💌	

Figure 30 – Location Configuration

HV; Reviewed: SPOC 11/6/2014 Solution & Interoperability Test Lab Application Notes ©2014 Avaya Inc. All Rights Reserved. In the **Location Pattern** section, click **Add** to enter IP Address patterns. The following patterns were used in testing:

• **IP Address Pattern:** 10.33.*, 10.10.98.*

3 Items 💝 Filter: Enal				
	IP Address Pattern	*	Notes	
	* 10.33.*			
	* 135.10.98.*			
elect	: All, None			

Figure 31 – IP Ranges Configuration

Click **Commit** to save.

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

6.4. Add SIP Entities

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

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

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

٠	Name:	Enter a descriptive name.
٠	FQDN or IP Address	Enter the FQDN or IP address of the SIP Entity that is used for SIP
		signaling.
٠	Туре:	Select Session Manager for Session Manager, CM for
		Communication Manager and Other for Avaya SBCE.
٠	Adaptation:	This field is only present if Type is not set to Session Manager .
		Adaptation module was not used in this configuration.
•	Location:	Select the Location that applies to the SIP Entity being created. For
		the compliance test, all components were located in Location
		Belleville.
•	Time Zone:	Select the time zone for the Location above.

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	30 of 108
SPOC 11/6/2014	©2014 Avaya Inc. All Rights Reserved.	VTCM63SM63SBCE

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 **SM63**. The IP address of Session Manager's signaling interface is entered for **FQDN or IP Address 10.33.10.26**. Select **Location** as **Belleville** and select **Time Zone** as **America/Toronto**.

Aura [®] System Manager 6.3		Last Logged on at December 12, 2013 3:50 PM Help About Change Password Log off admin
Home Routing *		
▼ Routing 4 Ho	me /Elements / Routing / SIP Entities	
Domains		Help ?
Locations	P Entity Details	Commit Cancel
Adaptations	eneral	
SIP Entities	* Name: SM63	
Entity Links	* FQDN or IP Address: 10.33.10.26	
Time Ranges	Type: Session Manager]
Routing Policies	Notes: SM R6.3	
Dial Patterns		
Regular Expressions	Location: Belleville	
Defaults	Outbound Proxy:	
	Time Zone: America/Toronto	_
	Credential name:	
SI	IP Link Monitoring SIP Link Monitoring: Use Session Manage	

Figure 32 – Session Manager SIP Entity

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

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

Port:	Port number on which Session Manager listens for SIP requests.
Protocol:	Transport protocol to be used with this port.
Default Domain:	The default domain associated with this port. For the compliance
test, th	nis 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, Avaya SIP telephones and SIP soft clients, port **5060** with **UDP** for connecting to Avaya SBCE.

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

	Failover por Failover port					
Add	Contraction of Section					Filter: Enable
+ ne	Port	•	Protocol	Default Domain	Notes	Ther, Lindbig
	5060]	TCP -	bvwdev7.com 💌		
	5060		UDP	bvwdev7.com		1
	L					

Figure 33 – 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 **SP3_CM63**. 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 **10.33.10.5**. Note that **CM** was selected for **Type**. The **Location** field is set to **Belleville** which is the Location that includes the subnet where Communication Manager resides. Select **Time Zone** as **America/Toronto**.

Aura [®] System Manager 6.3		Last Logged on at December 12, 2013 3:50 PM Help About Change Password Log off admin
Home Routing *		
Routing	Home /Elements / Routing / SIP Entities	
Domains	SIP Entity Details	Commit Cancel
Adaptations	General	
SIP Entities	* Name: SP3_CM63	
Entity Links	* FQDN or IP Address: 10.33.10.5	
Time Ranges	Туре: СМ	
Routing Policies	Notes:	
Dial Patterns		
Regular Expressions	Adaptation:	
Defaults	Location: Belleville	8.0
	Time Zone: America/Toronto	
	* SIP Timer B/F (in seconds): 4	
	Call Detail Recording: none 💌	

Figure 34 – 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 SBC's private network interface **10.10.98.13**. Note that **Other** was selected for **Type**. The **Location** field is set to **Belleville** which includes the subnet where the Avaya SBCE resides. Select **Time Zone** as **America/Toronto**.

Aura [©] System Manager 6.3		Last Logged o Help About Chan	n at December 12, 2013 3:50 PM ge Password Log off admin
Home Routing *			
Routing Home / Elements / Routing / SIP Entit	ties		
Mouting Home / Elements / Routing / SIP Entity Domains SIP Entity Details Locations General SIP Entity Links * FQDN of the second			Help ?
Locations SIP Entity Details		Commit Cancel	
Adaptations General			
SIP Entities	* Name: SBCE		
Entity Links * FQDN c	or IP Address: 10.10.98.13		
Time Ranges	Type: Other		
Routing Policies	Notes: SBCE R6.2	1	
Dial Patterns			
Regular Expressions	Adaptation:	•	
	Location: Belleville		
* SIP Timer B/F Cre Call Det CommProfile Typ	Time Zone: America/Toronto	-	
* SIP Timer B/F	(in seconds): 4		
	dential name:		
Cre			
Call Det	ail Recording: none 💌		
CommProfile Typ	e Preference: 📃 💌		

Figure 35 – 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** \rightarrow **Entity Links** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

•	Name:	Enter a descriptive name.
•	SIP Entity 1:	Select the Session Manager being used.
•	Protocol:	Select the transport protocol used for this link.
٠	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 0).
•	SIP Entity 2:	Select the name of the other system as defined in Section 6.4 .

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	34 of 108
SPOC 11/6/2014	©2014 Avaya Inc. All Rights Reserved.	VTCM63SM63SBCE

- **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 0**).
- **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 0**.

Aura [®] System Manager 6.3										ا Help About	ast Logged Change	on at August 7, 2014 10:04 AM Password Log off admin
Home Routing ×												
* Routing	• Home	/ Elements / Routing) / Entity Lin	ks								
Domains												Help ?
Locations	Entity	y Links						Comm	nit Cancel			
Adaptations												
SIP Entities	1 Iter	n 🏖										Filter: Enable
Entity Links Time Ranges		Name	SIP Entity 1	Protocol	Port	SIP Entity 2		DNS Override	Port	Connection Policy	Deny New Service	Notes
Routing Policies		* SM63_SP3_CM63_50	* SM63 🗸	TCP 🗸	* 5060	* SP3_CM63	~		* 5060	trusted 🗸		
Dial Patterns	Selec	t : All, None										
Regular Expressions												

Figure 36 – Communication Manager Entity Link

The following screen illustrates the Entity Links to Avaya SBCE. The protocol and ports defined here must match the values used on the Avaya SBCE mentioned in **Section 7.2.4** and **7.2.7**.

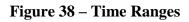
AVAYA Aura [®] System Manager 6.3										ر Help About	ast Logged Change	on at Augu Password	st 7, 2014 10:04 AM Log off admin
Home Routing *													
Routing Generation (Home / Elements / Routing / Entity Links													
Domains													Help ?
Locations	Entity	y Links						Comm	it Cancel				
Adaptations													
SIP Entities	1 Iter	n 健											Filter: Enable
Entity Links			1		-			DNS		Connection	Deny		
Time Ranges		Name	SIP Entity 1	Protocol	Port	SIP Entity 2		Override	Port	Policy	New Service	Notes	
Routing Policies		* SM63_SBCE_5060_U	* SM63 🗸	UDP 🗸	* 5060	* SBCE	~		* 5060	trusted 🗸			
Dial Patterns	Selec	t : All, None											
Regular Expressions													

Figure 37 – 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** \rightarrow **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.

						_						
me Routing ×												
Routing	Home	e /Elements	/ Routing /	Time Rang	ges							
Domains												Help
	Time	Ranges										
Locations	10											
Locations Adaptations	Nev	v Edit	Delete	Duplicate	Mo	re Actions	-					
	Nev	Edit	Delete	Duplicate	Mo	re Actions	•					
Adaptations		v Edit	Delete	Duplicate	Mo	re Actions	-					Filter: Enabl
Adaptations SIP Entities		em 🥲	Delete	Duplicate	We	Th	Fr	Sa	Su	Start Time	End Time	Filter: Enabl
Adaptations SIP Entities Entity Links	1 Ite	em 🍣						Sa	Su	Start Time 00:00	End Time 23:59	
Adaptations SIP Entities Entity Links Time Ranges	1 Ib	em 🍣	Mo	Tu	We	Th	Fr	1000	1000		10000	



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** \rightarrow **Routing Policies** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

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

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	36 of 108
SPOC 11/6/2014	©2014 Avaya Inc. All Rights Reserved.	VTCM63SM63SBCE

- 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 **Videotron_Inbound_To_CM63** associated with incoming PSTN calls from Videotron to Communication Manager. Observe the **SIP Entity as Destination** is the entity named **SP3_CM63**.

										Last I Help About	.ogged on at Septemb Change Password	er 4, 2014 8:03 A Log off admi
Home Routing ×												
* Routing	Home / Eleme	ents / Routing	/ Routing	Policies								
Domains								L.	-	2		Help ?
Locations	Routing Polic	y Details						L	Commit Cance	4		
Adaptations	General											
SIP Entities				* Name	Videotron_I	nbound ⁻	To CM63					
Entity Links				Disabled		_	_					
Time Ranges				* Retries								
Routing Policies	1							_				
Dial Patterns				Notes								
Regular Expressions		D 11 1										
Defaults		as Destinati	ion									
	Select											
	Name			FQDN or	IP Address					Туре	Notes	
	SP3_CM63			10.33.10	.5					Other		
		11										
	Time of Da Add Remove	View Gaps/Ov			1		1	1	1			Filter: Enable
	Add Remove	View Gaps/Ov	Mon		Ved Thu	Fri	Sat	Sun	Start Time	End Time	Notes	
	Add Remove	View Gaps/Ov		Tue W	Ved Thu	Fri	Sat V	Sun	Start Time 00:00	End Time 23:59	Notes Time Range 24	
	Add Remove	View Gaps/Ov	Mon									
	Add Remove	Name 24/7	Mon									
	Add Remove 1 Item Ranking 0 Select : All, Nor Dial Patter	Name 24/7	Mon									
	Add Remove	Name 24/7	Mon						00:00			/7
	Add Remove 1 Item 2 Ranking 0 Select : All, No Dial Patter Add Remove 1 Item 2	Name 24/7	Mon V	×		n		ing Loca	00:00	23:59	Time Range 24	/7

Figure 39 – Routing to Communication Manager

The following screen shows the **Routing Policy Details** for the policy named **Videotron_Outbound_To_SP3** associated with outgoing calls from Communication Manager to the PSTN via Videotron through the Avaya SBCE. Observe the **SIP Entity as Destination** is the entity named **SBCE**.

Avra [®] System Manager 6.3		Last L Help About C	ogged on at September 4, 2014 8:03 AM Change Password Log off admin
Home Routing *			
* Routing	Home / Elements / Routing / Routing Policies		
Domains			Help ?
Locations	Routing Policy Details		
Adaptations	General		
SIP Entities	* Name: Videotron_Outbound_To_SP3		
Entity Links	Disabled:		
Time Ranges	* Retries: 0		
Routing Policies	Notes:		
Dial Patterns	Notes.		
Regular Expressions	SIP Entity as Destination		
Defaults	Select		
	Name FODN or IP Address	Туре	Notes
	SBCE 10.10.98.13	Other	
	Time of Day Add Remove View Gaps/Overlaps		
	1 Item 🧬		Filter: Enable
	□ Ranking 🔺 Name Mon Tue Wed Thu Fri Sat Sun Start Time	End Time	Notes
		23:59	Time Range 24/7
	Select : All, None		

Figure 40 – Routing to Videotron

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 Videotron 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** \rightarrow **Dial Patterns** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

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

•	Pattern:	Enter a dial string that will be matched against the Request-URI of the call.
•	Mint	Enter a minimum longth used in the metch evitaria

- **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).

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	38 of 108
SPOC 11/6/2014	©2014 Avaya Inc. All Rights Reserved.	VTCM63SM63SBCE

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 maximum 11-digit dialed numbers that begin with **1613** and have a destination SIP Domain of **bvwdev7.com** uses Routing Policy Name **Videotron_Outbound_To_SP3** as defined in **Section 6.7**.

Aura [®] System Manager 6.3		Last Logged on at September 4, 2014 8:03 AM Help About Change Password Log off admin
Home Routing ×		
Routing	Home / Elements / Routing / Dial Patterns	
Domains	Dial Pattern Details	Help ?
Locations		
Adaptations	General	
SIP Entities	* Pattern: 1613	
Entity Links	* Min: 11	
Time Ranges	* Max: 11	
Routing Policies		
Dial Patterns	Emergency Call:	
Regular Expressions	Emergency Priority: 1	
Defaults	Emergency Type:	
	SIP Domain: bvwdev7.com 🗸	
	Notes: Videotron Outbound Calls	
	Originating Locations and Routing Policies	
	Add Remove	
	1 Item 🤣	Filter: Enable
	Originating Location Name A Originating Location Name A Routing Policy Name Rank Routing P	olicy Routing Policy Routing Policy Destination Notes
	-ALL- Videotron_Outbound_To_SP3 0	SBCE
	Select : All, None	

Figure 41 – Dial Pattern_1613

Note that the above Dial Pattern did not restrict outbound calls to specific US area codes. In real deployments, appropriate restriction can be exercised per customer business policies.

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

The second example shows that inbound 10-digit numbers that start with **514** uses Routing Policy Name **Videotron_Inbound_To_CM63** as defined in **Section 6.7**. This Dial Pattern matches the DID numbers assigned to the enterprise by Videotron.

