



Application Notes for Windstream SIP Trunking Service (Broadsoft Platform) with Avaya Aura® Communication Manager Release 5.2.1, Avaya Aura® Session Manager Release 6.3 and Avaya Session Border Controller for Enterprise Release 6.2 – Issue 1.0

Abstract

These Application Notes describe the steps to configure a Session Initiation Protocol (SIP) trunk between Windstream SIP Trunking Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager Evolution Server 5.2, Avaya Aura® Session Manager 6.3, Avaya Session Border Controller for Enterprise 6.2 and various Avaya endpoints. This documented solution does not extend to configurations without Avaya Aura® Session Manager and Avaya Session Border Controller for Enterprise.

Windstream 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 is conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

1. Introduction

These Application Notes describe the steps to configure SIP trunk between Windstream SIP Trunking Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Aura® Communication Manager 5.2 configured as an Evolution Server, Avaya Aura® Session Manager 6.3, Avaya SBC for Enterprise (Avaya SBCE) 6.2 and various Avaya endpoints.

Customers using this Avaya SIP-enabled enterprise solution with Windstream are able to place and receive PSTN calls via a broadband Internet connection. This converged network solution is an alternative to traditional PSTN trunk such as analog and/or ISDN-PRI.

2. General Test Approach and Test Results

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.

Windstream is a member of the Avaya DevConnect Service Provider Program. The general test approach is to connect a simulated enterprise to Windstream via the Internet and exercise the features and functionalities listed in **Section 2.1**.

2.1. Interoperability Compliance Testing

To verify Windstream SIP Trunking Service interoperability, the following features and functionalities are covered in the compliance testing:

- Inbound PSTN calls to various phone types including H.323, digital and analog telephone at the enterprise. All inbound calls from PSTN are routed to the enterprise across the SIP trunk from the service provider.
- Outbound PSTN calls from various phone types including H.323, digital and analog telephone at the enterprise. All outbound calls to PSTN are routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator (1XC) soft phone. Both the 1XC Computer Mode (where 1XC is used for call control as well as audio path) and the 1XC Telecommuter Mode (where 1XC is used for call control and a separate telephone is used for audio path) are tested. Both SIP and H.323 protocols are tested.
- Dialing plans including local, long distance, international, outbound toll-free, operator assisted, local directory assistance (411) calls... etc.
- Calling Party Name presentation and Calling Party Name restriction.
- Proper codec negotiation with G.729 and G.711MU codecs.
- Early Media transmissions using G.729 and G.711MU codecs.
- DTMF tone transmissions as out-of-band RTP events as per RFC2833.

- Voicemail navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, forward and conference.
- Off-net call transfer with REFER method.
- Inbound vector call redirection with REFER method.
- Off-net call forward with Diversion method.
- EC500 mobility (extension to cellular) with Diversion method.
- Routing inbound vector call to call center agent queues.
- Response to OPTIONS heartbeat.
- Response to incomplete call attempts and trunk errors.
- Session Timers implementation.

Items that are supported and not tested including the following:

- Inbound toll-free.
- Operator Assisted (0 + 10 digits) calls.
- Emergency calls (911 in US).

Items that are not support and therefore not tested including in the following:

- T38 Fax.

2.2. Test Results

Interoperability testing of Windstream SIP Trunking Service with the Avaya SIP-enabled enterprise solution is completed with successful results for all test cases with the exception of the observations/limitations described below.

- **OPTIONS** - Windstream Communications SIP Trunking sent OPTIONS message with request line header containing “SIP:ping@110.10.98.111”. This is not acceptable to SM. Using signalling manipulation script in Avaya SBCE to convert to “SIP:110.10.98.111”
- **Outbound call to busy PSTN number** - When a call is placed to a PSTN number that is busy, the caller will hear a busy tone, but Windstream will not return a “486 Busy Here”, instead the call is answered with a “200 OK” response and a busy tone is played in the RTP stream.
- **Network Call Redirection Using SIP 302 Redirection Message** - When a Communication Manager vector received an inbound call and the vector was programmed to redirect the call back out on the SIP trunk to a PSTN number using SIP 302 redirection message, even though Windstream responded with an ACK message, the call still failed. User will hear fast busy tone treatment.
- **Network Call Redirection using REFER with redirected to Busy party** - In the testing environment, when an inbound call was made to the enterprise, to a vector redirecting the call to another PSTN endpoint that was busy, using a REFER redirection message, the caller will hear a busy tone. But Windstream will not return a “486 Busy Here”, preventing any additional processing of the call by Communication Manager, like the routing of the call to a local agent on the enterprise.

2.3. Support

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

For technical support on Windstream SIP Trunking Service, please contact Windstream technical support at:

- Phone: 1 (866) 990-3282
- Website: <http://www.windstreambusiness.com/support/customer-support>

3. Reference Configuration

Figure 1 illustrates the sample Avaya SIP-enabled enterprise solution connected to the Windstream SIP Trunking Service (Vendor Validation circuit) through a public Internet connection.

For security purposes, the real public IP addresses and PSTN routable phone numbers used in the compliance test are not shown in these Application Notes.

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

- Avaya S8800 Server running Avaya Aura® System Manager
- Avaya S8800 Server running Avaya Aura® Session Manager
- Avaya S8800 Server running Avaya Aura® Communication Manager
- Avaya G450 Media Gateway
- Avaya S8800 Server running Avaya Aura® Messaging
- Avaya Session Border Controller for Enterprise
- Avaya 9600-Series IP Telephones (H.323/SIP)
- Avaya one-X® Communicator soft phones (H.323/SIP)
- Avaya digital and analog telephones

Located at the edge of the enterprise network is the Avaya SBCE. It has a public side that connects to Windstream via Internet and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise network flows through the Avaya SBCE which can protect the enterprise against any outside SIP-based attacks. The Avaya SBCE provides network address translation at both the IP and SIP layers. The transport protocol between the Avaya SBCE and Windstream across the public network is UDP, the transport protocol between the Avaya SBCE and Session Manager is TCP, while TCP is used as the transport protocol between Session Manager and Communication Manager.

In the compliance testing, the Avaya Customer-Premises Equipment (CPE) environment was configured with SIP domain “bvwddev7.com” for the enterprise. The Avaya SBCE is used to adapt the enterprise SIP domain to the IP address based URI-Host known to Windstream. **Figure 1** below illustrates the network diagram for the enterprise. All voice application elements are connected to internal trusted LAN.

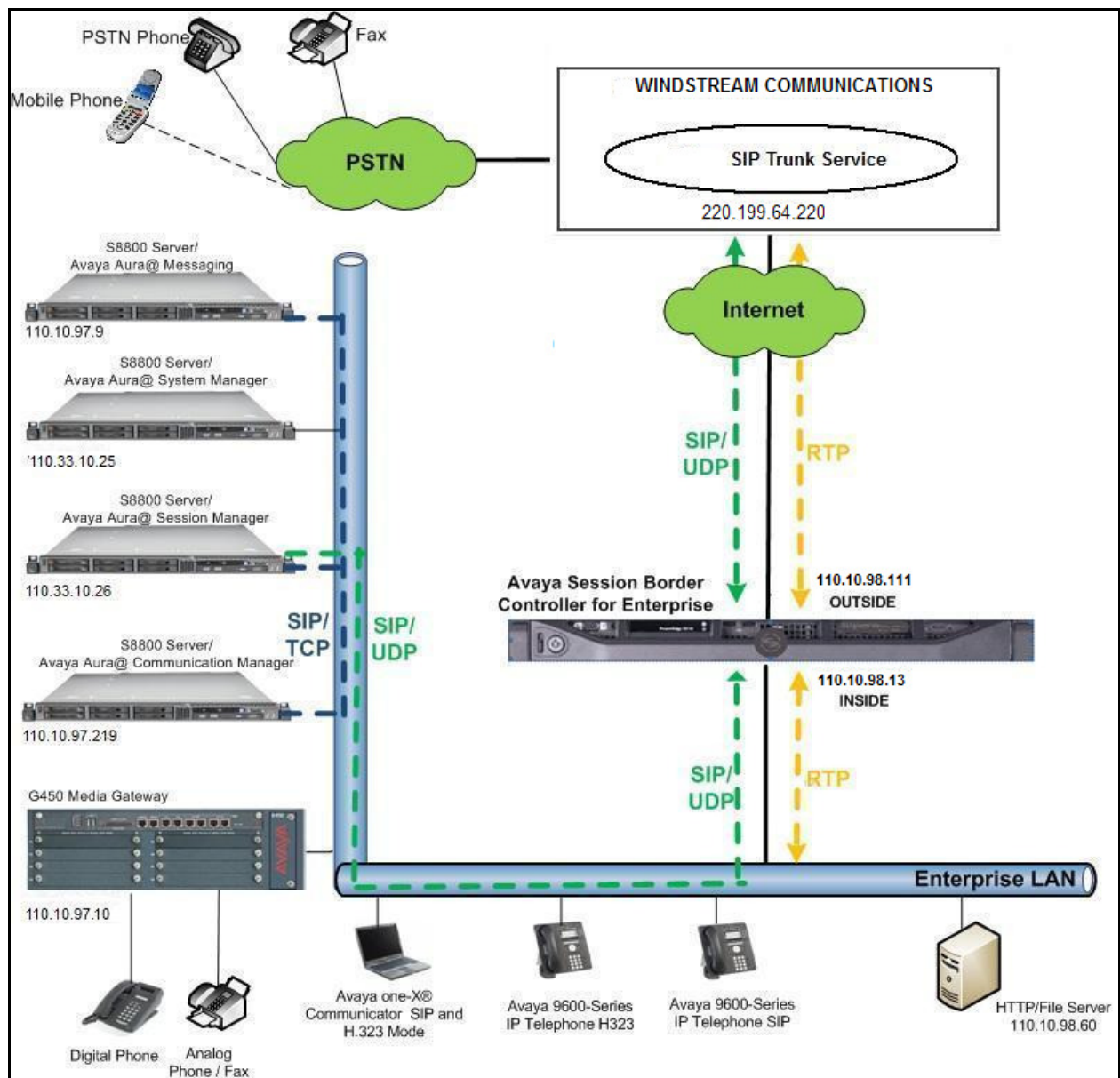


Figure 1: Avaya IP Telephony Network connecting to Windstream SIP Trunking Service