Aura [®] System Manager 6.3			н	Last Logged on at September 4, 2014 8:03 AM elp About Change Password Log off admin
Home Routing ×				
• Routing	Home / Elements / Routing / Dial Patter	ns		
Domains	Dial Pattern Details		Commit Cancel	Help ?
Locations			Commic Cancer	
Adaptations	General			
SIP Entities		* Pattern: 514		
Entity Links		* Min: 10		
Time Ranges		* Max: 10		
Routing Policies	Emer	rgency Call:		
Dial Patterns				
Regular Expressions		cy Priority: 1		
Defaults		jency Type:		
	SI	IP Domain: bvwdev7.com		
		Notes: Videotron Inbound Calls		
	Originating Locations and Routin	g Policies		
	Add Remove			
	1 Item			Filter: Enable
	Originating Location Name	Routing Policy Name	Rank Routing Policy Disabled	Routing Policy Destination Notes
	Belleville	Videotron_Inbound_To_CM63	0	SP3_CM63
	Select : All, None			

Figure 42 – Dial Pattern_514

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

System Manager 6.3									
me Routing *									
Routing	• Home	e / Eleme	nts / R	outing	/ Dial Patterns				
Domains	Di-14	Patterns							He
Locations	Dial	Patterns							
Adaptations	New	Edit De	elete	Duplicat	e More Actions •				
SIP Entities									
Sir Linutes	100000								
Entity Links	24 It	ems 🍣			1				Filter: En
Entity Links	24 It	ems 💸 Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Filter: En
Entity Links Time Ranges	24 It	1	Min 1	Max 15	Emergency Call	Emergency Type	Emergency Priority	SIP Domain bvwdev7.com	
Entity Links		Pattern	20			Emergency Type	Emergency Priority		Notes
Entity Links Time Ranges		Pattern <u>0</u>	1	15		Emergency Type	Emergency Priority	bvwdev7.com	Notes Videotron Outbound Calls
Entity Links Time Ranges Routing Policies Dial Patterns		Pattern 0 1416	1 11	15 11		Emergency Type	Emergency Priority	bvwdev7.com bvwdev7.com	Notes Videotron Outbound Calls Videotron Outbound Calls
Entity Links Time Ranges Routing Policies Dial Patterns Regular Expressions		Pattern 0 1416 1514	1 11 11	15 11 11		Emergency Type	Emergency Priority	bvwdev7.com bvwdev7.com bvwdev7.com	Notes Videotron Outbound Calls Videotron Outbound Calls Videotron Outbound Calls
Entity Links Time Ranges Routing Policies Dial Patterns		Pattern 0 1416 1514 1613	1 11 11 11	15 11 11 11		Emergency Type	Emergency Priority	bvwdev7.com bvwdev7.com bvwdev7.com bvwdev7.com	Notes Videotron Outbound Calls Videotron Outbound Calls Videotron Outbound Calls Videotron Outbound Calls
Entity Links Time Ranges Routing Policies Dial Patterns Regular Expressions		Pattern 0 1416 1514 1613 1800	1 11 11 11 11	15 11 11 11 11		Emergency Type	Emergency Priority	bvwdev7.com bvwdev7.com bvwdev7.com bvwdev7.com bvwdev7.com	Notes Videotron Outbound Calls Videotron Outbound Calls Videotron Outbound Calls Videotron Outbound Calls Videotron Outbound Calls

Figure 43 – 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 Videotron system.

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

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

7.1. Log in Avaya Session Border Controller for Enterprise

Access the web interface by typing "**https://x.x.x.k/sbc**/" (where x.x.x.x is the management IP of the Avaya SBCE).

Enter the Username and Password.

A\/A\/A	Log In				
AVAVA	Username:	ucsec			
	Password:	•••••			
		Log In			
Session Border Controller for Enterprise	This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws.				
	administrative and security expressly consents to such that if it reveals possible e	may be monitored and recorded for reasons. Anyone accessing this system n monitoring and recording, and is advised vidence of criminal activity, the evidence of id to law enforcement officials.			
	All users must comply wi protection of information ass	th all corporate instructions regarding the ets.			
	© 2011 - 2013 Avaya Inc. Al	I rights reserved.			

Figure 44 - Avaya SBCE Login

7.2. Global Profiles

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

7.2.1. Configure Server Interworking Profile - Avaya site

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

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

Select **avaya-ru** in Interworking Profiles. Click **Clone**. Enter Clone Name: **SM63** and Click **Finish** (not shown).

The following screen shows that Session Manager server interworking profile (named: **SM63**) was added.

Session Borde	r Controller i	or Enterp	orise			AVAY
Dashboard Administration Backup/Restore System Management	Interworking Profil Add Interworking Profiles	es: SM63		Click here to ac	ld a description.	Rename Clone Delete
Global Parameters	cs2100	General Timer	rs URI Manipulation	Header Manipulation	Advanced	
Global Profiles	avaya-ru		ord manipulation	Gene		
Domain DoS	OCS-Edge-Server	Hold Support		NONE	er al	<u>^</u>
Fingerprint	cisco-ccm	180 Handling		None		
Server Interworking	cups	181 Handling		None		
Phone Interworking Media Forking	OCS-FrontEnd-Server	182 Handling		None		
Routing	SM63	183 Handling		None		
Server Configuration		Refer Handling		No		
Topology Hiding		URI Group		None		
Signaling Manipulation		3xx Handling				
URI Groups SIP Cluster			and an Command	No		
Domain Policies			eader Support	No		
TLS Management		Delayed SDP H	-			
Device Specific Settings		Re-Invite Handli	ng	No		
		T.38 Support		No		
		URI Scheme		SIP		
		Via Header Forr	nat	RFC3261		
		6		Priva	icy	
		Privacy Enabled	1	No		
		User Name				
		P-Asserted-	Identity	No		
		P-Preferred-	Identity	No		

Figure 45 - Server Interworking – Avaya site

HV; Reviewed: SPOC 11/6/2014

Solution & Interoperability Test Lab Application Notes ©2014 Avaya Inc. All Rights Reserved.

7.2.2. Configure Server Interworking Profile – Videotron site

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

- Enter Profile name: **SP3**
- On the **General** tab, all options can be left at default.

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

The following screen shows that Videotron server interworking profile (named: SP3) was added.

Alarms Incidents Statistics		Users		Settings Help Log Ou
Session Borde	r Controller f	or Enterprise		AVAYA
Dashboard Administration Backup/Restore	Interworking Profil	es: SP3		Rename Clone Delete
System Management	Interworking Profiles cs2100		Click here to add a description.	
Global Parameters	avaya-ru	General Timers URI Manipulation	Header Manipulation Advanced	
Global Profiles Domain DoS	OCS-Edge-Server		General	<u>^</u>
Fingerprint	cisco-ccm	Hold Support	NONE	
Server Interworking		180 Handling	None	
Phone Interworking	cups	181 Handling	None	
Media Forking	OCS-FrontEnd-Server	182 Handling	None	
Routing	SP3	183 Handling	None	
Server Configuration Topology Hiding	SM63	Refer Handling	Νο	
Signaling Manipulation		URI Group	None	
URI Groups		3xx Handling	No	
SIP Cluster		Diversion Header Support	No	
Domain Policies		Delayed SDP Handling	No	
TLS Management		Re-Invite Handling	No	
Device Specific Settings		T.38 Support	No	
		URI Scheme	SIP	
		Via Header Format	RFC3261	
			Privacy	
		Privacy Enabled	No	
		User Name		
		P-Asserted-Identity	No	
		P-Preferred-Identity	No	
		Privacy Header		~ .

Figure 46 - Server Interworking – Videotron site

7.2.3. Configure URI Groups

The URI Group feature allows administrator to create any number of logical URI groups that are comprised of individual SIP subscribers located in that particular domain or group. The following URI Group configuration is used for this specific testing in DevConnect Lab environment. The URI-Group named **SP3** was used to match the "From" and "To" headers in a SIP call dialog received from both Enterprise and Videotron service. If there is a match, the Avaya SBCE will apply the appropriate Routing profile (see **Section 7.2.4, 7.2.5**), Server Flow

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	45 of 108
SPOC 11/6/2014	©2014 Avaya Inc. All Rights Reserved.	VTCM63SM63SBCE

(see Section 7.4.4), and Session Flow (see Section 7.4.5) to route incoming and outgoing calls to the right destinations. In production environment, there is not a requirement to define this URI.

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

Enter Group Name: SP3.

Edit the URI Type: Regular Expression (not shown).

Add URI: ***10\.10\.98\.111** (Avaya SBCE public interface IP address), ***10\.10\.98\.13** (Avaya SBCE internal interface IP address), ***192\.168\.163\.123** (Videotron Switch IP address), ***anonymous\.invalid** (Anonymous URI), ***bvwdev7\.com** (Enterprise domain), ***pbx21.local** (Videotron domain).

Click **Finish** (not shown).

Alarms Incidents Statistics	s Logs Diagnostics	Users	Settings He	elp Log Out
Session Borde	r Controller f	or Enterprise	,	avaya
Dashboard Administration	URI Groups: SP3			ne Delete
Backup/Restore			Renar	ne Delete
System Management	URI Groups	Click here to add a description.		
Global Parameters	SP3	URI Group		
 Global Profiles 	test			Add
Domain DoS	Emergency			Add
Fingerprint		URI Listing		
Server Interworking		.*10\.10\.98\.111	E	dit Delete
Phone Interworking		.*10\.10\.98\.13	E	Edit Delete
Media Forking		.*192\.168\.163\.123	E	Edit Delete
Routing		*anonymous\.invalid	E	Edit Delete
Server Configuration		*bywdev7\.com	F	Edit Delete
Topology Hiding				
Signaling Manipulation		.*pbx21\.local	E	Edit Delete
URI Groups				
SIP Cluster				

Figure 47 - URI Group

7.2.4. Configure Routing – Avaya site

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

From the menu on the left-hand side, select **Global Profiles** \rightarrow **Routing** \rightarrow **Add** Enter Profile Name: **SP3_To_SM63**.

- URI Group: SP3 (See Section 7.2.3).
- Next Hop Server 1: 10.33.10.26:5060 (Session Manager IP address).
- Check Routing Priority based on Next Hop Server (not shown).
- Outgoing Transport: UDP (not shown) (See Section 6.5).
- Click **Finish** (not shown).

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	46 of 108
SPOC 11/6/2014	©2014 Avaya Inc. All Rights Reserved.	VTCM63SM63SBCE

Alarms Incidents Statistic	cs Logs Diagnostics	Users		Settir	ngs Help	Log Out
Session Borde	er Controller f	or Enterprise			AV	AYA
Dashboard Administration Backup/Restore	Routing Profiles: S	P3_To_SM63		Renam	ne Clone	Delete
System Management	Routing Profiles default		Click here to add a descript	ion.		-
 Global Parameters Global Profiles Domain DoS 	SP3_To_SM63	Routing Profile				Add
Fingerprint		Priority URI Group	Next Hop Server 1 10.33.10.26:5060	Next Hop Server 2	Viev	v Edit
Server Interworking Phone Interworking Media Forking Routing Server Configuration			10.33.10.20.5060		Viev	r Luit

Figure 48 - Routing to Avaya

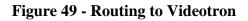
7.2.5. Configure Routing – Videotron site

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

From the menu on the left-hand side, select **Global Profiles** \rightarrow **Routing** \rightarrow **Add** Enter Profile Name: SM63_To_SP3.

- URI Group: SP3 (See Section 7.2.3).
- Next Hop Server 1: 192.168.163.123:5060 (Videotron Switch IP address).
- Check Routing Priority based on Next Hop Server (not shown).
- **Outgoing Transport** as **UDP** (not shown) (See Section 6.5).
- Click **Finish** (not shown).

Alarms Incidents Statistic	cs Logs Diagnostics	Users Setting	s Help	Log Out
Session Borde	er Controller f	or Enterprise	A	/AYA
Dashboard Administration Backup/Restore	Routing Profiles: S	Rename	Clone	Delete
System Management Global Parameters Global Profiles 	Routing Profiles default SM63_To_SP3	Click here to add a description. Routing Profile		Add
Domain DoS Fingerprint Server Interworking	SP3_To_SM63	Priority URI Group Next Hop Server 1 Next Hop Server 2 1 SP3 192.168.163.123.5060	Vie	
Phone Interworking Media Forking Routing Server Configuration				



7.2.6. 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.

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	47 of 108
SPOC 11/6/2014	©2014 Avaya Inc. All Rights Reserved.	VTCM63SM63SBCE

- Select **Global Profiles** from the menu on the left-hand side.
- Select the Signaling Manipulation.
- Select **Add**. Enter script Title: **SP3**. In the script editing window, enter the text exactly as shown in the screenshot below to perform the following:

Edit script to remove unexpected prefix in From/Contact SIP Headers from incoming calls.

Edit the script to remove unwanted SIP Headers from outgoing calls. Click **Save** (not shown).

Session Borde	er Controller f	or Enterprise	
			Furg
Dashboard	Signaling Manipula	ation Scripts: SP3	
Administration	Upload Add		Download Clone Delete
Backup/Restore	Signaling Manipulation	Click here to add a description.	
system Management	Scripts		
Global Parameters	SP3	Signaling Manipulation	
Global Profiles		within session "INVITE"	
Domain DoS		{ act on message where %DIRECTION="INBOUND" and %ENTRY POINT="AFTER NETWORK"	
Fingerprint		{	
Server Interworking		<pre>%HEADERS["From"][1].URI.USER.regex_replace("(\011)",""); %HEADERS["Contact"][1].URI.USER.regex_replace("(\011)","");</pre>	
Phone Interworking		}	
Media Forking		within session "All"	
Routing		<pre>{ act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"</pre>	
Server Configuration		{	
Topology Hiding			
Signaling		// Remove unwanted Headers	
Manipulation		<pre>remove(%HEADERS["Alert-Info"][1]);</pre>	
URI Groups		<pre>remove(%HEADERS["P-AV-Message-Id"][1]); remove(%HEADERS["P-Charging-Vector"][1]);</pre>	
SIP Cluster		remove(%HEADERS["Av-Global-Session-ID"][1]);	
Domain Policies		<pre>remove(%HEADERS["P-Location"][1]);</pre>	
TLS Management		}	
Device Specific Settings		1	

Figure 50 – Signaling Manipulation

7.2.7. Configure Server – Session Manager

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

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

Enter profile name: **SM63**.

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

- Server Type: Select Call Server
- IP Address/FQDNs: 10.10.33.26 (Session Manager IP Address)

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	48 of 108
SPOC 11/6/2014	©2014 Avaya Inc. All Rights Reserved.	VTCM63SM63SBCE

• Supported Transports: UDP, UDP Port: 5060 (See Section 6.5)

Session Borde	r Controller	٨\/٨\//		
Dashboard Administration Backup/Restore System Management	Server Configur	ation: SM63	at Advanced	Rename Clone Delete
 Global Parameters Global Profiles Domain DoS 	SM63	Server Type IP Addresses / FQDNs Supported Transports	Call Server 10.33.10.26 UDP	
Fingerprint Server Interworking Phone Interworking Media Forking		UDP Port	5060	
Routing Server Configuration Topology Hiding			Edit	

Figure 51 - Session Manager General Server Configuration

On the **Advanced** tab:

• Select SM63 for Interworking Profile (See Section 7.2.1).

Click **Finish** (not shown).

Alarms Incidents Statistics				Settings Help Log Ou
Session Borde	r Controller f	for Enterprise		AVAYA
Dashboard Administration	Server Configurat	ion: SM63		
Backup/Restore System Management	Add Server Profiles	General Authentication Heartbeat	vanced	Rename Clone Delete
Global Parameters	SM63	Enable DoS Protection		
Global Profiles Domain DoS		Enable Grooming		
Fingerprint		Interworking Profile	SM63	
Server Interworking		Signaling Manipulation Script	None	
Phone Interworking		UDP Connection Type	SUBID	
Media Forking Routing			Edit	
Server Configuration		L	2011-11-12-12-12-12-12-12-12-12-12-12-12-1	
Topology Hiding				

Figure 52 - Session Manager Advanced Server Configuration

7.2.8. Configure Server – Videotron

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

Enter profile name: **SP3**

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

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	49 of 108
SPOC 11/6/2014	©2014 Avaya Inc. All Rights Reserved.	VTCM63SM63SBCE

- Server Type: Select Trunk Server
- IP Address: 192.168.163.123 (Videotron Switch IP Address)
- Supported Transports: UDP
- UDP Port: 5060

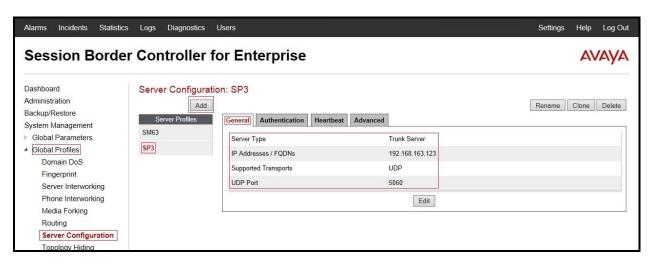


Figure 53 - Videotron General Server Configuration

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

- Interworking Profile: select SP3 (See Section 7.2.2)
- Signaling Manipulation Script: select SP3 (See Section 7.2.6)

Click **Finish** (not shown).

Alarms Incidents Statistic		Settings Help Log Ou		
Dashboard Administration Backup/Restore System Management > Global Parameters 4 Global Profiles Domain DoS Fingerprint Server Interworking Phone Interworking Media Forking Routing Server Configuration Topology Hiding	Server Configuration	on: SP3	Advanced Advanced SP3 SP3 SUBID Edit	Rename Clone Delete

Figure 54 - Videotron Advanced Server Configuration

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

- Check Enable Heartbeat.
- Select Method: OPTIONS
- Enter **Frequency**: **60 seconds**
- Enter From URI: 5146468001@10.10.98.111
- Enter To URI: 5146468001@pbx21.local

Click **Finish** (not shown).

Alarms Incidents Statistic	s Logs Diagnostics L	Jsers		Settings Help Log Out
Session Borde	r Controller fo	or Enterprise		AVAYA
Dashboard Administration Backup/Restore System Management Clobal Parameters Global Profiles Domain DoS Fingerprint Server Interworking Phone Interworking Media Forking Routing Server Configuration	Server Configuratio	n: SP3 General Authentication Heartbe Enable Heartbeat Method Frequency From URI To URI	Advanced Advanced OPTIONS 60 seconds 5146468001@10.10.98.111 5146468001@pbx21.local Edit	Rename Cione Delete
Topology Hiding				

Figure 55 - Videotron Heartbeat Server Configuration

HV; Reviewed:
SPOC 11/6/2014

Solution & Interoperability Test Lab Application Notes ©2014 Avaya Inc. All Rights Reserved.

7.2.9. 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** \rightarrow **Topology Hiding**.

Select Add, enter Profile Name: SP3_To_SM63.

- For the Header **To**,
 - In the **Criteria** column select **IP/Domain** In the **Replace Action** column select: **Overwrite** In the **Overwrite Value** column: **bvwdev7.com**
- For the Header **Request-Line**,
 - In the **Criteria** column select **IP/Domain** In the **Replace Action** column select: **Overwrite** In the **Overwrite Value** column: **bvwdev7.com** For the Header **From**,
 - In the Criteria column select IP/Domain
 - In the **Replace Action** column select: **Overwrite** In the **Overwrite Value** column: **bvwdev7.com**

Click **Finish** (not shown).

er Controller fo	or Enterprise			AN	/AYA
Topology Hiding Pr Add Topology Hiding Profiles default	rofiles: SP3_To_SM6		rre to add a description,	Rename Clone	Delete
cisco_th_profile	Header	Criteria	Replace Action	Overwrite Value	
SP3_To_SM63	To	IP/Domain	Overwrite	bvwdev7.com	
	Request-Line	IP/Domain	Overwrite	bvwdev7.com	
	From	IP/Domain	Overwrite	bvwdev7.com	
	-		Edit		
	Topology Hiding P Add Topology Hiding Profiles default cisco_th_profile	Topology Hiding Profiles: SP3_To_SM6 Add Topology Hiding Profiles default cisco_th_profile SP3_To_SM63 To Request-Line	Topology Hiding Profiles Click he default Cisco_th_profile SP3_To_SM63 To IP/Domain Request-Line IP/Domain	Topology Hiding Profiles: SP3_To_SM63 Click here to add a description. Click here to add a description. default cisco_th_profile SP3_To_SM63 Topology Hiding Topology Hiding Topology Hiding Topology Hiding To IP/Domain Overwrite Feed to IP/Domain Overwrite From IP/Domain Overwrite	Topology Hiding Profiles: SP3_To_SM63 Rename Clone Click here to add a description. default csco_th_profile SP3_To_SM63 Image: Click here to add a description. Click here to add a description. Image: Click here to add a description.



7.2.10. Configure Topology Hiding – Videotron site

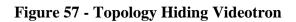
From the menu on the left-hand side, select **Global Profiles** \rightarrow **Topology Hiding**.

Select Add Profile, enter Profile Name: SM63_To_SP3.

- For the Header **From**,
 - In the **Criteria** column select **IP/Domain**
 - In the **Replace Action** column select: **Overwrite**
 - In the **Overwrite Value** column: **10.10.98.111**
- For the Header **To**,
 - In the Criteria column select IP/Domain
 - In the **Replace Action** column select: **Overwrite**
 - In the Overwrite Value column: pbx21.local
- For the Header **Request-Line**,
 - In the **Criteria** column select **IP/Domain**
 - In the **Replace Action** column select: **Overwrite**
 - In the **Overwrite Value** column: **pbx21.local**

Click **Finish** (not shown).

Alarms Incidents Statistic	s Logs Diagnostics	Users			Settings Help Log Out
Session Borde	r Controller	for Enterprise			AVAYA
Dashboard Administration Backup/Restore	Topology Hiding F	Profiles: SM63_to_SP3			Rename Clone Delete
System Management	Topology Hiding Profiles		Click he	re to add a description.	
Global Parameters	default	Topology Hiding			
Global Profiles	cisco_th_profile		0111	DATESTAN	0 N V I
Domain DoS	SM63_to_SP3	Header	Criteria IP/Domain	Replace Action	Overwrite Value
Fingerprint	SP3 To SM63	1.1.4.000			
Server Interworking	010_10_01100	То	IP/Domain	Overwrite	pbx21.local
Phone Interworking		Request-Line	IP/Domain	Overwrite	pbx21.local
Media Forking				Edit	
Routing		2			
Server Configuration					
Topology Hiding					
Signaling Manipulation					



7.3. Domain Policies

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

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	53 of 108
SPOC 11/6/2014	©2014 Avaya Inc. All Rights Reserved.	VTCM63SM63SBCE

7.3.1. Create Application Rules

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

For the compliance test, the predefined **default** application rule (shown below) was used for both Session Manager and the Videotron server.

From the menu on the left-hand side, select **Domain Policies** \rightarrow **Application Rules**. Select the **default** rule to view.

Alarms Incidents Statistic		Users				Settings	Help	Log Out
Session Borde	er Controller f	or Enterprise					AVA	ауа
Dashboard	Application Rules:	default						
Administration	Add	Filter By Device 🗸					Clone	
Backup/Restore	Application Rules	It is not recommended to edit the defaults	Try cloning or adding	o a nev	v rule instead.			
System Management	default			2 - 10				
 Global Parameters Global Profiles 	default-trunk	Application Rule						
 SIP Cluster 	default-subscriber-low	Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessi	ons Per End	point
Domain Policies		Audio	$\mathbf{\Sigma}$	\checkmark	2000	10		
Application Rules	default-subscriber-high	Video						
Border Rules	default-server-low	IM						
Media Rules	default-server-high							
Security Rules				Misce	ellaneous			
Signaling Rules		CDR Support	Non	e				
Time of Day Rules		RTCP Keep-Alive	No					
End Point Policy Groups					Edit			
Session Policies				201	M7			



7.3.2. Create Border Rules

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

For the compliance test, the predefined **default** border rule (shown below) was used for both Session Manager and the Videotron server.

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

• Select the **default** rule to view.

Solution & Interoperability Test Lab Application Notes ©2014 Avaya Inc. All Rights Reserved.

		-		- condition
Dashboard Administration	Border Rules: defa	ault Filter By Device V		Clone
Backup/Restore System Management > Global Parameters	Border Rules	It is not recommended to edit the defaults	. Try cloning or adding a new rule instead.	
 Global Profiles SIP Cluster 	No-Nat-Reg-Proxy	Enable Natting		
Domain Policies		Refresh Interval	80 second(s)	
Application Rules		Refresh For All Clients		
Border Rules Media Rules		Use SIP Published IP	\checkmark	
Security Rules		Use SDP Published IP	V	

Figure 59 – Border Rule

7.3.3. Create Media Rules

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

For the compliance test, the predefined **default-low-med** media rule (shown below) was used for both Session Manager and the Videotron server.

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

- Select the **default-low-med** rule to view.
- The Media NAT tab has no entries.

default-low-med	
deladit-low-filed	
Add Filter By Device V	Clone
It is not recommended to edit the defaults. Try cloning or adding a new rule instead.	
	a QoS
	lv.
	3
Edit	
6	
	It is not recommended to edit the defaults. Try cloning or adding a new rule instead. Media NAT Media Encryption Media Anomaly Media Silencing Media Media NAT Learn Media IP dynamical Media IP dynamical Media IP dynamical

Figure 60 – Media Rule

HV; Reviewed:
SPOC 11/6/2014

Solution & Interoperability Test Lab Application Notes ©2014 Avaya Inc. All Rights Reserved. The Media Encryption tab indicates that no encryption was used.

Alarms Incidents Statist	iics Logs Diagnostics	Users				Settin	gs Help	Log Out
Session Bord	er Controller f	or Enterprise					A	/AYA
Dashboard Administration Backup/Restore System Management Global Parameters Global Profiles SIP Cluster Domain Policies Application Rules Border Rules Border Rules Security Rules Signaling Rules Time of Day Rules End Point Policy Groups	Media Rules: defa Add Media Rules default-low-med default-low-med-enc default-high default-high default-high-enc avaya-low-med-enc	Filter By Device	defaults, Try cloning or ad (Media Anomaly N R R R R	ding a new rule in Aedia Silencing Audio Encrypti RTP Video Encrypti RTP Video Encrypti ZTP	Media QoS		Clone	
Session Policies TLS Management				Edit				

Figure 61 – Media Rule - Encryption

The Media Anomaly tab shows Media Anomaly Detection was disabled.

Media NAT Media	Encryption	edia Anomaly	Media Silencing	Media QoS
Media Anomaly Deter	ction			
		E	dit	

Figure 62 – Media Rule - Anomaly

The Media Silencing tab shows Media Silencing was disabled.

Media NAT	Media Encryption	Media Anomaly	Media Silencing	Media QoS	
Media Silen	ncing				
		E	dit		

Figure 63 – Media Rule - Silencing

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	56 of 108
SPOC 11/6/2014	©2014 Avaya Inc. All Rights Reserved.	VTCM63SM63SBCE

edia NAT Media Encryptic	n Media Anomaly Media Silencing Media QoS	
	Media QoS Reporting	
RTCP Enabled		
	Media QoS Marking	
Enabled		
QoS Type	DSCP	
	Audio QoS	
Audio DSCP	EF	
	Video QoS	
Video DSCP	EF	
	Edit	

The Media QoS settings are shown below.

Figure 64 – Media Rule - QoS

7.3.4. Create Security Rules

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

For the compliance test, the predefined **default-med** security rule (shown below) was used for both Session Manager and the Videotron server.

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

• Select the **default-med** rule to view.

Alarms Incidents Statis	stics Logs Diagnostics L	sers	Settings	Help	Log Out
Session Bord	ler Controller fo	or Enterprise		AV	AYA
Dashboard Administration Backup/Restore System Management Global Parameters Global Parameters Global Profiles SIP Cluster Domain Policies Application Rules Border Rules Media Rules	Security Rules: defa	It is not recommended to edit the defaults. Try cloning or adding a new rule instead. Authentication Compliance Fingerprint Scrubber Domain DoS Enabled No Edit		Clone	

Figure 65 – Security Rule

7.3.5. Create Signaling Rules

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

For the compliance test, the predefined **default** signaling rule (shown below) was used for both Session Manager and the Videotron server.

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

• Select the **default** rule to view.

Alarms Incidents Statistic	· · ·	Jsers					Settings	Help	Log Ou
Session Borde	er Controller fo	or Enterpris	se					A	ЛАУА
Dashboard Administration Backup/Restore System Management > Global Praneters > Global Profiles > SIR Cluster	Signaling Rules: de Add Signaling Rules default No-Content-Type-Ch	fault Filter By Device It is not recommended to General Requests	edit the default Responses	s, Try cloning or addin Request Headers	ig a new rule instead. Response Headers Inbound	Signaling QoS	UCID	Clone]
 SIP Cluster Domain Policies Application Rules Border Rules Border Rules Security Rules Signaling Rules Time of Day Rules End Point Policy Groups Session Policies 	Requests Allow Non-2XX Final Responses Allow Optional Request Headers Allow Optional Response Headers Allow			w					
		Requests Non-2XX Final Respo Optional Request Hea Optional Response He	ders	Outbound Allow Allow Allow Allow					
 TLS Management Device Specific Settings 		Enable Content-Type Action Exception List	Checks Allow	(Content-Type Policy Multipart Acti Exception Lis		w		
		Exception List			Exception Lis	st			

Figure 66 – Signaling Rule

The **Requests**, **Responses**, **Request Headers**, **Response Headers** and **UCID** tabs have no entries.

The **Signaling QoS** tab is shown below.

Alarms Incidents Statis	tics Logs Diagnostics I	Jsers					Settings	Help	Log Out
Session Bord	er Controller fo	or Enterp	rise					AV	/AYA
Dashboard Administration Backup/Restore System Management	Signaling Rules: de Add Signaling Rules	Filter By Device	✓ d to edit the defau	ts. Try cloning or addi	ng a new rule instead.		[Clone	
Global ParametersGlobal Profiles	default No-Content-Type-Ch	General Reques	ts Responses	Request Headers		Signaling QoS UC	CID		
 SIP Cluster Domain Policies Application Rules 		QoS Type DSCP		DS	SCP				
Border Rules Media Rules Security Rules		-			Edit				
Signaling Rules									

Figure 67 – Signaling Rule - QoS

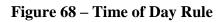
7.3.6. Create Time of Day Rules

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

For the compliance test, the predefined **default** Time of Day rule (shown below) was used for both Session Manager and the Videotron server.

From the menu on the left-hand side, select **Domain Policies** \rightarrow **Time of Day Rules**. Select the **default** rule to view.