4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Component	Release
Avaya Aura® Communication Manager running on an Avaya S8800 Server	5.2.1 (Avaya CM/ R015x.02.1.016.4 with Service Pack 13 02.1.016.4-19880)
Avaya G450 Media Gateway	28.22.0
Avaya Aura® System Manager running on an Avaya S8800 Server	6.3.0 SP1 (Build Number 6.3.0.8.5682-6.3.8.859) (System Platform 6.3.0)
Avaya Aura® Session Manager running on an Avaya S8800 Server	6.3.0 (6.2.2.0.622005)
Avaya Aura® Messaging running on an Avaya S8800 Server	6.1-11.0
Avaya Session Border Controller for Enterprise	6.2.0 Q36
Avaya 9611G IP Telephone (H.323)	Avaya one-X® Deskphone Edition S6.0.0
Avaya 9630G IP Telephone (H.323)	Avaya one-X® Deskphone Edition 3.1 SP5
Avaya 9630G IP Telephone (SIP)	SIP96xx_2_6_7_0.bin
Avaya one-X Communicator (H.323/SIP)	6.1.7.04-SP7-39506
Avaya 1408 Digital Telephone	n/a
Avaya 6210 Analog Telephone	n/a
Windstream SIP Trunking Service (ACME) Components	
Component	Release
Acme Net- Net 4250	v.SC6.2.0 Patch-3
BroadSoft	17sp5

Table 1: Equipment and Software Tested

Note: This solution will be compatible with other Avaya Server and Media Gateway platforms running similar version of Communication Manager.

5. Configure Communication Manager

This section describes the procedure for configuring Communication Manager for Windstream SIP Trunking. It is assumed the general installation of Communication Manager, Avaya G450 Media Gateway and Session Manager has been previously completed and is not discussed here.

The configuration of Communication Manager 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 and from the service provider. 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 sale representative to add the additional capacity or feature.

display system-parameters customer-options		Page 2 of 11
OPTIONAL FEATURES		
IP PORT CAPACITIES		USED
Maximum Administered H.323 Trunks:	450	0
Maximum Concurrently Registered IP Stations:	450	4
Maximum Administered Remote Office Trunks:	450	0
Maximum Concurrently Registered Remote Office Stations:	450	0
Maximum Concurrently Registered IP eCons:	68	0
Max Concur Registered Unauthenticated H.323 Stations:	450	0
Maximum Video Capable Stations:	450	0
Maximum Video Capable IP Softphones:	450	1
Maximum Administered SIP Trunks:	450	276
Maximum Administered Ad-hoc Video Conferencing Ports:	450	0
Maximum Number of DS1 Boards with Echo Cancellation:	80	0
Maximum TN2501 VAL Boards:	0	0
Maximum Media Gateway VAL Sources:	50	1
Maximum TN2602 Boards with 80 VoIP Channels:	0	0
Maximum TN2602 Boards with 320 VoIP Channels:	0	0
Maximum Number of Expanded Meet-me Conference Ports:	300	0
(NOTE: You must logoff & login to effect the permission changes.)		

5.2. System Features

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

```
change system-parameters features                               Page 1 of 18
      FEATURE-RELATED SYSTEM PARAMETERS
      Self Station Display Enabled? y
      Trunk-to-Trunk Transfer: all
      Automatic Callback with Called Party Queuing? n
      Automatic Callback - No Answer Timeout Interval (rings): 3
      Call Park Timeout Interval (minutes): 10
      Off-Premises Tone Detect Timeout Interval (seconds): 20
      AAR/ARS Dial Tone Required? y
```