Alarms Incidents Statisti		^{Users} or Enterpri	se		Setting	s Help	
Dashboard	Time of Day Rules						
Administration	Add	Filter By Device	\sim			Clone	
Backup/Restore	Time of Day Rules	It is not recommended.	to edit the defaults. Try cloning o	radding o now rule instead			
System Management	default	It is not recommended	to edit the defaults. Try clothing o	r adding a new rule instead.			
Global Parameters	delauit	Time of Day					
Global Profiles				Date			
SIP Cluster		Start Date	02/19/2007	End Date	Never		
 Domain Policies 				Line Date			
Application Rules				Time			
Border Rules		Start Time	12:00 AM	End Time	11:59 PM		
Media Rules							_
Security Rules				Recurrence			
Signaling Rules				This policy is applied every day.			
Time of Day Rules				Edit			
End Point Policy				free of the			



7.3.7. 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** \rightarrow **End Point Policy Groups**.

- Select Add
- Enter Group Name: SM63_SP3_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).

Session Borde	er Controller f	or En	terprise	е					A	VAYA
Dashboard	Policy Groups: SN	163_SP3	_PolicyG							ļ
Administration	Add	Filter By D	Device	\sim				Rename	Clone	Delete
Backup/Restore System Management	Showing page 1 of 2.				Click here to	add a descriptio	Π.			
Global Parameters	Policy > >> Groups				Hover over a rov	v to see its descri	iption.			
Global Profiles	default-low	Policy G	roup							
SIP Cluster	default-low-enc	i oney a						S	Summary	Add
Application Rules	default-med	Order	Application	Border	Media	Security	Signaling	Time of Day	y	
Border Rules	default-med-enc	1	default	default	default-low-med	default-med	default	default	Edit	Clone
Media Rules	default-high		- Antonia de la							
Security Rules Signaling Rules	default-high-enc									
Time of Day Rules	OCS-default-high									
End Point Policy	avaya-def-low-enc									
Groups	avaya-def-high-subs									
Session Policies TLS Management	avaya-def-high-server									

Figure 69 – Session Manager End Point Policy

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

- Select Add
- Enter Group Name: SP3_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).

Alarms Incidents Statistics	ELogs Diagnostics	Users					Setting	s Help	Log Out
Session Borde	r Controller f	or Enterpris	se					A	VAYA
Dashboard Administration Backup/Restore	Policy Groups: SP	P3_PolicyG Filter By Device	~				Rename	Clone	Delete
System Management	Showing page 1 of 2.			Click here to	add a descriptio	n.			
Global Parameters	Policy > >> Groups			Hover over a rov	v to see its descri	iption.			
 Global Profiles SIP Cluster 	default-low	Policy Group							
Domain Policies	default-low-enc						SI	ummary	Add
Application Rules	default-med	Order Application	n Border	Media	Security	Signaling	Time of Day	2	
Border Rules	default-med-enc	1 default	default	default-low-med	default-med	default	default	Edit	Clone
Media Rules	default-high								
Security Rules Signaling Rules	default-high-enc								
Time of Day Rules	OCS-default-high								
End Point Policy	avaya-def-low-enc								
Groups Session Policies	avaya-def-high-subs								
 TLS Management 	avaya-def-high-server								
 Device Specific Settings 	SM63_SP3_PolicyG								
	SP3_PolicyG								

Figure 70 – Videotron End Point Policy

7.3.8. Create Session Policy

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

- From the menu on the left-hand side, select **Domain Policies** → **Session Policies**. Select the **default** policy
 - Select Clone button
 - Enter Clone Name: SP3
 - Click **Finish** (not shown).
- Click **Edit** button on **Media** tab
 - Check Media Anchoring
 - Select **Finish** (not shown).

Alarms Incidents Statist	tics Logs Diagnostics Users	Settings Help Log Out
Session Bord	er Controller for Enterprise	AVAYA
Dashboard Administration	Session Policies: SP3 Add Filter By Device	Rename Clone Delete
Backup/Restore	Session Policies Click here to add a description.	
System Management Global Parameters Global Profiles SIP Cluster Domain Policies Application Rules Border Rules Media Rules	Gefault Codec Prioritization Media SP3 Media Anchoring Image: Codec Prioritization Media Forking Profile None Edit Edit	
Security Rules Signaling Rules Time of Day Rules End Point Policy Groups Session Policies		
TLS Management		



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**.

• Enter the **IP Address** and **Gateway Address** for both the Inside and the Outside interfaces:

IP Address for Inside interface: 10.10.98.13; Gateway: 10.10.98.1

IP Address for Outside interface: 10.10.98.111; Gateway: 10.10.98.97

- Select the physical interface used in the Interface column:
 - Inside Interface: A1
 - Outside Interface: B1

Alarms Incidents Statistic	s Logs Diagnostics	Users			Settings Help Log (
Session Borde	er Controller	for Enterprise			AVAY
Dashboard Administration Backup/Restore System Management > Global Parameters > Global Profiles > SIP Cluster > Domain Policies	Network Manag Devices SBCE62	Modifications or deletions of a can be issued from <u>System M</u> Changes will not take effect up	anagement. ntil the interface is updated.	require an application restart before t	
TLS Management		A1 Netmask 255.255.255.192	A2 Netmask	B1 Netmask B2 N 255.255.255.224	letmask
Device Specific Settings Network		Add			Save Clear
Management		IP Address	Public IP	Gateway	Interface
Media Interface		10.10.98.13		10.10.98.1	A1 Delete
Signaling Interface		10.10.98.111		10.10.98.97	B1 Delete
Signaling Forking		10.10.98.111		10.10.98.97	BI Delete
End Point Flows		10.10.98.21		10.10.98.1	A1 Delete
Session Flows		10.10.98.124		10.10.98.97	B1 Delete
Relay Services SNMP		10.10.30.124		[10.10.30.37	Delete
SNMP Syslog Management		10.10.98.99		135.10.98.97	B1 Delete

Figure 72 - Network Management

Solution & Interoperability Test Lab Application Notes ©2014 Avaya Inc. All Rights Reserved.

Select the **Interface Configuration** tab.

Toggle the state of the physical interfaces being used to **Enabled**.

Session Bord	er Controlle	r for Enterp	orise		AVA	ŊА
Dashboard Administration	Network Mana	agement: SBCE62	2			
Backup/Restore System Management > Global Parameters	Devices SBCE62	Network Configu	ration Interface Configuration	Administrative Status		1
Global Profiles		A1	Enable	ed	1	Toggle
SIP Cluster		A2	Disabl	led		Toggle
Domain Policies		B1	Enable	ed	13	Toggle
 TLS Management Device Specific Settings Network Management 		B2	Disabl	ed		Toggle

Figure 73 - Network Interface Status

7.4.2. Create Media Interfaces

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

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

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

		for Enterprise				,
Dashboard Administration	Media Interface	: SBCE62				
Backup/Restore						
System Management	Devices	Media Interface				
Global Parameters	SBCE62	Modifying or deleting an existing	media interface will require an application	restart before taking effect. Application	n restarts can	be
Global Profiles		issued from System Manageme				and the second
SIP Cluster		and the second se				Add
and the second se			Media IP			-
Domain Policies		Name		Port Range		
 Domain Policies TLS Management 		Name	10.10.98.13	Port Range 35000 - 40000	Edit	Delete
TLS Management		InsideMedia	10.10.98.13	35000 - 40000		
 TLS Management Device Specific Settings Network Management 		InsideMedia OutsideMedia	10.10.98.13 10.10.98.111	35000 - 40000 35000 - 40000	Edit	Delete
TLS Management Device Specific Settings		InsideMedia	10.10.98.13	35000 - 40000		Delete
TLS Management Device Specific Settings Network Management		InsideMedia OutsideMedia	10.10.98.13 10.10.98.111	35000 - 40000 35000 - 40000	Edit	Delete Delete
 TLS Management Device Specific Settings Network Management Media Interface 		InsideMedia OutsideMedia InsideMediaRW	10 10.98.13 10.10.98.111 10.10.98.21	35000 - 40000 35000 - 40000 35000 - 40000	Edit Edit	Delete Delete
 TLS Management Device Specific Settings Network Management Media Interface Signaling Interface 		InsideMedia OutsideMedia InsideMediaRW	10 10.98.13 10.10.98.111 10.10.98.21	35000 - 40000 35000 - 40000 35000 - 40000	Edit Edit	Delete Delete
 TLS Management Device Specific Settings Network Management Media Interface Signaling Interface Signaling Forking 		InsideMedia OutsideMedia InsideMediaRW	10 10.98.13 10.10.98.111 10.10.98.21	35000 - 40000 35000 - 40000 35000 - 40000	Edit Edit	Delete Delete
 TLS Management Device Specific Settings Network Management Media Interface Signaling Interface Signaling Forking End Point Flows 		InsideMedia OutsideMedia InsideMediaRW	10 10.98.13 10.10.98.111 10.10.98.21	35000 - 40000 35000 - 40000 35000 - 40000	Edit Edit	Delete Delete
 TLS Management Device Specific Settings Network Management Media Interface Signaling Interface Signaling Forking End Point Flows Session Flows 		InsideMedia OutsideMedia InsideMediaRW	10 10.98.13 10.10.98.111 10.10.98.21	35000 - 40000 35000 - 40000 35000 - 40000	Edit Edit	Delete Delete

Figure 74 - Media Interface

7.4.3. Create Signaling Interfaces

Signaling Interfaces define the type of signaling on the ports.

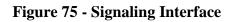
From the menu on the left-hand side, select **Device Specific Settings** \rightarrow **Signaling Interface**.

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

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

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

Session Borde	er Controller	for Enterpris	е					A	VAYA
Dashboard Administration Backup/Restore	Signaling Interf	-							
System Management	Devices	Signaling Interface							
Global Parameters	SBCE62								Add
Global Profiles		Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile		
SIP Cluster		InsideUDP	10.10.98.13		5060	<u></u>	None	Edit	Delete
Domain Policies		OutsideUDP	10.10.98.111		5060		None	Edit	Delete
 TLS Management Device Specific Settings 		InsideTCP	10.10.98.13	5060			None	Edit	Delete
Network Management		InsideTLS	10.10.98.13			5061	AvayaSBCServer	Edit	Delete
Media Interface		OutsideTCPTLS	10.10.98.111	5060	1.2223	5061	AvayaSBCServer	Edit	Delete
Signaling Interface		InsideTLSRW	10.10.98.21			5061	AvayaSBCServer	Edit	Delete
Signaling Forking End Point Flows		OutsideSIPRW	10.10.98.99	5060		5061	AvayaSBCServer	Edit	Delete



7.4.4. Configuration Server Flows

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

Create End Point Flows – SM63 Flow

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

- Select the Server Flows tab.
- Select Add, enter Flow Name: SM63 Flow
 - Server Configuration: SM63
 - URI Group: SP3
 - Transport: *
 - Remote Subnet: *
 - Received Interface: OutsideUDP
 - Signaling Interface: InsideUDP
 - Media Interface: InsideMedia
 - End Point Policy Group: SM63_SP3_PolicyG
 - Routing Profile: SM63_To_SP3
 - Topology Hiding Profile: SP3_To_SM63
 - Click **Finish** (not shown)

Alarms Incidents Statistics	Logs Diagnostics U	sers		Settings Help Log Out
Session Borde	r Controller fo	r Enterprise		Αναγα
Dashboard Administration Backup/Restore System Management > Global Parameters > Global Profiles	End Point Flows: SE Devices SBCE62	Subscriber Flows Server Flows		Add
 Global Profiles SIP Cluster Domain Policies TLS Management Device Specific Settings Network Management Media Interface Signaling Interface Signaling Forking End Point Flows Session Flows Relay Services SNMP Syslog Management Advanced Options Troubleshooting 		Flow Name Server Configuration URI Group Transport Remote Subnet Received Interface Signaling Interface Signaling Interface End Point Policy Group Routing Profile Topology Hiding Profile File Transfer Profile	Click here to add a row description Add Flow SM63 Flow SM63 V SP3 V * V (InsideUDP V InsideUDP V InsideUDP V SM63_SP3_PolicyG V SM63_SP3_PolicyG V SM63_To_SP3 V SP3_To_SM63 V Finish	X View Clone Edit Delete View Clone Edit Delete View Clone Edit Delete

Figure 76 - End Point Flow to Videotron

Create End Point Flows – Videotron Flow

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

- Select the **Server Flows** tab.
- Select Add, enter Flow Name: SP3 Flow
 - Server Configuration: SP3
 - URI Group: SP3
 - Transport: *
 - Remote Subnet: *
 - Received Interface: InsideUDP
 - Signaling Interface: OutsideUDP
 - Media Interface: OutsideMedia
 - End Point Policy Group: SP3_PolicyG
 - Routing Profile: SP3_To_SM63
 - Topology Hiding Profile: SM63_To_SP3
 - Click **Finish** (not shown)

Session Border	Controller fo	r Enterprise		AVAYA
Dashboard Administration Backup/Restore System Management • Global Parameters • Global Profiles • SIP Cluster • Domain Policies • TLS Management • Device Specific Settings • Network Management Media Interface • Signaling Interface • Signaling Interface	End Point Flows: SB	Subscriber Flows Server Flow Flow Name Server Configuration URI Group Transport Remote Subnet	Add X View Clone: Edit Delete	
Session Flows Relay Services SNMP Syslog Management Advanced Options In Troubleshooting		Received Interface Signaling Interface End Point Policy Group Routing Profile Topology Hiding Profile File Transfer Profile	InsideUDP V OutsideUDP V OutsideMedia V SP3_PolicyG V SP3_To_SM63 V SM63_to_SP3 V None V Finish	View Clone Edit Delete

Figure 77 - End Point Flow from Videotron

7.4.5. Create Session Flows

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

- Select **Device Specific Settings** from the menu on the left-hand side.
- Select the **Session Flows**.
- Select Add.
- Flow Name: SP3 URI Group#1: SP3 URI Group#2: SP3 Session Policy: SP3
- Select **Finish** (not shown).

Alarms Incidents Statistics	s Logs Diagnostics	Users						Se	ettings	Help	Log Ou
Session Borde	er Controller	for Ent	terprise							AV	ΆYA
Dashboard Administration Backup/Restore	Session Flows: S										
System Management Global Parameters 	Devices SBCE62	Session F								[Add
 Global Profiles SIP Cluster 				Hove	er over a row to see	ts descript	ion.				
 Domain Policies 		Priority	Flow Name	URI Group #1	URI Group #2	Subnet #1	Subnet #2	Session Policy			
TLS Management		1	SP3	SP3	SP3	#1	#2	SP3	Clone	Edit	Delete
 Device Specific Settings 		1	5P3	5P3	943			5P3	Cione	Eair	Delete
Network Management											
Media Interface											
Signaling Interface Signaling Forking											
End Point Flows											
Relay Services											



8. Videotron SIP Trunking Configuration

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

The configuration between Videotron and the enterprise is a static configuration.

9. Verification Steps

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

Verification Steps:

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

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	71 of 108
SPOC 11/6/2014	©2014 Avaya Inc. All Rights Reserved.	VTCM63SM63SBCE

Troubleshooting:

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.

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** \rightarrow **Session Manager** \rightarrow **System Tools** \rightarrow **Call Routing Test**. Enter the requested data to run the test.

traceSM -x – Session Manager command line tool for traffic analysis. Log into the Session Manager management interface to run this command.

10. Conclusion

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

11. References

This section references the documentation relevant to these Application Notes.

Product documentation for Avaya, including the following, is available at: <u>http://support.avaya.com/</u>

Avaya Aura[®] Session Manager/System Manager

- [1] Administering Avaya Aura[®] Session Manager, Release 6.3, Issue 2, June 2013
- [2] Maintaining and Troubleshooting Avaya Aura[®] Session Manager, Release 6.3, Issue 2, May 2013
- [3] Administering Avaya Aura[®] System Manager, Release 6.3, Issue 2, May 2013

Avaya Aura[®] Communication Manager

- [4] Administering Avaya Aura[®] Communication Manager, Document ID 03-300509, Release 6.3, Issue 8, May 2013
- [5] Programming Call Vectoring Features in Avaya Aura[®] Call Center Elite, Release 6.3, Issue 1, May 2013

Avaya one-X[®] IP Phones

- [6] Avaya one-X[®] Deskphone SIP 9621G/9641G User Guide for 9600 Series IP Telephones, Document ID 16-603596, Issue 1, August 2012
- [7] Avaya one-X[®] Deskphone H.323 9608 and 9611G User Guide, Document ID 16-603593, *Issue 3, February 2012*
- [8] Avaya one-X[®] Deskphone SIP for 9640/9640G IP Telephone User Guide, Document ID 16-602403, June 2013
- [9] Avaya one-X[®] Deskphone H.323 for 9630 and 9630G IP Deskphone User, Document ID 16-300700, June 2013
- [10] Using Avaya one- $X^{\text{®}}$ Communicator Release 6.1, October 2011
- Using Avaya Flare[®] Experience for Windows, Document ID 18-604158, Release 1.1, Issue 2, February 2013

Avaya Aura[®] Messaging

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

Avaya Session Border Controller for Enterprise

Product services for Avaya SBCE may be found at: <u>http://www.sipera.com/products-services/esbc</u>

- [14] Avaya Session Border Controller for Enterprise Overview and Specification, Issue 2, December 2013
- [15] Administering Avaya Session Border Controller for Enterprise, Release 6.2, Issue 2, January 2014
- [16] Configuring the Avaya Session Border Controller for IP Office Remote Workers, September 2013

Product documentation for Avaya products may be found at: <u>http://support.avaya.com</u>. Additional IP Office documentation can be found at: <u>http://marketingtools.avaya.com/knowledgebase/ipoffice/general/rss2html.php?XMLFILE=man</u> <u>uals.xml&TEMPLATE=pdf_feed_template.html</u>

IETF (Internet Engineering Task Force) SIP Standard Specifications

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

Product documentation for Videotron SIP Trunk may be found at: <u>http://affaires.videotron.com/web/ge/telephonie/sip-pbx/index-en.jsp</u>

12. Appendix A – Remote Worker Configuration on the Avaya Session Border Controller for Enterprise (Avaya SBCE)

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 Videotron SIP Trunking 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 Flare[®] Experience for Windows SIP softphone. Avaya 96x1 SIP Deskphones support SRTP, while Avaya one-X[®] Communicator and Avaya Flare[®] Experience for Windows softphones support RTP.

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.

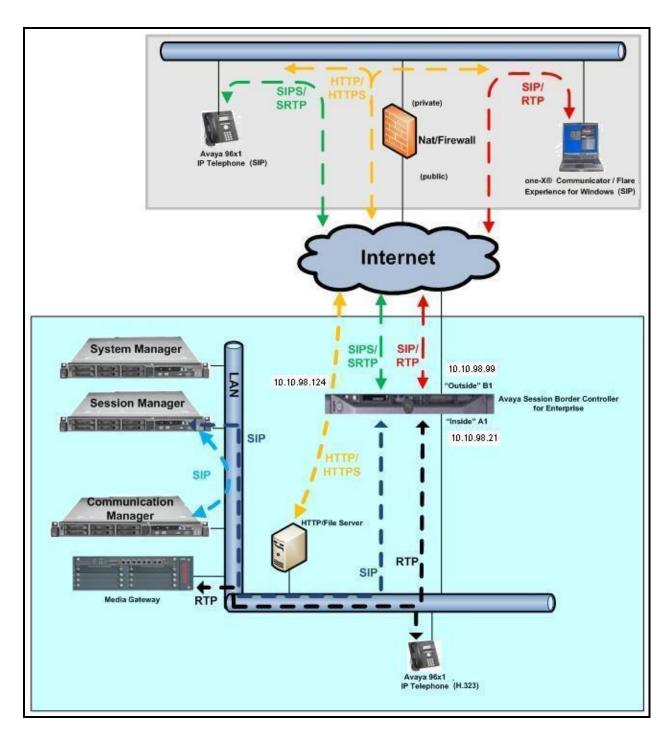


Figure 79: Avaya IP Telephony Network and Videotron SIP Trunking for Remote Worker

12.1. Network Management

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 Videotron (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 Videotron (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.

Alarms Incidents Statistic		Users			Settings	
Dashboard Administration	Network Manage	•				Every
Backup/Restore System Management	Devices SBCE62		<u>lanagement</u>	ta require an application restart before ta	aking effect. App etmask	plication restarts
TLS Management Device Specific Settings Network		255.255.255.192 Add		255.255.255.224	eunask	Save Clear
Management		IP Address	Public IP	Gateway	Interf	ace
Media Interface		10.10.98.13		10.10.98.1	A1	Delete
Signaling Interface Signaling Forking		10.10.98.111		10.10.98.97	B1	Delete
End Point Flows Session Flows		10.10.98.21		10.10.98.1	[A1	Delete
Relay Services		10.10.98.124		10.10.98.97	B1	Delete
SNMP		10.10.98.99		135.10.98.97	B1	Delete

Figure 80 - Network Management

HV; Reviewed: SPOC 11/6/2014

On the **Interface Configuration** tab, verify that Interfaces **A1** and **B1** are both set to **Enabled** as previously configured for the Videotron SIP Trunking access in **Section 7.4.1**.

Session Borde	er Controller	for Enterprise		Settings Help Log Ou
Dashboard Administration	Network Mana	gement: SBCE62		
Backup/Restore System Management Global Parameters	Devices SBCE62	Network Configuration Interface	Configuration	ative Status
Global Profiles		A1	Enabled	Toggle
SIP Cluster		A2	Disabled	Toggle
Domain Policies		B1	Enabled	Toggle
 TLS Management Device Specific Settings Network Management 		B2	Disabled	Toggle

Figure 81 - Network Interface Status

12.2. Media Interface

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

- Select Add
 - Name: InsideMediaRW Media IP: 10.10.98.21 (Internal IP Address toward Session Manager) Port Range: 35000 - 40000 Click Finish (not shown)
- Select Add
 - Name: OutsideMediaRW
 - Media IP: 10.10.98.99 (External IP Address toward Remote Worker phones)
 - Port Range: 35000 40000
 - Click **Finish** (not shown).

Session Bord	er Controller	for Enterprise			A	VAY
Dashboard Administration Backup/Restore	Media Interface:	SBCE62				
System Management Global Parameters Global Profiles SIP Cluster	SBCE62	Modifying or deleting an existing issued from <u>System Managemen</u>	media interface will require an application t .	n restart before taking effect. Application	restarts can	be Add
 Global Parameters Global Profiles SIP Cluster Domain Policies 				restart before taking effect. Application Port Range	restarts can	
 Global Parameters Global Profiles SIP Cluster Domain Policies TLS Management 		issued from <u>System Managemen</u>	L		restarts can Edit	
Global Parameters Global Profiles SIP Cluster Domain Policies TLS Management Device Specific Settings		issued from <u>System Managemen</u> Name	t. Media IP	Port Range		Add
 Global Parameters Global Profiles SIP Cluster Domain Policies TLS Management 		issued from <u>System Managemen</u> Name InsideMedia	t. Media IP 10.10.98.13	Port Range 35000 - 40000	Edit	Add Delete

Figure 82 - Media Interface

Note: Media Interface **OutsideMediaRW** is used in the Remote Worker Subscriber Flow (**Section 12.14.1**), and Media Interface **InsideMediaRW** is used in the Remote Worker Server Flow (**Section 0.0.0**).

12.3. Signaling Interface

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. Interface OutsideSIPRW supports TCP and TLS, while interface InsideTLSRW supports TLS only.

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

- Signaling IP = 10.10.98.99
- TCP Port = 5060
- TLS Port = 5061
- Select **TLS Profile** as **AvayaSBCServer** from the drop down menu.Click on **Finish** (not shown).

Repeat step 1 to create Signaling Interface **InsideTLSRW** using the parameters:

- Signaling IP = 10.10.98.21
- TLS Port = 5061
- Select **TLS Profile** as **AvayaSBCServer** from the drop down menu.Click on **Finish** (not shown).

Signaling Interface **OutsideSIPRW** is used in the three Subscriber Flows (**Section 12.14.1**), and in the Remote Worker Server Flow (**Section 0.0.0**). Signaling Interface **InsideTLSRW** is used in the Remote Worker Server Flow (**Section 0.0.0**).

Alarms Incidents Statistic	s Logs Diagnostics	Users					Settings	Help	Log O
Session Borde	r Controller	for Enterpris	e					A	/AY/
Dashboard Administration Backup/Restore	Signaling Interfa								
System Management	Devices SBCE62	Signaling Interface							Add
 Global Profiles SIP Cluster 		Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile		
Domain Policies		InsideUDP OutsideUDP	10.10.98.13 10.10.98.111		5060 5060		None None	Edit Edit	Delete Delete
 TLS Management Device Specific Settings 		InsideTLSRW	10.10.98.21			5061	AvayaSBCServer	Edit	Delete
Network Management Media Interface Signaling Interface Signaling Forking End Point Flows		OutsideSIPRW	10.10.98.99	5060	0.000	5061	AvayaSBCServer	Edit	Delete

Figure 83 - Signaling Interface

HV; Reviewed: SPOC 11/6/2014

12.4. Create Remote Worker URI group

The URI-Group named **RemoteWorker** was used to match the "From" header in a SIP call dialog received from Remote Worker SIP phone. If there is a match, the Avaya SBCE will apply the appropriate Routing profile (see **Section 12.5**), Subscriber Flow (see **Section 12.14.1**), and Remote Worker Server Flow (see **Section 0.0.0**) to route the calls to the right destinations.

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

Enter Group Name: **RemoteWorker**. Edit the URI Type: **Regular Expression**. **Add** URI: **.*bvwdev7\.com** (Enterprise domain) Click **Finish**.

Alarms Incidents Statistics	s Logs Diagnostics U	sers	Settings Help Log Out
Session Borde	r Controller fo	or Enterprise	AVAYA
Dashboard Administration Backup/Restore	URI Groups: Remo		Rename Delete
System Management Global Parameters Global Profiles 	RemoteWorker SP3	Click here to add a description.	Add
Domain DoS Fingerprint Server Interworking Phone Interworking		URI Listing Add URI	X Edit Delete
Media Forking Routing Server Configuration		WARNING: Invalid or incorrectly entered regular expressions may cause unexpected results Note: This regular expression is case-insensitive. Ex: [0-9][3,5]\user@domain\.com, (simple advanced)\-user[A-Z][3]@.*	
Topology Hiding Signaling Manipulation URI Groups SIP Cluster		C Plain URI Type C Dial Plan © Regular Expression	
 Domain Policies TLS Management Device Specific Settings 		URI *bvwdev7.com	

Figure 84 – Remote Worker URI Group

12.5. Routing Profile

Note – **10.33.10.26** is the IP address of Session Manager in the reference configuration (see **Section 7.2.7**).

The Routing Profile To_SM_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_SM_RW. URI Group: RemoteWorker.

Next Hop Server 1: 10.33.10.26 (IP address of Session Manager).

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	80 of 108
SPOC 11/6/2014	©2014 Avaya Inc. All Rights Reserved.	VTCM63SM63SBCE

Check Routing Priority based on Next Hop Server. Outgoing Transport as TLS.Click Finish.

The Routing Profile To_SM_RW is used in the Subscriber Flows (Section 12.14.1).

Alarms Incidents Statistics	i Logs Diagnostics U	sers		Setting	s Help Log Out
Session Borde	r Controller fo	or Enterprise			AVAYA
Dashboard Administration Backup/Restore System Management Global Parameters Global Profiles Domain DoS	Routing Profiles: To Add Routing Profiles default To_SM_RW SM63_To_SP3	_SM_RW Routing Profile Priority URI Group	Click here to add a description. Next Hop Server 1	Rename Next Hop Server 2	Cione Delete
Fingerprint Server Interworking Phone Interworking Media Forking Routing Server Configuration Topology Hiding	SP3_To_SM63	Each URI group may only be used URI Group Next Hop Server 1 IP. IP Port, Domain, Port	Edit Routing Rule	X	View Edit
Signaling Manipulation URI Groups SIP Cluster Domain Policies TLS Management Device Specific Settings		Next Hop Server 2 IP. IP.Port. Domain. or Domain.Port Routing Priority based on Next Hop Server Use Next Hop for In Dialog Messages		-	
		Ignore Route Header for Messages Outside Dialog NAPTR SRV Outgoing Transport		-	
			Finish		

Figure 85 – Remote Worker Routing to SM

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

- Verify the **NAPTR** and **SRV** boxes are checked.
- Use defaults for all remaining parameters.Click **Finish** (not shown).

The Routing Profile **default_RW** is used in the Remote Worker Server Flow in **Section 0.0.0**.

Alarms Incidents Statistics				Setting	is Help Log Out
Session Borde	r Controller for	r Enterprise			AVAYA
Dashboard Administration Backup/Restore System Management	Routing Profiles: defa	ult_RW	Click here to add a description.	Rename	Clone Delete
Global Parameters Global Profiles Domain DoS	default To_SM_RW default_RW	Routing Profile			Add
Fingerprint Server Interworking Phone Interworking	SM63_To_SP3 SP3_To_SM63	Priority URI Group	Next Hop Server 1 Edit Routing Rule Lance per Routing Profile.	Next Hop Server 2	View Edit
Media Forking Routing Server Configuration Topology Hiding Signaling Manipulation URI Groups SIP Cluster Domain Policies TLS Management Device Specific Settings		URI Group Next Hop Server 1 IP, IP: Port, Domain, or Domain:Port Next Hop Server 2 IP, IP: Port, Domain, Port Routing Priority based on Next Hop Server Use Next Hop for In Dialog Messages Ignore Route Header for Messages Outside Dialog	Next Hop Routing		
		NAPTR SRV Outgoing Transport	✓ ○ TLS ○ TCP ○ UDP Finish		

Figure 86 – Remote Worker Default Routing

12.6. Configure Server Interworking Profile - Avaya site

From the menu on the left-hand side, select **Global Profiles** → **Server Interworking** Select Profile name as **SM63**

On the **Advanced** tab, click **Edit** button, verify that **Topology Hiding: Change Call-ID** must be **No** and **Avaya extensions** should be **Yes**. Otherwise, calls to Remote Worker will fail.