On **Page 9**, verify that a text string has been defined to replace the Calling Party Number (CPN) for restricted or unavailable calls. The compliance test used the value of **anonymous** for restricted call and unavailable call.

```
change system-parameters features                               Page 9 of 18
      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: 001

      ENBLOC DIALING PARAMETERS
      Enable Enbloc Dialing without ARS FAC? n

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

5.3. IP Node Names

Use the **change node-names ip** command to verify that node names have been previously defined for the IP addresses of Communication Manager (**procr**) and Session Manager (**SPSM63**). These node names will be needed for defining the service provider signaling groups in **Section 5.6**.

change node-names ip		Page 1 of 2
		IP NODE NAMES
Name	IP Address	
SPSM63	110.10.97.26	
default	0.0.0.0	
procr	110.10.97.219	
procr6	::	

5.4. Codecs

Use the **change ip-codec-set** command to define a list of codecs to be used for calls between the enterprise and the service provider. This compliance test used ip-codec-set 5. Windstream supports G.729A and G.711MU. To use these codecs, enter **G.729A** and **G.711MU** in the **Audio Codec** column of the table in the order of preference.

The following screen shows the configuration for ip-codec-set 1. During testing, the codec set specifications are varied to test for individual codec support as well as codec negotiation between the enterprise and the network at call setup time.

change ip-codec-set 1		Page 1 of 2
		IP Codec Set
Codec Set: 1		
Audio Codec	Silence Suppression	Frames Per Pkt
1: G.729A	n	2
2: G.711MU	n	2
3:		

On **Page 2**, set the Fax Mode to *off* since T.38 faxing is not supported by Windstream SIP Trunking.

change ip-codec-set 1		Page 2 of 2
		IP Codec Set
		Allow Direct-IP Multimedia? n
FAX	Mode	Redundancy
Modem	off	0
TDD/TTY	US	3
Clear-channel	n	0

5.5. IP Network Region

A separate IP network region for the service provider trunk groups is created. This allows separate codec or quality of service setting to be used (if necessary) for call between the enterprise and the service provider versus call within the enterprise or elsewhere. For the compliance testing, ip-network-region 1 was created by the **change ip-network-region 1** command with the following parameters:

- Set the **Authoritative Domain** field to match the SIP domain of the enterprise. In the compliance testing, the domain name is *bvwdev7.com*. This domain name appears in the “From” header of SIP message 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 Media Gateway. By default, both **Intra-region** and **Inter-region IP-IP Direct Audio** are set to *yes*. Shuffling can be further restricted at the trunk level under Signaling Group form.
- Set the **Codec Set** field to the IP codec set defined in **Section 5.4**.
- Default values can be used for all other fields.

change ip-network-region 1		Page	1 of 19
IP NETWORK REGION			
Region: 1			
Location: 1	Authoritative Domain: bvwdev7.com		
Name: SIP testing			
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		RTCP Reporting Enabled? y	
Call Control PHB Value: 46	RTCP MONITOR SERVER PARAMETERS		
Audio PHB Value: 46	Use Default Server Parameters? y		
Video PHB Value: 26			
...			

On **Page 4**, define the IP codec set to be used for traffic between region 1 and other regions. In the compliance testing, Communication Manager, the Avaya G450 Media Gateway, IP phones, Session Manager and the Avaya SBCE were assigned to the same region 1. To configure IP codec set between regions, enter the desired IP codec set in the **codec set** column of the table with appropriate destination region (**dst rgn**). Default values may be used for all other fields. The example below shows codec set 1 will be used for call between region 1 and other regions.

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

Non-IP telephones (e.g., analog, digital) derive network region from IP interface the Avaya G450 Media Gateway to which the device is connected. IP telephones can be assigned a network region based on an IP address mapping.

To define network region 1 for IP interface **procr**, use **change ip-interface procr** command as shown in the following screen.

change ip-interface procr		Page 1 of 1
IP INTERFACES		
Type: procr		
		Target socket load: 1700
Enable Interface? y	Allow H.323 Endpoints? y	
	Allow H.248 Gateways? y	
Network Region: 1	Gatekeeper Priority: 5	

To define network region 1 for the Avaya G450 Media Gateway, use **change media-gateway** command as shown in the following screen.

change media-gateway 1		Page 1 of 1
MEDIA GATEWAY		
Number: 1	Registered? y	
Type: g450	FW Version/HW Vintage: 28 .22 .0 /1	
Name: Media Gateway 1	MGP IP Address: 110.10 .97 .247	
Serial No: 08IS38199691	Controller IP Address: 110.10 .97 .219	
Encrypt Link? y	MAC Address: 00:1b:4f:03:51:08	
Network Region: 1	Location: 1	Enable CF? n
		Site Data:
Recovery Rule: none		
...		

5.6. Signaling Group

Use the **add signaling-group** command to create a signaling group between Communication Manager and Session Manager for use by the service provider trunk. This signaling group is used for inbound and outbound calls between the service provider and the enterprise. For the compliance test, signaling group 50 was used for this purpose and was configured using the parameters highlighted below.

- Set the **Group Type** field to **sip**.
- Set the **IMS Enabled** field to **n**.
- Set the **Transport Method** to **tcp** The transport method specified here is used between the Communication Manager and Session Manager.
- Set the **Near-end Listen Port** and **Far-end Listen Port** to **5060**.
- Set the **Near-end Node Name** to **procr**. This node name maps to the IP interface of **procr** defined in Section 5.3.

- Set the **Far-end Node Name** to **SPSM63**. This node name maps to the IP address of Session Manager as defined in **Section 5.3**.
- Set the **Far-end Network Region** to the IP network region **1** defined for the service provider in **Section 5.5**.
- Set the **Far-end Domain** to **bvwddev7.com**.
- Set the **DTMF over IP** to **rtp-payload**. This setting enables Communication Manager to send or receive the DTMF transmissions using RFC2833.
- Set **Enable Layer 3 Test?** to **y**. This setting allows Communication Manager to send OPTIONS heartbeat to Session Manager on the SIP trunk.
- Set **Direct IP-IP Audio Connections** to **y**. This field will enable media shuffling on the SIP trunk allowing Communication Manager to redirect media traffic directly between the SIP trunk and the enterprise endpoint. If this value is set to **n**, then the Avaya G450 Media Gateway will remain in the media path between the SIP trunk and the endpoint for the duration of the call. Depending on the number of media resources available in the Avaya G450 Media Gateway, these resources may be depleted during high call volume preventing additional calls from completing.
- Set the **Direct IP-IP Early Media** is set to **n**.
- Set the **Alternate Route Timer** to **30**. This defines the number of seconds Communication Manager will wait for a response (other than 100 Trying) to an outbound INVITE before canceling the call.
- Default values may be used for all other fields.

add signaling-group 50		Page 1 of 1
SIGNALING GROUP		
Group Number: 50	Group Type: sip	
	Transport Method: tcp	
IMS Enabled? n		
IP Video? n		
Near-end Node Name: procr		Far-end Node Name: SPSM63
Near-end Listen Port: 5060		Far-end Listen Port: 5060
		Far-end Network Region: 1
Far-end Domain: bvwddev7.com		
Incoming Dialog Loopbacks: eliminate	Bypass If IP Threshold Exceeded? n	
DTMF over IP: rtp-payload	RFC 3389 Comfort Noise? n	
Session Establishment Timer(min): 3	Direct IP-IP Audio Connections? y	
Enable Layer 3 Test? y	IP Audio Hairpinning? n	
H.323 Station Outgoing Direct Media? n	Direct IP-IP Early Media? n	
	Alternate Route Timer(sec): 30	

5.7. Trunk Group

Use the **add trunk-group** command to create trunk group for the signaling group created in **Section 5.6**. For the compliance testing, trunk group 50 was configured using the parameters highlighted below.

- Set the **Group Type** field to *sip*.
- Enter a descriptive name for the **Group Name**.
- Enter an available Trunk Access Code (TAC) that is consistent with the existing dial plan in the **TAC** field.
- Set the **Outgoing Display** to *y* to enable name display on the trunk.
- Set the **Service Type** field to *public-ntwrk*.
- Set the **Signaling Group** to the signaling group shown in **Section 5.6**.
- Set the **Number of Members** field to **32**. It is the number of trunk members in the SIP trunk group. This value determines how many simultaneous SIP calls can be supported by this trunk group.
- Default values are used for all other fields.

add trunk-group 50		Page 1 of 21	
TRUNK GROUP			
Group Number: 50	Group Type: sip	CDR Reports: y	
Group Name: SP Trunk	COR: 1	TN: 1	TAC: *001
Direction: two-way	Outgoing Display? y	Night Service:	
Dial Access? n			
Queue Length: 0			
Service Type: public-ntwrk	Auth Code? n		
		Signaling Group: 50	
		Number of Members: 32	

On **Page 2**, verify that the **Preferred Minimum Session Refresh Interval (sec)** is set to a value acceptable to service provider. This value defines the interval a re-INVITEs must be sent to refresh the Session Timer. For the compliance testing, a default value of **3600** seconds was used.

add trunk-group 50		Page 2 of 21	
Group Type: sip			
TRUNK PARAMETERS			
Unicode Name: auto			
		Redirect On OPTIM Failure: 5000	
SCCAN? n	Digital Loss Group: 18		
Preferred Minimum Session Refresh Interval(sec): 3600			
Disconnect Supervision - In? y Out? y			

On **Page 3**, set the **Numbering Format** field to *private*. This field specifies the format of the CPN sent to the far-end. The public numbers are automatically preceded with a + sign when passed in the “From”, “Contact” and “P-Asserted Identity” headers. The addition of the + sign impacted interoperability with service provider. Thus, the **Numbering Format** is set to **private** and the **Numbering Format** in the route pattern is set to *lev0-pvt* (see **Section 5.9**).

Set the **Replace Restricted Numbers** and **Replace Unavailable Numbers** fields to **y**. This will allow the CPN displayed on local endpoint to be replaced with the value set in **Section 5.2**, if inbound call enabled CPN block. Default values are used for all other fields.

add trunk-group 50	Page 3 of 21
TRUNK FEATURES	
ACA Assignment? n	Measured: none
	Maintenance Tests? y
Numbering Format: private	
	UII Treatment: service-provider
	Replace Restricted Numbers? y
	Replace Unavailable Numbers? y
Show ANSWERED BY on Display? y	

On **Page 4**, the **Network Call Redirection** field can be set to **y**. The setting of **Network Call Redirection** flag to **y** enables use of the SIP REFER message to transfer an inbound call to a back to PSTN.

- Set the **Send Diversion Header** field to **y**. This field provides additional information to the network if the call has been re-directed. This is needed to support call forwarding of inbound call back to PSTN and Extension to Cellular (EC500) call scenarios.
- Set the **Support Request History** field to **n**. This parameter determines if History-Info header will be excluded in the call-redirection INVITE from the enterprise.
- Set the **Telephone Event Payload Type** to **101**, the value is preferred by Windstream.

add trunk-group 50	Page 4 of 21
PROTOCOL VARIATIONS	
Mark Users as Phone? n	
Prepend '+' to Calling Number? n	
Send Transferring Party Information? n	
Network Call Redirection? y	
Send Diversion Header? y	
Support Request History? n	
Telephone Event Payload Type: 101	

5.8. Calling Party Information

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

The screen below shows a subset of the DID numbers assigned for testing. These 3 numbers were mapped to the 3 enterprise extensions 1130, 1131 and 1132. These same 10-digit numbers were used in the outbound calling party information on the service provider trunk when calls were originated from these 3 extensions.

change private-numbering 0					Page 1 of 2
NUMBERING - PRIVATE FORMAT					
Ext Len	Ext Code	Trk Grp (s)	Private Prefix	Total Len	
4	1130	50	4693418165	10	Total Administered: 15
4	1131	50	4693418166	10	Maximum Entries: 540
4	1132	50	4693418167	10	
4	181	50		4	

Even though private numbering is selected, currently the number used in the SIP Diversion header is derived from the public unknown numbering table and not the private numbering table. As a workaround for this, the entries in the private numbering table must be repeated in the public unknown numbering table.

change public-unknown-numbering 0					Page 1 of 2
NUMBERING - PUBLIC/UNKNOWN FORMAT					
Ext Len	Ext Code	Trk Grp (s)	CPN Prefix	Total CPN Len	
4	1130	50	4693418165	10	Total Administered: 18
4	1131	50	4693418166	10	Maximum Entries: 240
4	1132	50	4693418167	10	

5.9. Outbound Routing

In these Application Notes, the **Automatic Route Selection** (ARS) feature is used to route outbound call via the SIP trunk to service provider. In the compliance testing, a single digit 9 was used as the ARS access code. Enterprise caller will dial 9 to reach an outside line. To define feature access code (**fac**) 9, use the **change dialplan analysis** command as shown in the table below.

change dialplan analysis									Page 1 of 12
DIAL PLAN ANALYSIS TABLE									
Location: all					Percent Full: 1				
Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	Dialed String	Total Length	Call Type	
0	3	fac							
6	1	fac							
9	1	fac							
*	4	dac							
3	4	udp							

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

```

change feature-access-codes                                     Page 1 of 10
                                FEATURE ACCESS CODE (FAC)
Abbreviated Dialing List1 Access Code:
Abbreviated Dialing List2 Access Code:
Abbreviated Dialing List3 Access Code:
Abbreviated Dial - Prgm Group List Access Code:
Announcement Access Code: #007
Answer Back Access Code:
Attendant Access Code:
Auto Alternate Routing (AAR) Access Code: 6
Auto Route Selection (ARS) - Access Code 1: 9      Access Code 2:
...

```

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 testing. See **Section 2.1** for the complete list of call types tested. All dialed strings are mapped to route pattern 50 for outbound call which contains the SIP trunk to the service provider (as defined next).