Click **Finish** (not shown).

Session Borde	r Controller f	or Enterprise	AVAYA
Dashboard Administration Backup/Restore System Management Global Parameters Global Parameters Global Profiles Domain DoS Fingerprint Server Interworking Media Forking Routing Server Configuration Topology Hiding Signaling Manipulation URI Groups SIP Cluster Domain Policies SIP Cluster Domain Policies TLS Management Device Specific Settings	Interworking Profile Add Interworking Profiles cs2100 avaya-ru OCS-Edge-Server cisco-ccm cups OCS-FrontEnd-Server SP3 SM63	es: SM63	Rename Clone Delete a description. Advanced

Figure 87 – Server Interworking for Remote Worker

12.7. Server Configuration

Note - 10.33.10.26 is the IP address of Session Manager in the reference configuration (see Section 7.2.7).

The following screens show the **Server Configuration** for the Profile **SM63** created previously for SIP Trunking with Videotron in **Section 7.2.7** for Session Manager. That configuration includes UDP (5060) transport protocol. TCP and TLS transport protocols are also added here for the Remote Worker configuration.

From the menu on the left-hand side, select **Global Profiles** \rightarrow **Server Configuration** Select **Server Profile** as **SM63**, on **General** tab, click **Edit** button and enter the following:

- Supported Transports: TCP, TCP Port: 5060
- Supported Transports: TLS, TLS Port: 5061
- Click on **Finish** (not shown).

Session Borde	r Controller f	for Enterprise		AVAYA
Dashboard Administration Backup/Restore	Server Configurat Add Server Profiles		anced	Rename Clone Delete
System Management Global Parameters Global Profiles	SM63 SP3	Server Type IP Addresses / FQDNs	Call Server 10.33.10.26	
Domain DoS Fingerprint Server Interworking		Supported Transports TCP Port	TCP, UDP, TLS	
Phone Interworking Media Forking		UDP Port TLS Port	5060	
Routing Server Configuration Topology Hiding			Edit	

Figure 88 – Server Configuration for Remote Worker

On Advanced tab, click Edit button and enter the following:

- Select TLS Client Profile as AvayaSBCClient.
- Click on **Finish** (not shown).

This Server Configuration is used by the Server Flows defined in Section 12.14.2.

Session Borde	AVAYA			
Dashboard Administration	Server Configuratio	on: SM63		
Backup/Restore	Add Server Profiles	General Authentication Heartbeat	vanced	Rename Clone Delete
System Management Global Parameters	SM63	Enable DoS Protection		
Global Profiles	SP3	Enable Grooming		
Fingerprint		Interworking Profile	SM63	
Server Interworking		TLS Client Profile	AvayaSBCClient	
Phone Interworking		Signaling Manipulation Script	None	
Media Forking Routing		TCP Connection Type	SUBID	
Server Configuration		UDP Connection Type	SUBID	
Topology Hiding		TLS Connection Type	SUBID	
Signaling Manipulation URI Groups			Edit	

Figure 89 – Advanced Server Configuration for Remote Worker

12.8. User Agents

User Agents were created for each type of endpoint tested. This allows for different policies to be applied based on the type of device. For example, Avaya one-X[®] 96x1Deskphones will use TLS and SRTP while one-X[®] Communicator and Avaya Flare[®] Experience for Windows will use TCP and RTP.

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	84 of 108
SPOC 11/6/2014	©2014 Avaya Inc. All Rights Reserved.	VTCM63SM63SBCE

<u>.</u>			
Session Bord	ler Controller for En	terprise	AVA
Dashboard	User Agents		
Administration	_		
Backup/Restore			
System Management	User Agents		
 Global Parameters 			Ad
	Name	Regular Expression	_
RADIUS			
RADIUS DoS / DDoS	one-X Communicator	Avaya one-X Communicator.*	Edit Dele
		· · ·	Edit Dele

Figure 90 – User Agents for Remote Worker

The following abridged output of traceSM shows the details of an INVITE from an Avaya one-X Deskphone. The **User-Agent** shown in this trace will match User Agent **one-X Deskphone** shown above with a **Regular Expression** of "**Avaya one-X Deskphone.***". In this expression, "**.***" will match any software version listed after the user agent name.

INVITE sip:8001@bvwdev7.com SIP/2.0
From: sip:8010@bvwdev7.com;tag=-59f03c7f529fb7c152aa3fd4_F0950710.10.98.136
To: sip:8001@bvwdev7.com
CSeq: 24 INVITE
Call-ID: 18 a7e80-49279ea452aa365c I@10.33.5.58
Contact: <sip:8010@10.10.98.21:5061;transport=tls;subid_ipcs=592904751></sip:8010@10.10.98.21:5061;transport=tls;subid_ipcs=592904751>
Record-Route: <sip:10.10.98.21:5061;ipcs-line=3472;lr;transport=tls></sip:10.10.98.21:5061;ipcs-line=3472;lr;transport=tls>
Record-Route: <sip:10.10.98.99:5061;ipcs-line=3472;lr;transport=tls></sip:10.10.98.99:5061;ipcs-line=3472;lr;transport=tls>
Allow:
INVITE,CANCEL,BYE,ACK,SUBSCRIBE,NOTIFY,MESSAGE,INFO,PUBLISH,REFER,UPDATE,PRACK
Supported: eventlist, 100rel, replaces
User-Agent: Avaya one-X Deskphone
Max-Forwards: 69
Via: SIP/2.0/TLS 10.10.98.21:5061;branch=z9hG4bK-s1632-001362762279-1s1632-
Via: SIP/2.0/TLS 10.10.98.136:5061;branch=z9hG4bK18_a7e80-312c149e52aa3fe8_I09507
Accept-Language: en
Content-Type: application/sdp
Content-Length: 340

Figure 91 – Output of trace for User Agent

The three User Agents are defined in their associated Subscriber Flows in Section 12.14.1.

12.9. Relay Services

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.

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	85 of 108
SPOC 11/6/2014	©2014 Avaya Inc. All Rights Reserved.	VTCM63SM63SBCE

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

- Set the **Remote Domain** to the domain, **bvwdev7.com**, previously specified for SIP Trunking with Videotron in Communications Manager (**Section 5.5**) and in Session Manager (**Section 6.2**).
- Set the **Remote IP:Port** to the IP address of the enterprise file server (e.g., **10.10.98.60:80**) used to provide the firmware updates and configuration data for the Remote Worker endpoints.
- Set the **Remote Transport** to **TCP**.
- Set the **Published Domain** to **bvwdev7.com**.
- Set Listen IP:Port to the IP address of the Avaya SBCE's external IP address designated for file transfers (10.10.98.124:80).
- Set the **Connect IP** to the internal IP address of the Avaya SBCE used for Remote Worker (10.10.98.21).
- Set the Listen Transport to TCP.
- Click on **Finish** (not shown).

Alarms Incidents Statistic:	s Logs Diagnostics	Jsers							Settings	Help	Log Out
Session Borde	r Controller f	or Enter	prise							A	/AYA
Dashboard Administration Backup/Restore System Management Global Parameters	Relay Services: S	Application Re	lay File Transf	er							Add
 Global Profiles SIP Cluster Domain Policies TLS Management 		Remote Domain bvwdev7.com	Remote IP:Port	Remote Transport TCP	Published Domain bwwdev7.com	Listen IP:Port 10.10.98.124:80	Listen Transport TCP	Connect IP 10.10.98.21	Whitelist Flows	Edit	Delete
 Device Specific Settings Network Management Media Interface Signaling Interface Signaling Forking End Point Flows Session Flows Relay Services 											

Figure 92 – Relay Services Setup

12.10. Cluster Proxy

A **Cluster Proxy** is defined for Personal Profile Manager (PPM) data and Presence services between the Remote Worker endpoints and Session Manager. The following screen shows the cluster proxy **RW** created in the sample configuration. This enables the remote Avaya SIP

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	86 of 108
SPOC 11/6/2014	©2014 Avaya Inc. All Rights Reserved.	VTCM63SM63SBCE

endpoints to send and receive PPM information to and from Session Manager via the Avaya SBCE.

Note - A Presence Services server was not part of the reference configuration. Therefore, configuration of the Cluster Proxy for use with Presence is not shown.

From the menu on the left-hand side, select SIP Cluster \rightarrow Cluster Proxy

- Click on the **Add** button and enter the following:
- Enter a name (e.g., **RW**), and click on **Next** (not shown). Note that the **Call Server Type** field will default to **Avaya**.
- In the **Domain Name** field, enter the domain **bvwdev7.com**.
- In the **Configuration Update Interval** field enter **15 minute**(s).
- Click on Next (not shown) and the Primary Device window will open (not shown).

Alarms Incidents Statistic	s Logs Diagnostics U	sers		Settings Help Log Out
Session Borde	er Controller fo	or Enterprise		Αναγα
Dashboard Administration Backup/Restore System Management	Cluster Proxy: RW Add Cluster Proxies		tiary	Delete
 Global Parameters 	RW		Cluster Information	
 Global Profiles SIP Cluster 		Call Server Type	Avaya	
Cluster Proxy			Security Information	
Domain Policies		Secure Mode	Disabled	
TLS Management			Miscellaneous Information	
Device Specific Settings		Domain Name	bvwdev7.com	
		Configuration Update Interval	15 minute(s)	
			Edit	

Figure 93 – Cluster Proxy Setup

- In the **Device Configuration** section, PPM traffic received on **Device IP** (B1) will be routed to the **Configuration Server Client Address** (A1). Enter the following:
 - In the **Device Name** field, enter **SBCE62**
 - In the **Device IP** field, enter **10.10.98.99** (B1).
 - In the **Configuration Server Client Address** field enter **10.10.98.21** (A1).
 - Click On Next to open the Configuration Servers window (not shown).
- In the **Configuration Servers** section, HTTP traffic is defined. The **Real Server IP** field is not used for PPM, so any IP address can be entered, (e.g., **1.2.3.4**). This enables the remote Avaya SIP endpoints to send and receive PPM information to and from Session Manager via the Avaya SBCE. Enter the following:
 - In the Server Type field, select HTTP Server from the drop down menu.
 - In the **Real Server Type** field, select **HTTP** from the drop down menu.
 - Do not check **Relay** or **Rewrite URL**.

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	87 of 108
SPOC 11/6/2014	©2014 Avaya Inc. All Rights Reserved.	VTCM63SM63SBCE

- In the **Port** field enter **80**.
- In the **Real Server IP** field enter **1.2.3.4**.
- Click on **Next** to open the **Signaling Servers** window (not shown).
- In the **Signaling Servers** section, enter the following:

In the **Server Configuration Profile** field, select **SM63** (see **Section 12.7**) from the drop down menu.

In the **Endpoint Signaling Interface** field, select **OutsideSIPRW** (see Section 12.3) from the drop down menu.

In the **Session Policy Group** field, use the **default** value. Click on **Finish** (not shown).

Alarms Incidents Statistic	s Logs Diagnostics U	sers								Settings He	lp Log Out
Session Borde	er Controller fo	or Ent	erpri	se						4	VAYA
Dashboard Administration Backup/Restore System Management	Cluster Proxy: RW Add Cluster Proxies	General	Primary	Secondary	/ Tertiary						Delete
Global Parameters Global Profiles	RW	Device	Informatio	on —		SBCE62					
 Global Profiles SIP Cluster Cluster Proxy 		Devi	ice IP	erver Client Ad	ldress	10.10.98.9					
 Domain Policies TLS Management Device Specific Settings 			1678			E	Edit				
Device operand countyp		Config	uration Se	rvers —							Add
			Туре	Real Type	Port	Real IP	Real Port	Relay Mode	Rewrite URL	Server TLS Profile	
		HTTP S	erver	HTTP	80	1.2.3.4	80	No	(***		Edit
		- Signal	ing Server	s ———							Add
		SM63	Gerver Config	guration Profile		End Point Signa ideSIPRW	aling Interface	defaul		olicy Group	Edit

Figure 94 – Cluster Proxy Setup - Primary

12.11. Application Rules

The following section describes two **Application Rules**; rule **default**, (previously used for SIP Trunking with Videotron in **Section 7.3.1**), and rule **RemoteWorker_AR**. In a typical customer installation, set the **Maximum Concurrent Sessions** for the **Voice** application to a value slightly larger than the licensed sessions.

As described above the **default** rule was previously used in **Section 7.3.1**, and is shown here for completeness.

Alarms Incidents Statisti	cs Logs Diagnostics	Users				Settings	Help Log O
Session Borde	er Controller fo	or Enterprise					AVAYA
Dashboard Administration	Application Rules:	default					Clone
Backup/Restore System Management ≻ Global Parameters	Application Rules default default-trunk	It is not recommended to edit the defaults: Try Application Rule	cloning or adding	j a nev	v rule instead.		
 Global Profiles SIP Cluster 	default-subscriber-low	Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sess	sions Per Endpoint
Domain Policies	default-subscriber-high	Audio			2000	10	
Application Rules	default-server-low	Video					
Border Rules Media Rules	default-server-high	IM					
Security Rules				Misce	llaneous		1
Signaling Rules		CDR Support	Non	е			
Time of Day Rules		RTCP Keep-Alive	No				
End Point Policy Groups					Edit		
Session Policies		L		251			

Figure 95 – Default Application Rule

To create the **RemoteWorker_AR** rule, from the menu on the left-hand side, select **Domain Policies** \rightarrow **Application Rules**. Select **Add** button and enter the following:

- Enter a name (e.g., **RemoteWorker_AR**), and click on **Next** (not shown).
- 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).

а : в I	0 (11)	E 1 - 1				•	
Session Bord	er Controller f	or Enterprise					AVAYA
Dashboard	Application Rules	: RemoteWorker_AR					
Administration	Add	Filter By Device				Rename	Clone Delete
Backup/Restore System Management	Application Rules		Click he	ere to	add a description.		
Global Parameters	default	Application Rule					
Global Profiles	default-trunk	Application T	voe In	Out	Maximum Concurrent Ses	cione Maximum Soco	ions Per Endpoint
SIP Cluster	default-subscriber-low	Voice	ype III	V	2000	2000	ions i el chapolite
Domain Policies Application Rules	default-subscriber-high		O Read IN		2000	2000	
Border Rules	default-server-low	Video					
Media Rules	default-server-high	IM		Γ			
Security Rules	RemoteWorker AR			Minor	ellaneous		
Signaling Rules	Remotevorker_AR	CDR Support	None		ellaneous		
Time of Day Rules		1993		5			
End Point Policy		RTCP Keep-Alive	No				
Groups					Edit		
Session Policies							

Figure 96 – Remote Worker Application Rule

The rule **RemoteWorker_AR** is assigned to the End Point Policy Groups in Section 12.13.

12.12. Media Rules

The following section describes two **Media Rules**; new rule **default_sRTP_RW** (cloned from the **default-low-med-enc** rule), and the existing rule **default** (previously used for SIP Trunking with Videotron in **Section 7.3.3**). Note that both rules have **Interworking** checked. Based on how calls are routed through Avaya SBCE, this will convert SRTP media to RTP and vice versa. In the sample configuration, Avaya SBCE will convert the SRTP media stream from remote Avaya 96x1 SIP Telephones to RTP towards the enterprise and also towards remote endpoints using TCP. Avaya SBCE will also convert RTP traffic from calls originating from Session Manager to SRTP towards Avaya 96x1 SIP Telephones using TLS through the external IP interface.

As described above the **default** rule was previously used for Videotron SIP Trunking in **Section 7.3.3**, and is shown here for completeness.

Session Bord	er Controller f	r Enterprise	AVAYA
Dashboard Administration Backup/Restore System Management	Media Rules: defau Add Media Rules	t-low-med Filter By Device If is not recommended to edit the defaults. Try cloning or adding a new rule inst	Clone
 Global Parameters Global Profiles SIP Cluster 	default-low-med default-low-med-enc default-high	Media NAT Media Encryption Media Anomaly Media Silencing Media NAT Learn Media IP dyna	Media QoS amically
Domain Policies Application Rules Border Rules Media Rules Security Rules	default-high-enc avaya-low-med-enc	Edit	

Figure 97–Default-Low-Med Media Rule

To create the new **default_sRTP_RW** rule, select the **default-low-med-enc** rule, and then click on **Clone**. Enter the following:

- Enter a name (e.g., **default_sRTP_RW**), and click on **Next** (not shown).
- The **Media Nat** window (**Media Nat** tab) will open (not shown). Use the default values and select **Next**.
- In the **Media Rule** window (**Media Encryption** tab), enter the following values:
 - Audio Encryption From the drop down menu, set **Preferred Formats** to **SRTP_AES_CM_128_HMAC_SHA1_80**.
 - 1. Uncheck Encrypted RTCP.
 - 2. Check **Interworking**
 - Video Encryption
 - 1. Set **Preferred Formats** to **RTP** from the drop down menu.
 - 2. Check Interworking
 - Miscellaneous

Uncheck Capability Negotiation

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	90 of 108
SPOC 11/6/2014	©2014 Avaya Inc. All Rights Reserved.	VTCM63SM63SBCE

- Select Next.

Session Borde	r Controller f	or Enternrise		A\/A\//
Session Dorde	ound one in	or Enterprise		FIVELYE
Dashboard	Media Rules: defa	ault sRTP RW		
Administration	Add	Filter By Device		Rename Clone Delete
Backup/Restore	Media Rules		Of the second se	
System Management	default-low-med		Click here to add a description.	
Global Parameters	default-low-med	Media NAT Media Encryption	Media Anomaly Media Silencing Media QoS	
Global Profiles	default-low-med-enc		Audio Encryption	
SIP Cluster	default-high	Preferred Formats	SRTP_AES_CM_128_HMAC_SHA1_80	2. 2
Domain Policies	default-high-enc			
Application Rules	Sector States	Encrypted RTCP		
Border Rules	avaya-low-med-enc	Interworking	<u>र</u>	
Media Rules	default_sRTP_RW			
Security Rules			Video Encryption	
Signaling Rules		Preferred Formats	RTP	
Time of Day Rules		Interworking	N	
End Point Policy		interworking		
Groups			Miscellaneous	
Session Policies		Capability Negotiation	F	
TLS Management		Capability Negotiation	1	

Figure 98 – Default SRTP Media Rule for Remote Worker

• On Media Anomaly tab, uncheck Media Anomaly Detection. Click Next.

Alarms Incidents Statisti	cs Logs Diagnostics U	Jsers	Settings Help Log Out
Session Borde	er Controller f	or Enterprise	AVAYA
Dashboard Administration	Media Rules: defa	Ruit_SRTP_RW	Rename Clone Delete
Backup/Restore	Media Rules		
System Management Global Parameters Global Profiles SIP Cluster Dormain Policies Application Rules 	default-low-med default-low-med-enc default-high default-high-	Click here to add a description. Media NAT Media Encryption Media Anomaly Media Silencing Media QoS Media Anomaly Detection Edit	
Border Rules Media Rules Security Rules Signaling Rules Time of Day Rules	avaya-low-med-enc default_sRTP_RW		
End Point Policy			

Figure 99 – Default SRTP Media Rule for Remote Worker – Media Anomaly

• On Media Silencing tab, verify Media Silencing is unchecked. Click Next.

Alarms Incidents Statist	ics Logs Diagnostics U	Jsers	Settings Help Log Out
Session Bord	er Controller f	or Enterprise	AVAYA
Dashboard Administration	Media Rules: defa	Filter By Device	Rename Clone Delete
Backup/Restore System Management Global Parameters	Media Rules default-low-med	Click here to add a description.	
 Global Parameters Global Profiles SIP Cluster 	default-low-med-enc	Media NAT Media Encryption Media Anomaly Media Silencing Media QoS	
Domain Policies Application Rules	default-high default-high-enc	Edit	1
Border Rules	avaya-low-med-enc		
Security Rules Signaling Rules			
Time of Dav Rules			

Figure 100 – Default SRTP Media Rule for Remote Worker – Media Silencing

- For Media QoS (Media QoS tab), enter the following:
 - Verify **RTCP Enabled** in **not** checked.
 - Enable **QoS Marking** and set it to **DSCP**.
 - Set Audio QoS and Video QoS to AF11.
 - Click on **Finish** (not shown).

Alarms Incidents Statistic	s Logs Diagnostics U	Jsers		Settings Help Log Out
Session Borde	er Controller fo	or Enterprise	5	AVAYA
Dashboard	Media Rules: defa	ult_sRTP_RW		
Administration	Add	Filter By Device	•	Rename Clone Delete
Backup/Restore	Media Rules		Click here to add a description.	
System Management	default-low-med		Click here to add a description.	
Global Parameters	default-low-med	Media NAT Media End	ryption Media Anomaly Media Silencing Media QoS	
Global Profiles	default-low-med-enc	S H	Media QoS Reporting	ِ ا
SIP Cluster	default-high		A Designation of a state of the	
 Domain Policies 	default-high-enc	RTCP Enabled		
Application Rules	A CONTRACTOR OF A CONTRACT		Media QoS Marking	
Border Rules	avaya-low-med-enc			
Media Rules	default_sRTP_RW	Enabled	N	
Security Rules		QoS Type	DSCP	
Signaling Rules		1 24		
Time of Day Rules			Audio QoS	
End Point Policy Groups		Audio DSCP	AF11	
Session Policies			Video QoS	
TLS Management		Video DSCP	AF11	
Device Specific Settings			Edit	

Figure 101 – Default SRTP Media Rule for Remote Worker – Media QoS

New rule default_sRTP_RW is assigned to the End Point Policy Group in Section 12.13.

HV; Reviewed:
SPOC 11/6/2014

12.13. End Point Policy Groups

Three new End Point Policy Groups are defined for Remote Worker: **SM_RW**, **RemoteUser_SRTP**, and **RemoteUser_RTP**.

In addition, the End Point Policy Group **SP3_PolicyG** was previously created for SIP Trunking with Videotron (see **Section 7.3.7**) and is shown here for completeness.

The End Point Policy Group **SP3_PolicyG** is used in the Server Flow defined in the **Section 0.0.0**.

Alarms Incidents Statistic	s Logs Diagnostics	Jsers	Settings Help Log Out
Session Borde	r Controller f	or Enterprise	AVAYA
Dashboard Administration	Policy Groups: SP	B_PolicyG Filter By Device	Rename Clone Delete
Backup/Restore System Management	Showing page 1 of 2.	Click here to add a description.	
Global Parameters	Policy > >> Groups	Hover over a row to see its description.	
Global Profiles	default-low	Policy Group	
 SIP Cluster Domain Policies 	default-low-enc		Summary Add
Application Rules	default-med	Order Application Border Media Security Signaling	Time of Day
Border Rules	default-med-enc	1 default default default-low-med default-med default	default Edit Clone
Media Rules	default-high		
Security Rules Signaling Rules	default-high-enc		
Time of Day Rules	OCS-default-high		
End Point Policy	avaya-def-low-enc		
Groups Session Policies	avaya-def-high-subs		
 TLS Management 	avaya-def-high-server		
 Device Specific Settings 	SM63_SP3_PolicyG		
	SP3_PolicyG		

Figure 102 – Videotron End Point Policy

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

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

The End Point Policy Group **SM_RW** is used in the Server Flow **SM63_Remote_Worker** in **Section 0.0.0**.

HV; Reviewed:
SPOC 11/6/2014

Session Borde	r Controller f	or En	terprise						4	VAY
Dashboard Administration Backup/Restore	Policy Groups: SM	I_RW Filter By D	Pevice 🗸					Rename	Clone	Delete
System Management	Showing page 1 of 2.				Click here to	add a description				
Global Parameters	Policy > >> Groups				Hover over a row	v to see its descrip	tion.			-
 Global Profiles SIP Cluster 	default-low	Policy Gr	oup							
Domain Policies	default-low-enc								Summary	Add
Application Rules	default-med	Order	Application	Border	Media	Security	Signaling	Time of D	lay	
Border Rules	default-med-enc	1	RemoteWorker AR	default	default-low-	default-low	default	default	Edit	Clone
Media Rules	default-high				med					
Security Rules Signaling Rules	default-high-enc									02
Time of Day Rules	OCS-default-high									
End Point Policy	avaya-def-low-enc									
Groups	avaya-def-high-subs									
Session Policies TLS Management	avaya-def-high-server									
Device Specific Settings	SM_RW									
	SM63_SP3_PolicyG									
	SP3 PolicyG									

Figure 103 – Remote Worker End Point Policy

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

- Enter a name (e.g., **RemoteUser_SRTP**), and click on **Next** (not shown).
- The **Policy Group** window will open. Enter the following:
 - Application Rule = RemoteWorker_AR (Section 12.11)
 - Border Rule = default
 - Media Rule = default_sRTP_RW (Section 12.12)
 - Security Rule = default-low
 - Signaling Rule = default
 - Time of Day Rule = default
 - Click on **Finish** (not shown).

The End Point Policy Group **RemoteUser_SRTP** is used in the Subscriber Flow **Remote-User-96x1** defined in the **Section 12.14.1**.

Session Borde	er Controller f	or Ent	erprise						4	VAY
Dashboard Administration Backup/Restore	Policy Groups: Re	moteUser_			Click here to ad	d a description		Rename	Clone	Delete
System Management Global Parameters Global Profiles	Policy > >> Groups default-low	Policy Grou	ID		Hover over a row to		эп.			
SIP Cluster Domain Policies	default-low-enc default-med		· .						Summary	Add
Application Rules Border Rules Media Rules Security Rules	default-med default-med-enc default-high default-high-enc	Order	Application RemoteWorker_AR	Border default	Media default_sRTP_RW	Security default-low	Signaling default	Time of Da default		Clone
Signaling Rules Time of Day Rules	OCS-default-high									
End Point Policy Groups	avaya-def-low-enc									
Session Policies TLS Management Device Specific Settings	avaya-def-high-server									
	SM_RW SM63_SP3_PolicyG									
	SP3_PolicyG									

Figure 104 – Remote Worker End Point Policy - SRTP

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 12.11)
 - **Border Rule** = default
 - **Media Rule** = default_low_med
 - **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 Subscriber Flows **Remote-User-one-X** and **Flare** defined in the **Section 12.14.1**.

Dashboard	Policy Groups: Re	moteUser	RTP							
Administration	Add	Filter By De	-	i				Rename	Clone	Delete
Backup/Restore		r nor by be		1	The second s			Rename	CIDITE	Delete
System Management	Showing page 1 of 2.				Click here to	add a description				
Global Parameters	Policy > >> Groups				Hover over a rov	v to see its descrip	tion.			
Global Profiles	default-low	Policy Gro	up							
SIP Cluster	default-low-enc		-					P.	immary	Add
Domain Policies Application Rules	default-med	Order	Application	Border	Media	Security	Signaling	Time of Day	hinnary	Add
Border Rules	default-med-enc	-		200000000000	default-low-					
Media Rules	default-high	1	RemoteWorker_AR	default	med	default-low	default	default	Edit	Clone
Security Rules	0									
Signaling Rules	default-high-enc									
Time of Day Rules	OCS-default-high									
End Point Policy	avaya-def-low-enc									
Groups	avaya-def-high-subs									
Session Policies TLS Management	avaya-def-high-server									
Device Specific Settings	RemoteUser SRTP									
Device opecine octangs	RemoteUser RTP									
	SM_RW									

Figure 105 – Remote Worker End Point Policy - RTP

12.14. End Point Flows

12.14.1. Subscriber Flow

Three **Subscriber Flows** are defined for Remote Workers. One for each **User Agent** previously created: **Remote-User-96x1** (Avaya 96x1 Deskphones), **Flare** (Avaya Flare[®] Experience for Windows softphone), and **Remote-User-one-X** (one-X[®] Communicator softphone).

Session Borde	er Controller	for Ent	erprise							AV	AYA
Dashboard Administration Backup/Restore System Management 9 Global Parameters 9 Global Profiles	End Point Flows Devices SBCE62	Subscribe			k here to a	dd a row descripti	20			ļ	Add
 SIP Cluster Domain Policies 		Priority	Flow Name	URI Group	Source Subnet	User Agent	End Point Policy Group				
 TLS Management Device Specific Settings 		1	Remote-User-96x1	RemoteWorker	•	one-X Deskphone	RemoteUser_SRTP	View	Clone	Edit	Delete
Network Management Media Interface		2	Flare	RemoteWorker	*	Flare	RemoteUser_RTP	View	Clone	Edit	Delete
Signaling Interface Signaling Forking		3	Remote-User-one-X	RemoteWorker		one-X Communicator	RemoteUser_RTP	View	Clone	Edit	Delete

Figure 106 – Remote Worker Subscriber Flows

The following screen shows the details of the flow **Remote-User-96x1** used in the reference configuration for Remote Worker Avaya 96x1 Series IP Deskphones.

To create the **Remote-User-96x1** Subscriber Flow, click on **Add** and the Criteria window will open (not shown). Enter the following:

Enter a name (e.g., **Remote-User-96x1**) **URI Group = RemoteWorker User Agent = one-X_Deskphone (Section 12.8) Source Subnet = *** (default) **Via Host = *** (default) **Contact Host = *** (default) **Signaling Interface = OutsideSIPRW (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 = one-X_Deskphone
- Media Interface = OutsideMediaRW
- End Point Policy Group = RemoteUser_SRTP
- Routing Profile = To_SM_RW (Section 12.5)
- Topology Hiding Profile = None
- Phone Interworking Profile = Avaya-RU
- TLS Client Profile = AvayaSBCClient
- **RADIUS Profile = None**
- File Transfer Profile = None
- Signaling Manipulation Script = None

Click on Finish.