```

change ars analysis 0                                         Page 1 of 2
                                ARS DIGIT ANALYSIS TABLE
                                Location: all                    Percent Full: 0

```

Dialed String	Total		Route Pattern	Call Type	Node Num	ANI Req'd
	Min	Max				
0	1	1	50	pubu		n
011	13	24	50	intl		n
1	11	11	50	pubu		n
1800	11	11	50	fnpa		n
281	10	10	50	pubu		n
411	3	3	50	svcl		n
613	10	10	50	pubu		n
866	10	10	50	pubu		n
911	3	3	50	svcl		n

As being mentioned above, the route pattern defines which trunk group will be used for the outbound calls and performs necessary digit manipulation. Use the **change route-pattern** command to configure the parameters for route pattern 50 in the following manner.

- **Pattern Name:** Enter a descriptive name.
- **Grp No:** Enter the outbound trunk group for the SIP service provider. For the compliance testing, trunk group **50** 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: lev0-pvt.** All calls using this route pattern will use the private numbering table. See setting of the **Numbering Format** in the trunk group form for full details in **Section 7**.

change route-pattern 50															Page 1 of 3	
										Pattern Number: 50		Pattern Name: WS Route				
										SCCAN? n		Secure SIP? n				
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted				DCS/	IXC				
No			Mrk	Lmt	List	Del	Digits				QSIG					
							Dgts				Intw					
1:	50	0									n	user				
2:											n	user				
....																
		BCC	VALUE	TSC	CA-TSC	ITC BCIE		Service/Feature	PARM	No.	Numbering	LAR				
		0	1	2	M	4	W	Request			Dgts	Format				
										Subaddress						
1:	y	y	y	y	y	n	n	rest		lev0-pvt		none				
...																

5.10. Saving Communication Manager Configuration Changes

The command “**save translation all**” can be used to save the configuration changes made on Communication Manager.

6. Configure Avaya Aura® Session Manager

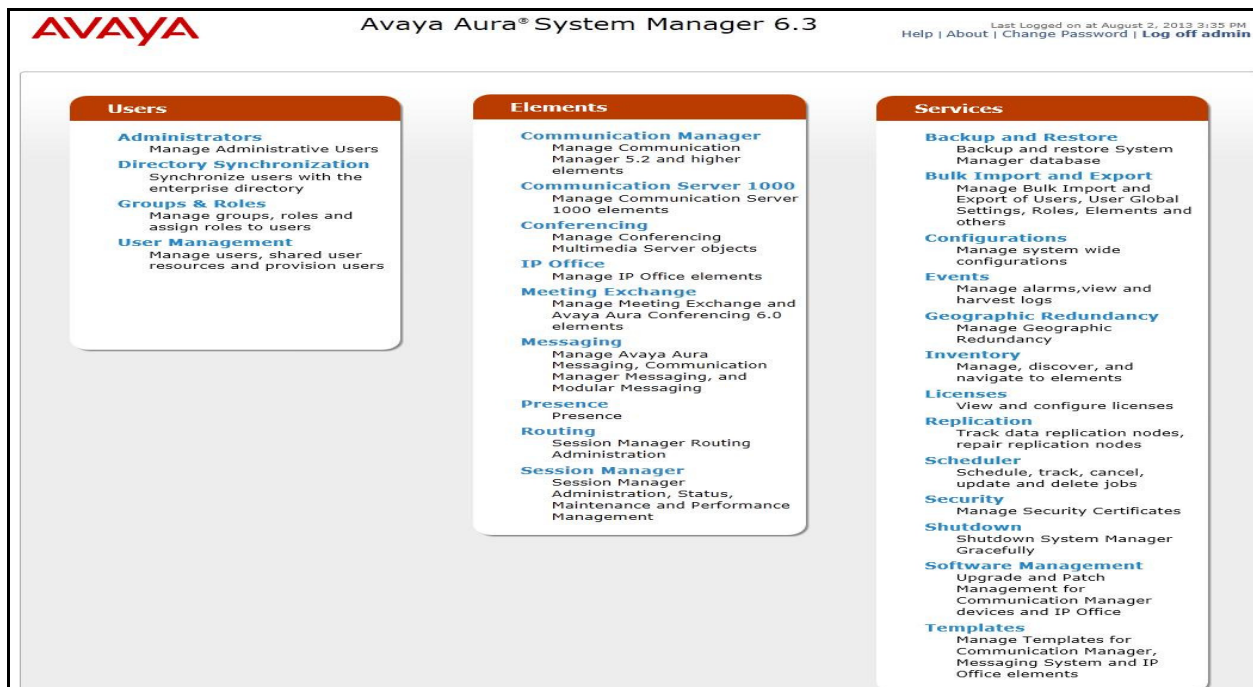
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain
- Logical/physical Location that can be occupied by SIP Entities
- SIP Entities corresponding to Communication Manager, Session Manager and the Avaya SBCE
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities
- Routing Policies, which control call routing between the SIP Entities
- Dial Patterns, which govern to which SIP Entity a call is routed
- Session Manager, corresponding to the Session Manager server to be managed by System Manager

It may not be necessary to create all the items above when creating 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. System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the Web GUI of System Manager, using the URL “https://<ip-address>/SMGR”, where “<ip-address>” is the IP address of System Manager. At the **System Manager Log On** screen, provide the appropriate credentials and click on **Login** (not shown). The initial screen shown below is then displayed.



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

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

AVAYA Avaya Aura® System Manager 6.3 Last Logged on at August 2, 2013 3:35 PM
Help | About | Change Password | **Log off admin**

Routing * Home

Home / Elements / Routing Help ?

Introduction to Network Routing Policy

Network Routing Policy consists of several routing applications like "Domains", "Locations", "SIP Entities", etc.

The recommended order to use the routing applications (that means the overall routing workflow) to configure your network configuration is as follows:

- Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).
- Step 2: Create "Locations"
- Step 3: Create "Adaptations"
- Step 4: Create "SIP Entities"

- SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"

6.2. Specify SIP Domain

To view or change SIP domains, select **Routing** → **Domains**, then click on the checkbox next to the name of the SIP domain and **Edit** to edit an existing domain, or the **New** button to add a domain. Click the **Commit** button (not shown) after changes are completed.

The following screen shows the list of configured SIP domains. The domain “bvwddev7.com” was already being created for communication Session Manager and Communication Manager. The domain “bvwddev7.com” is not known to the Windstream. It will be adapted by the Avaya SBCE to IP address based URI-Host to meet the SIP specification of Windstream.

AVAYA Avaya Aura® System Manager 6.3 Last Logged on at August 2, 2013 3:35 PM
Help | About | Change Password | **Log off admin**

Routing * Home

Home / Elements / Routing / Domains Help ?

Domain Management

New **Edit** **Delete** **Duplicate** **More Actions** ▼

3 Items Refresh Filter: Enable

<input type="checkbox"/>	Name	Type	Notes
<input type="checkbox"/>	avayalab.com	sip	Avaya DevConnect Lab
<input type="checkbox"/>	bvwddev7.com	sip	
<input type="checkbox"/>	enterprise.com	sip	

Select : All, None

6.3. Add Location

Locations can be used to identify logical and/or physical locations where SIP Entities reside for bandwidth management and call admission control purposes. To add a location, navigate to **Routing → Locations** in the left-hand navigation pane and click the **New** button in the right pane (not shown).

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

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

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

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

Displayed below are the screenshots for location **Belleville**, which includes all equipment on the enterprise network including Communication Manager, Session Manager and the Avaya SBCE. Click **Commit** to save.

AVAYA Avaya Aura® System Manager 6.3

Last Logged on at August 2, 2013 4:32 PM
Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Locations

Location Details

Commit Cancel

General

* Name: Belleville

Notes: GSSCP Belleville

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

Location Pattern

Add Remove

3 Items Refresh Filter: Enable

IP Address Pattern	Notes
* 10.33.*	
* 110.10.97.*	
* 110.10.98.*	

Select : All, None

6.4. Add Adaptation Module

Session Manager can be configured with Adaptation modules that can modify SIP messages before or after routing decisions have been made. A generic Adaptation module

DigitConversionAdapter supports digit conversion of telephone numbers in specific headers of SIP messages. Other Adaptation modules are built on this generic, and can modify other headers to permit interoperability with third party SIP products.

For interoperability with Windstream SIP Trunking, one Adaptation is needed. This Adaptation is applied to the Communication Manager SIP Entity and maps inbound DID numbers from Windstream to local Communication Manager extensions.

To create an Adaptation, navigate to **Routing → Adaptations** in the left-hand navigation pane and click on the **New** button in the right pane (not shown).

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

- **Adaptation Name:** Enter a descriptive name for the adaptation.
- **Module Name:** Enter *DigitConversionAdapter*

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

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

Click **Commit** to save.

In the example shown bellow, if a user on the PSTN dials 469-341-8165, Session Manager will convert the number to 1130 before sending out the SIP INVITE to Communication Manager. As such, it would not be necessary to use the incoming call handling table of the receiving Communication Manager trunk group to convert the DID number to its corresponding extension. For an outbound call, the Communication Manager private-numbering table was configured with an entry to convert 1130 to 4693418165 before sending the call on the trunk group to Session Manager (as shown in **Section 5.8**).

During the compliance test, the digit conversions (or number mappings) in Session Manager Adaptation as well as in private-numbering table on Communication Manager were varied to

route inbound calls to various destinations (including access number to Communication Manager Messaging and Communication Manager Vector Directory Numbers) for different test cases.

AVAYA Avaya Aura® System Manager 6.3 Last Logged on at August 2, 2013 4:32 PM
Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Adaptations Help ?

Adaptation Details Commit Cancel

General

Adaptation name: SP CM521 Adaptation

Module name: DigitConversionAdapter

Module parameter:

Egress URI Parameters:

Notes: Use with Avaya SBCE

Digit Conversion for Incoming Calls to SM

Add Remove

0 Items Refresh Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>									

Digit Conversion for Outgoing Calls from SM

Add Remove

3 Items Refresh Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data
<input type="checkbox"/>	*4693418165	*10	*10		*10	1130	destination	
<input type="checkbox"/>	*4693418166	*10	*10		*10	1131	destination	
<input type="checkbox"/>	*4693418167	*10	*10		*10	1132	destination	

Select : All, None

6.5. Add SIP Entities

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

To add a new SIP Entity, navigate to **Routing → SIP Entities** in the left navigation pane and click on the **New** button in the right pane (not shown).

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

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Select **Session Manager** for Session Manager, **CM** for Communication Manager and **Other** for the Avaya SBCE.
- **Location:** Select one of the locations defined previously in **Section 6.3**.
- **Time Zone:** Select the time zone for the location above.

The following screen shows the addition of Session Manager SIP Entity. The IP address of the Session Manager signaling interface is entered for **FQDN or IP Address**.

AVAYA Avaya Aura® System Manager 6.3

Last Logged on at August 2, 2013 4:32 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

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

Home / Elements / Routing / SIP Entities

SIP Entity Details [Commit](#) [Cancel](#) [Help ?](#)

General

* Name: SM63

* FQDN or IP Address: 110.33.10.26

Type: Session Manager

Notes: GSSCP SM R6.3

Location: Belleville

Outbound Proxy:

Time Zone: America/Toronto

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

To define the ports used by Session Manager, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for the **Session Manager** SIP Entity. In the **Port** section, click **Add** and enter the following values. Use default values for all remaining fields:

- **Port:** Port number on which the Session Manager can listen for SIP requests.
- **Protocol:** Transport protocol to be used to send SIP requests.
- **Default Domain:** The domain used for the enterprise.