Criteria		11	Ontional Cattions			
Flow Name	Remote-User-96x1		- Optional Settings	None		
URI Group	RemoteWorker		Topology Hiding Profile			
User Agent	one-X Deskphone		Phone Interworking Profile	Avaya-Ru		
Source Subnet	*		TLS Client Profile	AvayaSBCClient		
Via Host	*		RADIUS Profile	None		
	*		File Transfer Profile	None		
Contact Host			Signaling Manipulation Script	None		
Signaling Interface	OutsideSIPRW		k.			
Profile						
Source		Subscriber				
	efore REGISTER					
Methods Allowed B		one-X Deskphone				
		one-X De	skphone			
User Agent		one-X De OutsideN				
Methods Allowed B User Agent Media Interface End Point Policy G	oup	OutsideM				

Figure 107 – Remote Worker Subscriber Flows - Avaya 96x1 Series IP Deskphones

Repeat steps 1-3 to create Subscriber Flows for Communicator and Flare, with the following changes:

To create the **Remote-User-one-X** Subscriber Flow, click on **Add** and the Criteria window will open (not shown). Enter the following:

- Enter a name (e.g., **Remote-User-one-X**)
- User Agent = one-X Communicator (Section 12.8)
- End Point Policy Group = RemoteUser_RTP

	View	Flow: Remote-Us	er-one-X		Х
Criteria Flow Name URI Group User Agent Source Subnet Via Host Contact Host	Remote-User-one-X RemoteWorker one-X Communicator * *	Topo Phor TLS RAD	ional Settings logy Hiding Profile ne Interworking Profile Client Profile IUS Profile Transfer Profile	None Avaya-Ru None None None	
Signaling Interface	OutsideSIPRW	Sign	aling Manipulation Script	None	
Source		Subscriber			Ì
Methods Allowed B User Agent	elore REGISTER	one-X Communic	ator		
Media Interface End Point Policy G	quo	OutsideMediaRW RemoteUser_RTF			
		To_SM_RW			

Figure 108 – Remote Worker Subscriber Flows - Avaya one-X[®] Communicator

To create the **Flare** Subscriber Flow, click on **Add** and the Criteria window will open (not shown). Enter the following:

Enter a name (e.g., Flare) User Agent = Flare (Section 12.8) End Point Policy Group = RemoteUser_RTP

		View Flo	ow: Flare	х
Criteria Flow Name URI Group User Agent Source Subnet Via Host	Flare RemoteWorker Flare *		Optional Settings Topology Hiding Profile Phone Interworking Profile TLS Client Profile RADIUS Profile File Transfer Profile	None Avaya-Ru None None
Contact Host Signaling Interface Profile	* OutsideSIPRW		Signaling Manipulation Script	None
Source Methods Allowed Be User Agent	efore REGISTER	Subscribe Flare	er.	
Media Interface End Point Policy Gr	roup	OutsideM RemoteU		
Routing Profile		To_SM_F	RM.	

Figure 109 – Remote Worker Subscriber Flows - Flare

12.14.2. Server Flow

The following screens show the new **Server Flow** settings for Remote Worker access to Session Manager. The existing Server Flow **SM63 Flow**, created for Videotron SIP Trunking in **Section 7.4.4** is also shown for completeness. Both flows are defined as part of the **SM63** Server Configuration discussed in **Section 12.7**.

Remote Worker Server Flow

Select **Device Specific Settings** from the menu on the left-hand side. Select **Endpoint Flows.** Select the **Server Flows** tab. Select **Add** (not shown), and enter the following:

- Name = SM63_RemoteWorker
- Server Configuration = SM63 (Section 12.7)
- URI Group = RemoteWorker

HV; Reviewed:	Solution & Interoperability Test Lab Application Notes	100 of 108
SPOC 11/6/2014	©2014 Avaya Inc. All Rights Reserved.	VTCM63SM63SBCE

- **Transport** = * (default)
- **Remote Subnet** = * (default)
- Received Interface = OutsideSIPRW (Section 12.3)
- Signaling Interface = InsideTLSRW (Section 12.3)
- Media Interface = InsideMediaRW (Section 12.2)
- End Point Policy Group = SM_RW (Section 12.13)
- Routing Profile = default_RW (Section 12.5)
- **Topology Hiding Profile** = **None** (default)
- **File Transfer Profile** = **None** (default)

Click **Finish** (not shown).

	View Flow: SM	163_RemoteWorker	
Criteria —		Desete	
Flow Name	SM63_RemoteWorker	Signaling Interface	InsideTLSRW
Server Configuration	SM63		
URI Group	RemoteWorker	Media Interface	InsideMediaRW
Transport	*	End Point Policy Group	SM_RW
Remote Subnet	*	Routing Profile	default_RW
		Topology Hiding Profile	None
Received Interface	OutsideSIPRW	File Transfer Profile	None

Figure 110 – Remote Worker Server Flow

Trunking Server Flow

The Videotron SIP Trunking Server Flow is defined in Section 7.4.4 of this document.

View		low: SM63 Flow	
Criteria ———		Profile	
Flow Name	SM63 Flow	Signaling Interface	InsideUDP
Server Configuration	SM63	Media Interface	InsideMedia
URI Group	SP3	End Point Policy Group	SM63_SP3_PolicyG
Transport	*	Routing Profile	SM63_To_SP3
Remote Subnet	*	Topology Hiding Profile	SP3_To_SM63
Received Interface	OutsideUDP	File Transfer Profile	None

12.15. System Manager

12.15.1. Modify Session Manager Firewall: Elements \rightarrow Session Manager \rightarrow Network Configuration \rightarrow SIP Firewall

Select Rule Sets as Rule Set for SM63, click Edit button.

ura [©] System Manager 6.3				Last Logged on at December 18, 2013 9:1 Help About Change Password Log off ad
Home Session Manager *				
Session Manager	Home /Elements / Session Ma	nager / Network Configuration /	SIP Firewall	
Dashboard Session Manager Administration	SIP Firewall Config Create, configure and assign SIP Fi	guration rewall Rule Sets to Session Managers		Help :
Communication Profile Editor Network Configuration	Rule Sets	P Edit Q View	Assign 👻 🥥 Delete	Import • Status
Failover Groups	5 Items 😂			
Local Host Name	Rule Sets	Assigned Count	Avaya Provided	Description
Resolution	BSM 6.3.4.0	Q	Default	Avaya provided Rule Set for BSM
Remote Access	BSM 6.3.2.0	Q	Yes	Avaya provided Rule Set for BSM
SIP Firewall	□ <u>SM 6.3.4.0</u>	<u>0</u>	Default	Avaya provided Rule Set for SM
Device and Location	☐ SM 6.3.2.0	0	Yes	Avaya provided Rule Set for SM
Configuration	Rule Set for SM63	1	No	
Application Configuration	Select : All, None			

Figure 112 – 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., **255.255.255.0**). Select **Apply As Current**.

AVAYA Aura [®] System Manager 6.3			He	Last Logged on at December 18, 2013 9:16 AM elp About Change Password Log off admin
Home Session Manager *				
* Session Manager	Home / Elements / Session Man	ager / Network Configuration / 9	SIP Firewall	
Dashboard Session Manager Administration	Rule Set Edit or view SIP Firewall Rule Set wh	nitelist, blacklist, and rules.	Done	Help ?
Communication Profile	*Name Rule Set for S	SM63		
Editor	Description			
Network Configuration				
Failover Groups Local Host Name Resolution	Rules Blacklist Whitelist	Enabled 🛛 🗹		
Remote Access	Кеу	Value		Mask
SIP Firewall	Remote IP Address	10.10.98.21		255.255.255
Device and Location Configuration	Select : All, None			
▶ Application				

Figure 113 – Session Manager – SIP Firewall Configuration - Whitelist

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

Select the Session Manager instances as SM63, and select Edit.

AVAYA Aura [®] System Manager 6.3	Last Logged on at Help About Change P	December 18, Password Lo	2013 9:16 AM 9 g off admin
Home Session Manager *			
Session Manager	Home /Elements / Session Manager / Session Manager Administration		
Dashboard			Help ?
Session Manager	Session Manager Administration		
Administration	This page allows you to administer Session Manager instances and configure their global settings.		
Communication Profile Editor	Global Settings		
▶ Network Configuration	Save		
Device and Location	Allow Unauthenticated Emergency Calls 🔲		
Configuration	Allow Unsecured PPM Traffic 🔽		
Application	Failback Policy Auto		
Configuration			
System Status	ELIN SIP Entity None		
System Tools	Better Matching Dial Pattern or Range in Location ₩ ALL Overrides Match in Originator's Location		
Performance	Ignore SDP for Call Admission Control		
	Disable Call Admission Control Threshold Alarms		
	Disable Loop Detection Alarms		
	*Loop Detection Alarms Threshold (hours) 24		
	Enable TLS Endpoint Certificate Validation 🔲		
	Enable Dial Plan Ranges 🛛		
	Session Manager Instances		
	New View Edit Delete		
	1 Item 🧔	Filter:	Enable
	Name Primary Communication Profiles Secondary Communication Profiles Maximum Active Communication Profiles	Description	VMware
	C SM63 4 0 4		
	Select : None		

Figure 114 – 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 **Return**.

Personal Profile Manager (PPM) - Connection Se	ttings 👻
Limited PPM Client Connection	
Maximum Connection per PPM Client 3	
PPM Packet Rate Limiting	
PPM Packet Rate Limiting Threshold 200	
Event Server 🔹	
Clear Subscription on Notification Failure No	

Figure 115 – Session Manager – Disable PPM limit

12.16. Remote Worker IP Telephone Configuration

The following screens illustrate Avaya one- X^{\otimes} SIP Deskphone administration settings for the Remote Worker, used in the reference configuration (note that some screen formats may differ from endpoint to endpoint).

12.16.1. ADDR Screen

In the reference configuration, the Remote Worker endpoints use DHCP to receive IP address assignments, therefore set the **Use DHCP** field to **Yes**. The reference configuration uses an HTTP file server, therefore the Avaya SBCE IP address defined for Remote Worker file transfer; **10.10.98.124** (see **Section 12.1**), is specified in the **HTTP File Server** field.

		3:40pm 9/3/14
Address Pr	ocedures	
Obtain net	work settings aut	omatically
A Use DHC	Р	Yes 🔶
Phone:		10.10.98.136
Router:		10.10.98.126
Mask: 255.255.2		255.255.255.0
HTTPS F	ile Server:	
HTTP Fil	e Server:	10.10.98.124
Save	Change	Cancel

Figure 116 – Avaya one-X[®] SIP Deskphone - Address Settings

HV; Reviewed: SPOC 11/6/2014

12.16.2. SIP Global Settings Screen

Under SIP Global Settings, the SIP Domain is set to bvwdev7.com (see Section 12.10). The Avaya Config Server parameter is set to the outside interface of the Avaya SBCE defined for Remote Worker telephony, 10.10.98.99 (see Section 12.1). The other fields are default.

	4:70pm 9/3/14
SIP Global Settings	•
Use ◀▶ to change setting.	
SIP Mode:	Proxied 🔶
SIP Domain:	bvwdev7.com
Avaya Environment:	Auto 🔶
Reg. Policy	simultaneous 🚸
Failback Policy	auto 🔶
Avaya Config Server:	10.10.98.99
Change	Back

Figure 117 – Avaya one-X[®] SIP Deskphone - SIP Global Settings

12.16.3. SIP Proxy Settings Screen

Under **SIP Proxy Settings**, the **SIP Proxy Server** is set to the external IP address of Avaya SBCE designated for Remote Worker telephony traffic, **10.10.98.99** (see **Section 12.1**). **TLS** transport and port **5061** is also specified.

	4:55pm 9/3/14
SIP Proxy Settings	•
UDP or TCP or TLS.	
SIP Proxy Server	10.10.98.99
Transport Type:	TLS 🚸
SIP Port:	5061

Figure 118 – Avaya one- $X^{$ ® SIP Deskphone - SIP Proxy Settings

12.17. Avaya IP Telephone 46xxsettings Configuration File

The **46xxsettings.txt** file contains configuration parameters used by Avaya IP endpoints. This file resides in the wwwroot directory of the HTTP file server used in the reference configuration. Whenever an Avaya IP endpoint is rebooted, it will attempt to download the 46xxsettings file from the designated file server (**Section 12.9**).

The following screens show an Avaya one-X[®] SIP Deskphone 46xxsettings file for SIP phone.

```
****
##
# Group8
## General - All Phones
SET STATIC 0
SET APPSTAT 1
SIP
SET SIPDOMAIN "avayalab.com"
SET SIPPROXYSRVR "10.10.98.99"
SET ENABLE PPM SOURCED SIPPROXYSRVR 0
SET PPM ENABLE 1
SET CONFIG SERVER 10.10.98.99
SET CONFIG SERVER SECURE MODE 0
SET ENABLE AVAYA ENVIRONMENT 1
SET ENABLE G711U 1
SET MSGNUM 8000
SET DTMF PAYLOAD TYPE 101
SET SEND DTMF TYPE 2
SET SECURECALL 1
SET MEDIAENCRYPTION 1
SET DISPLAY NAME NUMBER 1
SET DIALPLAN "1xxx|91xxxxxxxx|90xxxxxxxxxxxxxxxx
SET ENABLE REDIAL LIST 1
SET SIP CONTROLLER LIST 10.10.98.99:5061;transport=tls
SET COUNTRY "USA"
SET GMTOFFSET "-5:00"
SET DAYLIGHT SAVING SETTING MODE 2
SET DATEFORMAT %m/%d/%y
SET TIMEFORMAT 0
SET TCP KEEP ALIVE STATUS 1
SET TCP KEEP ALIVE TIME 60
SET TCP KEEP ALIVE INTERVAL 10
GOTO END
****
# END
```

13. Appendix B: SigMa Script

The following is the Signaling Manipulation script used in the configuration of the SBCE, **Section 7.2.6**:

```
within session "INVITE"
{
    act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
    {
        %HEADERS["From"][1].URI.USER.regex_replace("(\011)","");
        %HEADERS["Contact"][1].URI.USER.regex_replace("(\011)","");
    }
}
within session "All"
{
    act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
    {
}
```

// Remove unwanted Headers

```
remove(%HEADERS["Alert-Info"][1]);
remove(%HEADERS["P-AV-Message-Id"][1]);
remove(%HEADERS["P-Charging-Vector"][1]);
remove(%HEADERS["Av-Global-Session-ID"][1]);
remove(%HEADERS["P-Location"][1]);
```

} }

©2014 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by [®] and TM 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 <u>devconnect@avaya.com</u>.