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

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

Port

TCP Failover port:

TLS Failover port:

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

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

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

Select : All, None

The following screen shows the addition of Communication Manager SIP Entities. In order for Session Manager to send SIP traffic on an entity link to Communication Manager, it is necessary to create a SIP Entity for Communication Manager. The **FQDN or IP Address** field is set to the IP address of Communication Manager. Select **Type** is **CM**.

AVAYA Avaya Aura® System Manager 6.3

Last Logged on at August 2, 2013 4:32 PM
Help | About | Change Password | Log off admin

Routing x Home

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit Cancel

Help ?

General

* Name: CM521

* FQDN or IP Address: 110.10.97.219

Type: CM

Notes:

Adaptation: SP CM521 Adaptation

Location: Belleville

Time Zone: America/Toronto

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Link Monitoring Disabled

The following screen shows the addition of the SIP Entity for the Avaya SBCE. The **FQDN or IP Address** field is set to the IP address of its private network interface (see **Figure 1**). Select **Type** as **Other**. Select **SIP Link Monitoring** as **Link Monitoring Enabled** with the interval of 60 seconds. This setting allows Session Manager to send outbound OPTIONS heartbeat in every 60 seconds to service provider (which is forwarded by the Avaya SBCE) to query for the status of the SIP trunk connecting to service provider.

AVAYA Avaya Aura® System Manager 6.3

Last Logged on at August 2, 2013 4:32 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off](#)
 admin

Routing * **Home**

Home / Elements / Routing / SIP Entities

SIP Entity Details

General

* Name: SBCE_TCP

* FQDN or IP Address: 110.10.98.13

Type: Other

Notes: GSSCP SBCE R6.2

Adaptation: SP CM521 Adaptation

Location: Belleville

Time Zone: America/Toronto

Override Port & Transport with DNS ☐

SRV: ☐

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

Credential name:

Call Detail Recording: none

CommProfile Type Preference:

Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Link Monitoring Enabled

* Proactive Monitoring Interval (in seconds): 60

* Reactive Monitoring Interval (in seconds): 60

* Number of Retries: 5

Commit **Cancel**

6.6. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. During compliance testing, two Entity Links were created, one for Communication Manager and the other for the Avaya SBCE. To add an Entity Link, navigate to **Routing → Entity Links** in the left navigation pane and click on the **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager.

- **Protocol:** Select the transport protocol used for this link, TCP for the Entity Link to Communication Manager and UDP for the Entity Link to the Avaya SBCE.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For Communication Manager, this must match the **Far-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**.
- **SIP Entity 2:** Select the name of the other system. For Communication Manager, select the Communication Manager SIP Entity defined in **Section 6.4**. For the Avaya SBCE, select the Avaya SBCE SIP Entity defined in **Section 6.4**.
- **Port:** Port number on which the other system receives SIP requests from the Session Manager. For the Communication Manager, this must match the **Near-end Listen Port** defined on the Communication Manager signaling group in **Section 5.6**.
- **Connection Policy:** Select **Trusted**. **Note:** If this is not selected, calls from the associated SIP Entity specified in **Section 6.4** will be denied.

Click **Commit** to save.

The following screens illustrate the Entity Links to Communication Manager and the Avaya SBCE.

Entity Link to Communication Manager:

1 Item Refresh		Filter: Enable							
	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service	Notes
<input type="checkbox"/>	* SM63_CM521_5060	* SM63	TCP	* 5060	* CM521	* 5060	trusted	<input type="checkbox"/>	Link to CM 5.2.1

Select : All, None

Entity Link to the Avaya SBCE:

1 Item Refresh		Filter: Enable							
	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service	Notes
<input type="checkbox"/>	* SM63_SBCE_TCP_50	* SM63	TCP	* 5060	* SBCE_TCP	* 5060	trusted	<input type="checkbox"/>	Link to SBC

Select : All, None

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 were added, one for Communication Manager and the other for the Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left navigation pane and click on the **New** button in the right pane (not shown). The following screen is displayed. Fill in the following:

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

- **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 is displayed in the **Routing Policy Details** page as shown below. Use default values for remaining fields. Click **Commit** to save.

The following screens show the Routing Policies for Communication Manager and Avaya SBCE respectively.

The screenshot shows the 'Routing Policy Details' page for a policy named 'CM521 TRK50 Policy'. The left sidebar has 'Routing Policies' highlighted. The 'General' section contains fields for Name, Disabled (checkbox), Retries (0), and Notes ('WS SP testing'). The 'SIP Entity as Destination' section has a 'Select' button and a table with one entry: CM521, 110.10.97.219, CM. The 'Time of Day' section has 'Add', 'Remove', and 'View Gaps/Overlaps' buttons, followed by a table with one item: 24/7, 00:00, 23:59.

Name	FQDN or IP Address	Type	Notes
CM521	110.10.97.219	CM	

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7	✓	✓	✓	✓	✓	✓	✓	00:00	23:59	

The screenshot shows the 'Routing Policy Details' page for a policy named 'SBCE62 Policy'. The left sidebar has 'Routing Policies' highlighted. The 'General' section contains fields for Name, Disabled (checkbox), Retries (0), and Notes. The 'SIP Entity as Destination' section has a 'Select' button and a table with one entry: SBCE_TCP, 110.10.98.13, Other, GSSCP SBCE R6.2. The 'Time of Day' section has 'Add', 'Remove', and 'View Gaps/Overlaps' buttons, followed by a table with one item: 24/7, 00:00, 23:59.

Name	FQDN or IP Address	Type	Notes
SBCE_TCP	110.10.98.13	Other	GSSCP SBCE R6.2

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7	✓	✓	✓	✓	✓	✓	✓	00:00	23:59	

6.8. Add Dial Patterns

Dial Patterns are needed to route specific calls through Session Manager. For the compliance testing, dial patterns were needed to route calls from Communication Manager to Windstream and vice versa. Dial Patterns define which route policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing → Dial Patterns** in the left navigation pane and click on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

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

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

In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria. Lastly, select the routing policy from the list that will be used to route all calls that match the specified criteria. Click **Select**.

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

Two examples of the dial patterns used for the compliance testing were shown below, one for outbound calls from the enterprise to the PSTN and one for inbound calls from the PSTN to the enterprise.

The first example shows that 10-digit dialed numbers that begin with 613 and has a destination domain of “bvwddev7.com” uses route policy as defined in **Section 6.7**.

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

Commit Cancel

General

* Pattern: 613

* Min: 10

* Max: 10

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: bvwddev7.com

Notes: Windstream Outbound Calls

Originating Locations and Routing Policies

Add Remove

1 Item Refresh

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
Belleville	GSSCP Belleville	To Windstream	0	<input type="checkbox"/>	SBCE_TCP	To Windstream from SH/CM 5.2.1

Select : All, None

The second example shows that inbound 10-digit numbers that start with 469341816 to domain “bvwddev7.com” uses route policy as defined in **Section 6.7**. These are the DID numbers assigned to the enterprise by Windstream.

The screenshot shows the 'Dial Patterns' configuration page. The left sidebar has a menu with 'Dial Patterns' highlighted. The main area is titled 'Dial Pattern Details' and has a 'Commit' button. The 'General' section contains the following fields:

- Pattern:** 469341816
- Min:** 10
- Max:** 10
- Emergency Call:** ☐
- Emergency Priority:** 1
- Emergency Type:** (empty)
- SIP Domain:** bvwddev7.com
- Notes:** Inbound WS DID numbers

Below the 'General' section is a table titled 'Originating Locations and Routing Policies'. It has buttons for 'Add' and 'Remove' and a 'Refresh' link. The table has 7 columns: 'Originating Location Name', 'Originating Location Notes', 'Routing Policy Name', 'Rank', 'Routing Policy Disabled', 'Routing Policy Destination', and 'Routing Policy Notes'. There is one row with the following data:

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
Belleville	GSSCP Belleville	CM521 TRK50 Policy	0	<input type="checkbox"/>	CM521	WS SP testing

At the bottom of the table, there is a 'Select : All, None' option.

6.9. Add/View Session Manager

The creation of a Session Manager element provides the linkage between System Manager and Session Manager. This is most likely done as part of the initial Session Manager installation. To add a Session Manager, navigate to **Home → Elements → Session Manager → Session Manager Administration** in the left navigation pane and click on the **New** button in the right pane (not shown). If the Session Manager already exists, click **View** (not shown) to view the configuration. Enter/verify the data as described below and shown in the following screen:

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

- **SIP Entity Name:** Select the SIP Entity created for Session Manager.
- **Description:** Add a brief description (optional).
- **Management Access Point Host Name/IP:** Enter the IP address of the Session Manager management interface.
- **Directs Routing to Endpoints:** Enabled, to enable call routing on the Session Manager.

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

- **SIP Entity IP Address:** Should be filled in automatically based on the SIP Entity Name.
- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager.
- **Default Gateway:** Enter the IP address of the default gateway for Session Manager.

Use default values for the remaining fields. Click **Commint** to save (not shown).

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

The screenshot displays the 'View Session Manager' configuration page for 'SM63'. The left sidebar contains a navigation menu with 'Session Manager Administration' highlighted. The main content area is divided into two sections: 'General' and 'Security Module'. The 'General' section includes fields for 'SIP Entity Name' (SM63), 'Description', 'Management Access Point Host Name/IP' (110.33.10.25), 'Direct Routing to Endpoints' (Enable), and 'VMware Virtual Machine' (unchecked). The 'Security Module' section includes fields for 'SIP Entity IP Address' (110.33.10.26), 'Network Mask' (255.255.255.0), 'Default Gateway' (110.33.10.1), 'Call Control PHB' (46), 'QOS Priority' (6), 'Speed & Duplex' (Auto), and 'VLAN ID'.

General	
SIP Entity Name	SM63
Description	
Management Access Point Host Name/IP	110.33.10.25
Direct Routing to Endpoints	Enable
VMware Virtual Machine	<input type="checkbox"/>

Security Module	
SIP Entity IP Address	110.33.10.26
Network Mask	255.255.255.0
Default Gateway	110.33.10.1
Call Control PHB	46
QOS Priority	6
Speed & Duplex	Auto
VLAN ID	

7. Configure Avaya Session Border Controller for Enterprise

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

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

7.1. Avaya Session Border Controller for Enterprise Login

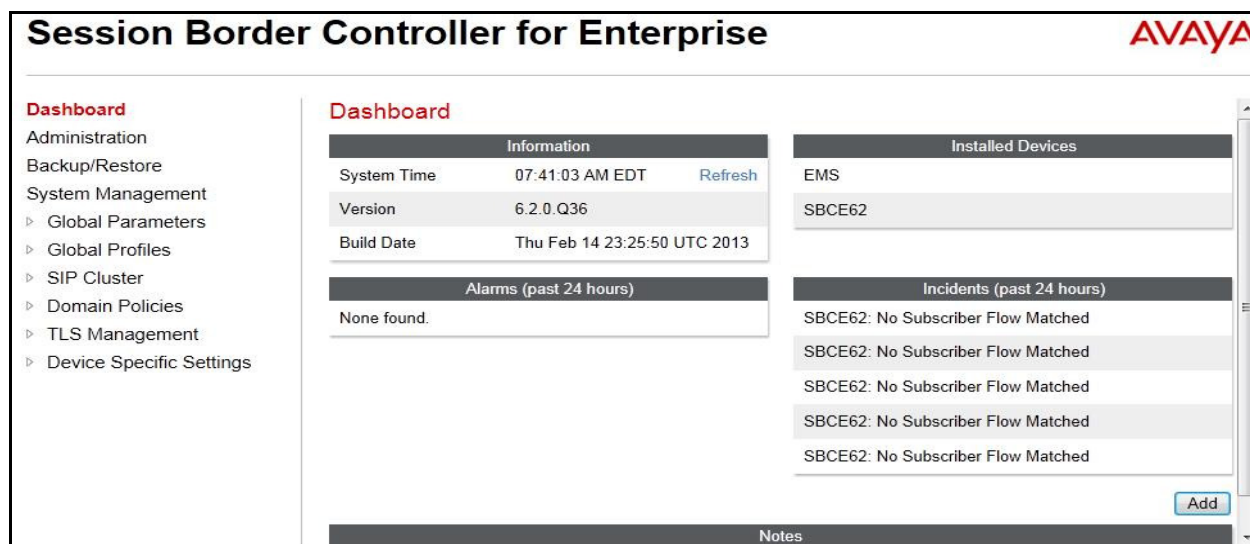
Use a Web browser to access the Unify Communication Security (UC-Sec) web interface, enter `https://<ip-addr>/ucsec` in the address field of the web browser (not shown), where `<ip-addr>` is the management LAN IP address of UC-Sec.

Enter appropriate credentials and click **Log In**.



The login page features the Avaya logo on the left. The main heading is "Session Border Controller for Enterprise". On the right, there is a "Log In" section with fields for "Username:" and "Password:", followed by a "Log In" button. Below the login fields, there is a disclaimer: "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." Another paragraph states: "The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials." A final note says: "All users must comply with all corporate instructions regarding the protection of information assets." At the bottom, it says "© 2011 - 2013 Avaya Inc. All rights reserved."

The main page of the Avaya SBCE will appear as shown below.



The dashboard has a left sidebar with a "Dashboard" header and a list of navigation items: Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, SIP Cluster, Domain Policies, TLS Management, and Device Specific Settings. The main content area is titled "Dashboard" and contains three panels. The "Information" panel shows System Time (07:41:03 AM EDT), Version (6.2.0.Q36), and Build Date (Thu Feb 14 23:25:50 UTC 2013). The "Alarms (past 24 hours)" panel shows "None found." The "Installed Devices" panel shows "EMS" and "SBCE62". The "Incidents (past 24 hours)" panel shows five entries, all stating "SBCE62: No Subscriber Flow Matched". There is an "Add" button at the bottom right of the incidents panel. A "Notes" section is at the bottom of the dashboard.

7.2. Global Profiles

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

7.2.1. Uniform Resource Identifier (URI) Groups

URI Group feature allows user to create any number of logical URI Groups that are comprised of individual SIP subscribers located in that particular domain or group. These groups are used by the various domain policies to determine which actions (Allow, Block, or Apply Policy) should be used for a given call flow.

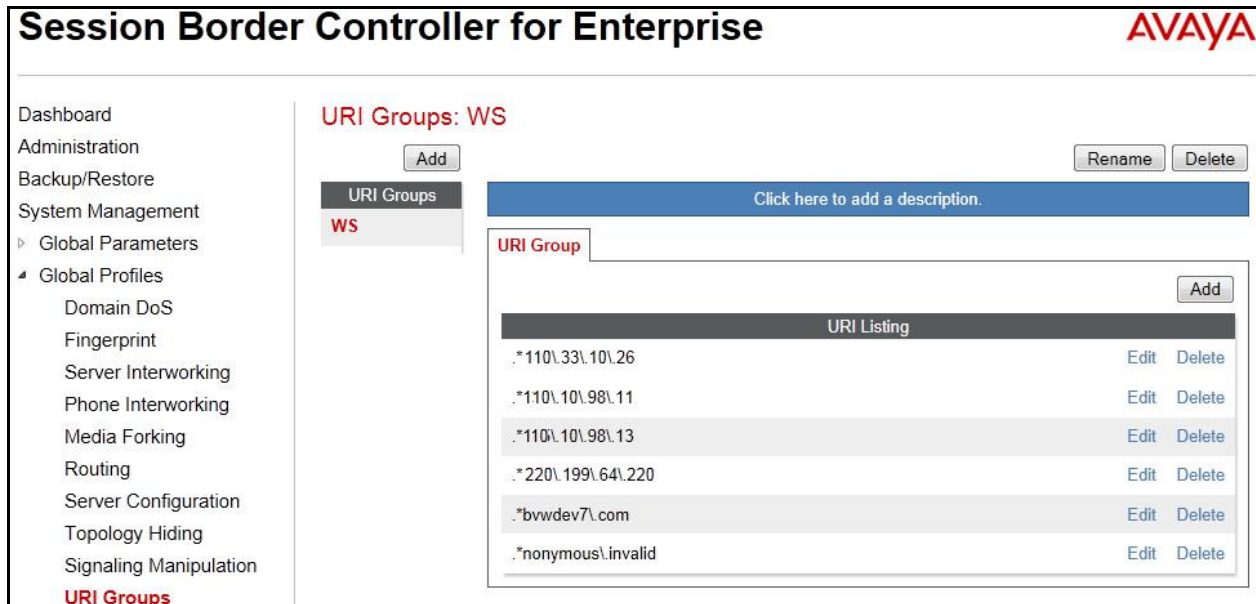
To add an URI Group, select **Global Profiles → URI Groups**. Click on **Add** button (not shown).

In the compliance testing, a URI Group named **WS** was added with URI type Regular Expression (not shown) and consists of:

- **.*bvwddev7\com**: Enterprise domain used for calls across the enterprise networks. This domain matches the domain configured for Communication Manager (see **Section 5.5** and **Section 5.6**) and Session Manager (see **Section 6.2**).
- **.*nonymous\invalid**: enterprise domain, defined to support private call.
- **.*110\10\98\111** and **.*220\199\64\220**: IP address based URI-Host, used for public calls to/from the service provider. The Avaya SBCE public IP address, 110.10.98.111, is set as URI-Host of the “From”, “PAI” and “Diversion” headers while the public IP address of Windstream, 220.199.64.220, is set as URI-Host of “Request-URI” and “To” headers.
- **.*110\33\10\26** and **.*110\10\97\189**: IP address based URI-Host, defined to support routing for the outbound OPTIONS heartbeat originated by Session Manager on the Entity Link to the Avaya SBCE (see **Section 6.6**). The OPTIONS will be forwarded by the Avaya SBCE to the service provider for response to confirm the status of the SIP trunk.

This URI-Group is used to match the “From” and “To” headers in a SIP call dialog received from both Session Manager and Windstream. If there is a match, the Avaya SBCE will apply the appropriate Routing Profile and Server Flow to route the inbound or outbound calls to the right destination. The Routing Profile and Server Flow are appropriately discussed in **Section 7.2.2** and **Section 7.4.4**.

The screenshot below illustrates the URI listing for the URI Group.



7.2.2. Routing Profiles

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.

To create a Routing Profile, select **Global Profiles → Routing**. Click on **Add** button (not shown).

In the compliance testing, a Routing Profile **SM63-to-WS** was created to use in conjunction with the server flow defined for Session Manager. This entry is to route the outbound call from the enterprise to Windstream.

In the opposite direction, a Routing Profile named **WS-to-SM63** was created to be used in conjunction with the server flow defined for Windstream. This entry is to route the inbound call from Windstream to the enterprise.

7.2.2.1 Routing Profile for Windstream

The screenshot below illustrates the **Global Profiles → Routing: SM63-to-WS**. As shown in **Figure 1**, Windstream SIP trunk is connected with transportation protocol UDP. If there is a match in the “To” header with the URI Group **WS** defined in **Section 7.2.1**, the call will be routed to the **Next Hop Server 1** which is the IP address of Windstream SIP trunk on port 5060.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with options: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (selected), Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, and Routing (highlighted in red). The main content area is titled "Routing Profiles: SM63-to-WS" and includes an "Add" button, "Rename", "Clone", and "Delete" buttons. Below this is a table for the Routing Profile configuration:

Priority	URI Group	Next Hop Server 1	Next Hop Server 2
1	WS	220.199.64.220:5060	---

Buttons for "View" and "Edit" are located next to the last row. A blue bar at the top of the table area says "Click here to add a description."

7.2.2.2 Routing Profile for Session Manager

The Routing Profile **WS-to-SM63** was defined to route call where the “To” header matches the URI Group **WS** defined in **Section 7.2.1** to **Next Hop Server 1** which is the IP address of Session Manager, on port 5060 as a destination. As shown in **Figure 1**, SIP trunk between Session Manager and the Avaya SBCE is connected with transportation protocol TCP.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with options: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (selected), Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, and Routing (highlighted in red). The main content area is titled "Routing Profiles: WS-to-SM63" and includes an "Add" button, "Rename", "Clone", and "Delete" buttons. Below this is a table for the Routing Profile configuration:

Priority	URI Group	Next Hop Server 1	Next Hop Server 2
1	WS	110.33.10.26:5060	---

Buttons for "View" and "Edit" are located next to the last row. A blue bar at the top of the table area says "Click here to add a description."

7.2.3. Topology Hiding

Topology Hiding is an Avaya SBCE security feature which allows changing certain key SIP message parameters to ‘hide’ or ‘mask’ how the enterprise network may appear to an unauthorized or malicious user.

To create a Topology Hiding profile, select **Global Profiles → Topology Hiding**. Click on **Add** button (not shown).

In the compliance testing, two Topology Hiding profiles **SM3-to-WS** and **WS-to-SM63** were created.

7.2.3.1 Topology Hiding Profile for Windstream

Profile **SM63-to-WS** was defined to mask the enterprise SIP domain bvwdev7.com in “Request-URI” and “To” headers to IP **220.199.64.220** (the IP address Winsdread uses as URI-Host portion for “Request-URI” and “To” headers to meet the SIP specification requirement of Windstream); mask the enterprise SIP domain bvwdev7.com in the “From” and “PAI” headers to IP **110.10.98.111** (the Avaya SBCE public IP address); and replace Record-Route, Via headers and SDP (originated from Communication Manager) by external IP address known to Windstream. It is to secure the enterprise network topology and to meet the SIP requirement of the service provider.

Notes:

- The **Criteria** should be selected as **IP/Domain** to give the Avaya SBCE the capability to mask both domain name and IP address present in URI-Host.
- The masking applied on “From” header also applies to “Referred-By” and “P-Asserted-Identity” headers.
- The masking applied on “To” header also applies to “Refer-To” header.

The screenshots below illustrate the Topology Hiding profile **SM63-to-WS**.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with options like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, Routing, Server Configuration, Topology Hiding, and Signaling. The main content area is titled "Topology Hiding Profiles: SM63-to-WS" and includes an "Add" button, a list of profiles (SM63-to-WS and WS-to-SM63), and buttons for Rename, Clone, and Delete. Below this is a table for the "Topology Hiding" profile configuration.

Header	Criteria	Replace Action	Overwrite Value
From	IP/Domain	Overwrite	110.10.98.111
SDP	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	220.199.64.220
To	IP/Domain	Overwrite	220.199.64.220
Via	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---

7.2.3.2 Topology Hiding Profile for Communication Manager

Profile **WS-to-SM63** was also created to mask Windstream URI-Host in “Request-URI”, “From”, “To” headers to the enterprise domain bvwdev7.com, replace Record-Route, Via

headers and SDP added by Windstream by internal IP address known to Communication Manager.

Notes:

- The **Criteria** should be **IP/Domain** to give the Avaya SBCE the capability to mask both domain name and IP address present in URI-Host.
- The masking applied on “From” header also applies to “Referred-By” and “P-Asserted-Identity” headers.
- The masking applied on “To” header also applies to “Refer-To” header.

The screenshots below illustrate the Topology Hiding profile **WS-to-SM63**.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with options like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, Routing, Server Configuration, and Topology Hiding. The main content area is titled 'Topology Hiding Profiles: WS-to-SM63' and includes an 'Add' button, a list of profiles (SM63-to-WS and WS-to-SM63), and a table for configuring the profile. The table has columns for Header, Criteria, Replace Action, and Overwrite Value. The 'WS-to-SM63' profile is selected, and the table shows the following configuration:

Header	Criteria	Replace Action	Overwrite Value
From	IP/Domain	Overwrite	bvwdev7.com
SDP	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	bvwdev7.com
To	IP/Domain	Overwrite	bvwdev7.com
Via	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---

7.2.4. Server Interworking

Interworking Profile features are configured differently for Call Server and Trunk Server.

To create a Server Interworking profile, select **Global Profiles → Server Interworking**. Click on **Add** button (not shown).

In the compliance testing, two Server Interworking profiles were created for Windstream and Session Manager respectively.

7.2.4.1 Server Interworking profile for Windstream

Profile **WS_SI** was defined to match the specification of Windstream. The **General** and **Advanced** settings are configured with following parameters while the other settings for **Timers**, **URI Manipulation** and **Header Manipulation** are kept as default.

General settings:

- **Hold Support = None.** The Avaya SBCE will not modify the hold/ resume signaling from Communication Manager to Windstream.

- **18X Handling = *None*.** The Avaya SBCE will not handle 18X, it will keep the 18X messages unchanged from Communication Manager to Windstream.
- **Refer Handling = *No*.** The Avaya SBCE will not handle REFER. It will keep the REFER message unchanged from Communication Manager to Windstream.
- **T.38 Support = *No*.** Windstream does not support T.38 fax in the compliance testing.
- **Privacy Enabled = *No*.** The Avaya SBCE will not mask the “From” header with anonymous for the outbound call to Windstream. It depends on Communication Manager to enable/ disable privacy on individual call basis.
- **DTMF Support = *None*.** The Avaya SBCE will send original DTMF method from Communication Manager to Windstream.

Advanced settings:

- **Record Routes = *Both Sides*.** The Avaya SBCE will send “Record-Route” header to both call and trunk servers.
- **Topology Hiding: Change Call-ID = *Yes*.** The Avaya SBCE will modify “Call-ID” header for the call toward Windstream.
- **Change Max Forwards= *Yes*.** The Avaya SBCE will adjust the original Max-Forwards value from Communication Manager to Windstream by reducing the intermediate hops involving in the call flow.
- **Has Remote SBC = *Yes*.** Windstream has SBC which interfaces its Central Office (CO) which interfaces to the enterprise SIP trunk. This setting allows the Avaya SBCE to always use the SDP received from Windstream for the media.

The screenshots below illustrate the Server Interworking profile **WS_SI**.

Dashboard

Administration

Backup/Restore

System Management

Global Parameters

Global Profiles

Domain DoS

Fingerprint

Server Interworking

Phone Interworking

Media Forking

Routing

Server Configuration

Topology Hiding

Signaling Manipulation

URI Groups

SIP Cluster

Domain Policies

TLS Management

Device Specific Settings

Interworking Profiles: WS_SI

Add

Interworking Profiles

SM63_WS_SI

WS_SI

Rename

Clone

Delete

Click here to add a description.

GeneralTimersURI ManipulationHeader ManipulationAdvanced

General

Hold SupportNONE

180 HandlingNone

181 HandlingNone

182 HandlingNone

183 HandlingNone

Refer HandlingNo

3xx HandlingNo

Diversion Header SupportNo

Delayed SDP HandlingNo

T.38 SupportNo

URI SchemeSIP

Via Header FormatRFC3261

Privacy

Privacy EnabledNo

User Name

P-Asserted-IdentityNo

P-Preferred-IdentityNo

Privacy Header

DTMF

DTMF SupportNone

Edit

Dashboard

Administration

Backup/Restore

System Management

Global Parameters

Global Profiles

Domain DoS

Fingerprint

Server Interworking

Phone Interworking

Media Forking

Routing

Server Configuration

Topology Hiding

Signaling Manipulation

URI Groups

SIP Cluster

Domain Policies

TLS Management

Device Specific Settings

Interworking Profiles: WS_SI

Add

Interworking Profiles

SM63_WS_SI

WS_SI

Rename

Clone

Delete

Click here to add a description.

GeneralTimersURI ManipulationHeader ManipulationAdvanced

Advanced

Record RoutesBoth

Topology Hiding: Change Call-IDYes

Call-Info NATNo

Change Max ForwardsYes

Include End Point IP for Context LookupNo

OCS ExtensionsNo

AVAYA ExtensionsNo

NORTEL ExtensionsNo

Diversion ManipulationNo

Metaswitch ExtensionsNo

Reset on Talk SpurtNo

Reset SRTP Context on Session RefreshNo

Has Remote SBCYes

Route Response on Via PortNo

Cisco ExtensionsNo

Edit

7.2.4.2 Server Interworking profile for Session Manager

Profile **SM63_WS_SI** was defined to match the specification of Communication Manager. The **General** and **Advanced** settings are configured with the following parameters while the other settings for **Timers**, **URI Manipulation** and **Header Manipulation** are kept as default.

General settings:

- **Hold Support** = *RFC3264*. Communication Manager supports hold/ resume as per RFC3264.
- **18X Handling** = *None*. The Avaya SBCE will not handle 18X, it will keep the 18X messages unchanged from Windstream to Communication Manager.
- **Refer Handling** = *No*. The Avaya SBCE will not handle REFER, it will keep the REFER messages unchanged from Windstream to Communication Manager.
- **T.38 Support** = *No*. Windstream does not support T.38 fax in the compliance testing.
- **Privacy Enabled** = *None*. The Avaya SBCE will not mask the “From” header with anonymous for inbound call from Windstream. It depends on the Windstream to enable/disable privacy on individual call basis.
- **DTMF Support** = *None*. The Avaya SBCE will send original DTMF method from Windstream to Communication Manager.

Advanced settings:

- **Record Routes** = *Both Sides*. The Avaya SBCE will send Record-Route header to both call and trunk servers.
- **Topology Hiding: Change Call-ID** = *No*. The Avaya SBCE will modify “Call-ID” header for the call toward Communication Manager.
- **Change Max Forwards** = *Yes*. The Avaya SBCE will adjust the original Max-Forwards value from Windstream to Communication Manager by reducing the intermediate hops involving in the call flow.
- **Has Remote SBC** = *Yes*. This setting allows the Avaya SBCE to always use the SDP received from Communication Manager for the media.

The screenshots below illustrate the Server Interworking profile **SM63_WS_SI**.

Dashboard

Administration

Backup/Restore

System Management

Global Parameters

Global Profiles

- Domain DoS
- Fingerprint
- Server Interworking**
- Phone Interworking
- Media Forking
- Routing
- Server Configuration
- Topology Hiding
- Signaling Manipulation
- URI Groups

SIP Cluster

Domain Policies

TLS Management

Device Specific Settings

Interworking Profiles

SM63_WS_SI

WS_SI

Add

Interworking Profiles: SM63_WS_SI

RenameCloneDelete

Click here to add a description.

GeneralTimersURI ManipulationHeader ManipulationAdvanced

General

Hold Support	RFC2543
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
T.38 Support	No
URI Scheme	SIP
Via Header Format	RFC3261

Privacy

Privacy Enabled	No
User Name	
P-Asserted-Identity	No
P-Preferred-Identity	No
Privacy Header	

DTMF

DTMF Support	None
--------------	------

Edit

Dashboard

Administration

Backup/Restore

System Management

Global Parameters

Global Profiles

- Domain DoS
- Fingerprint
- Server Interworking**
- Phone Interworking
- Media Forking
- Routing
- Server Configuration
- Topology Hiding
- Signaling Manipulation
- URI Groups

SIP Cluster

Domain Policies

TLS Management

Device Specific Settings

Interworking Profiles

SM63_WS_SI

WS_SI

Add

Interworking Profiles: SM63_WS_SI

RenameCloneDelete

Click here to add a description.

GeneralTimersURI ManipulationHeader ManipulationAdvanced

Advanced

Record Routes	Both
Topology Hiding: Change Call-ID	No
Call-Info NAT	No
Change Max Forwards	Yes
Include End Point IP for Context Lookup	No
OCS Extensions	No
AVAYA Extensions	Yes
NORTEL Extensions	No
Diversion Manipulation	No
Metaswitch Extensions	No
Reset on Talk Spurt	No
Reset SRTP Context on Session Refresh	No
Has Remote SBC	Yes
Route Response on Via Port	No
Cisco Extensions	No

Edit

7.2.5. Signaling Manipulation

Signaling Manipulation feature allows the ability to add, change and delete any of the headers in a SIP message. This feature will add the ability to configure such manipulation in a highly flexible manner using a proprietary scripting language called SigMa. The SigMa scripting language is designed to express any of the SIP header manipulations done by the Avaya SBCE. Using this language, a script can be written and tied to a given Server.

Configuration (see **Section** Error! Reference source not found.) through the Avaya SBCE Web interface. The Avaya SBCE appliance then interprets this script at the given entry point or “hook point”.

These Application Notes will not discuss the full feature of the Signaling Manipulation but will show an example of a script created during compliance testing to aid in Topology Hiding.

To create a Signaling Manipulation script, select **Global Profiles → Signaling Manipulation** then click on the **Add Script** button (not shown).

In the compliance testing, SigMa script **OutboundChgContact** was created for Server Configuration for Windstream.

The statement **act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"** is to specify the script will take effect on all type of SIP messages for outgoing calls to Windstream and the manipulation will be done after routing. The manipulation will be according to the rules contained in this statement.

The statement **act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"** is to specify the script will take effect on all type of SIP messages for outgoing calls to Windstream and the manipulation will be done after routing. The manipulation will be according to the rules contained in this statement.

In the compliance testing, the manipulation is created as shown bellow.

Signaling Manipulation Scripts: OutboundChgContact

Upload Add Download Clone Delete

Click here to add a description.

Signaling Manipulation

```
// Windstream - remove "epv" in Contact header
{
  within session "All"
  {
    act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
    {
      // Remove unwanted Headers
      remove(%HEADERS["contact"][1].URI.PARAMS["epv"]);
      remove(%HEADERS["History-Info"][3]);
      remove(%HEADERS["History-Info"][2]);
      remove(%HEADERS["History-Info"][1]);
      remove(%HEADERS["Alert-Info"][1]);
      remove(%HEADERS["x-nt-e164-clid"][1]);
      remove(%HEADERS["P-AV-Message-Id"][1]);
      remove(%HEADERS["P-Changing-Vector"][1]);
      remove(%HEADERS["Av-Global-Session-ID"][1]);
    }
  }
  act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
  {
    %HEADERS["Request_Line"][1].regex_replace("sip:ping@110.10.98.111:5060","sip:110.10.98.111:5060");
  }
}
```

Edit

7.2.6. Server Configuration

Server Configuration screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. These tabs are used to configure and manage various SIP Call Server specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics and trusted domains.

To create a Server Configuration entry, select **Global Profiles → Server Configuration**. Click on **Add** button (not shown).

In the compliance testing, two separate Server Configurations were created, server entry **WS_SC** for Windstream and server entry **SM63_SC** for Session Manager.

7.2.6.1 Server Configuration for Windstream

Server Configuration named **WS_SC** was created for Windstream. It will be discussed in detail as below. **General** and **Advanced** tabs are provisioned but no configuration is done for **Authentication** tab as Windstream does not implement authentication on the SIP trunk. The **Heartbeat** tab is kept as disabled as default to allow the Avaya SBCE to forward the OPTIONS heartbeat from Session Manager to Windstream to query the status of the SIP trunk. The additional **DoS Whitelist** and **DoS Protection** tabs are displayed after DoS Protection is enabled under **Advanced** tab, the settings for these tabs are kept as default.

In the **General** tab, click on **Edit** button to set **Server Type** for Windstream to **Trunk Server** (not shown). In the compliance testing, Windstream supported UDP and listened on port 5060.

Dashboard

Administration

Backup/Restore

System Management

Global Parameters

Global Profiles

Domain DoS

Fingerprint

Server Interworking

Phone Interworking

Media Forking

Routing

Server Configuration

Server Configuration: WS_SC

Add

Server Profiles

SM63_SC

WS_SC

General

Authentication

Heartbeat

Advanced

DoS Whitelist

DoS Protection

Server Type

Trunk Server

IP Addresses / FQDNs

220.199.64.220

Supported Transports

UDP

UDP Port

5060

Edit

Under **Advanced** tab, check on **Enable DoS Protection** (not shown) For **Interworking Profile** drop down list, select **WS_SI** as defined in **Section 7.2.4**. For **Signaling Manipulation Script**, select **OutboundChgContact**, which is created in **Section 7.2.5**. This configuration applies the specific SIP profile to the Windstream traffic. The other settings are kept as default.

Dashboard
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
Domain DoS
Fingerprint
Server Interworking
Phone Interworking
Media Forking
Routing
Server Configuration

Server Configuration: WS_SC

Add Rename Clone Delete

Server Profiles
SM63_SC
WS_SC
BellCanada
CS1K76
Frontier

General Authentication Heartbeat **Advanced** DoS Whitelist DoS Protection

Enable DoS Protection ☒
Enable Grooming ☐
Interworking Profile WS_SI
Signaling Manipulation Script OutboundChgContact
UDP Connection Type SUBID
Edit

7.2.6.2 Server Configuration for Session Manager

Server Configuration named **SM63_SC** was created for Session Manager is discussed in detail below. **General** and **Advanced** tabs are provisioned but no configuration is done for **Authentication** tab. The **Heartbeat** tab is kept as disabled as default to allow the Avaya SBCE to forward the OPTIONS heartbeat from Windstream to Session Manager to query the status of the SIP trunk.

In the **General** tab, click on **Edit** button to specify **Server Type** for Session Manager as **Call Server** (not shown). In the compliance testing, the link between the Avaya SBCE and Session Manager was TCP and Session Manager listened on port 5060.

Dashboard
Administration
Backup/Restore
System Management
Global Parameters
Global Profiles
Domain DoS
Fingerprint
Server Interworking
Phone Interworking
Media Forking
Routing
Server Configuration

Server Configuration: SM63_SC

Add Rename Clone Delete

Server Profiles
SM63_SC
WS_SC

General **Authentication** Heartbeat Advanced

Server Type Call Server
IP Addresses / FQDNs 110.33.10.26
Supported Transports TCP
TCP Port 5060
Edit

Under **Advanced** tab, click on **Edit** button (not shown), for **Interworking Profile** drop down list select **SM63_WS_SI** as defined in **Section 7.2.4** and for **Signaling Manipulation Script** drop down list select **None**. The other settings are kept as default.

The screenshot displays the 'Server Configuration: SM63_SC' window. On the left, a sidebar lists navigation options: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (with sub-items: Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, Routing), and Server Configuration (highlighted). The main panel has a title bar with 'Add', 'Rename', 'Clone', and 'Delete' buttons. Below the title bar are tabs for 'General', 'Authentication', 'Heartbeat', and 'Advanced' (selected). The 'Advanced' tab contains a table of settings:

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	SM63_WS_SI
Signaling Manipulation Script	None
TCP Connection Type	SUBID

An 'Edit' button is located at the bottom right of the settings table.

7.3. Domain Policies

Domain Policies feature configures various rule sets (policies) to control unified communications based upon criteria of communication sessions originating from or terminating at the enterprise. These criteria can be used to trigger policies which, in turn, activate various security features of the UC-Sec security device to aggregate, monitor, control and normalize call flow. There are default policies available for use, or a custom domain policy can be created.

7.3.1. Application Rules

Application Rules define which types of SIP-based Unified Communications (UC) applications the UC-Sec security device will protect: voice, video, and/or Instant Messaging (IM). In addition, it is possible to configure the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion.

Application Rule is created to set the number of concurrent voice traffic. The sample configuration is cloned and modified to increase the number of **Maximum Concurrent Session** and **Maximum Sessions Per Endpoint**.

To clone an Application Rule, navigate to **Domain Policies → Application Rules**. With the default rule chosen, click on **Clone** button (not shown).

Enter a rule with a descriptive name **WS_AR** and click **Finish** (not shown).

Click **Edit** button (not shown) to modify the rule. Set the **Maximum Concurrent Sessions** and **Maximum Session Per Endpoint** for the **Voice** application to a value high enough for the amount of traffic the network is able process. The following screen shows the modified **Application Rule** with the **Maximum Concurrent Sessions** and **Maximum Session Per Endpoint** set to 1000 (not shown). In the compliance testing, Communication Manager is programmed to control the concurrent sessions by setting the number of members in the trunk

group (Section 5.7) to the allotted number. Therefore, the values in the **Application Rule** named **WS_AR** are set high enough to be considered non-blocking.

Application Rules: WS_AR

Buttons: Add, Filter By Device..., Rename, Clone, Delete

Click here to add a description.

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Voice	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1000	1000
Video	<input type="checkbox"/>	<input type="checkbox"/>		
IM	<input type="checkbox"/>	<input type="checkbox"/>		

Miscellaneous

CDR Support	None
RTCP Keep-Alive	No

Edit

7.3.2. Media Rules

Media Rules 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 packet matching the criteria will be handled by the UC-Sec security product.

A custom Media Rule is created to set the **Quality of Service** and **Media Anomaly Detection**. The sample configuration shows Media Rule **DH_MR** used for both the enterprise and Windstream.

In the compliance testing, Media Rule **WS_MR** is clone from the **default-low-med** Media Rule.

To create Media Rule, navigate to **Domain Policies** → **Media Rules**. With **default-low-med** selected, click **Clone** button (not shown).

Enter a Media Rule with a descriptive name **WS_MR** and click **Finish** (not shown).

7.3.3. Signaling Rules

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

To clone a Signaling Rule, navigate to **Domain Policies** → **Signaling Rules**. With the **default** rule chosen, click on **Clone** button (not shown).

In the compliance testing, two Signaling Rules; **WS_SR** and **SM63_WS_SR**, were created from **default** Signaling Rules for Windstream and Session Manager respectively (not shown).

7.3.4. Endpoint Policy Groups

The rules created within the **Domain Policy** section are assigned to an **Endpoint Policy Group**. The **Endpoint Policy Group** is then applied to a **Server Flow** defined in the next section.

Endpoint Policy Groups were created for the Windstream and the Session Manager.

To create a new policy group, navigate to **UC-Sec Control Center → Domain Policies → Endpoint Policy Groups** and click on **Add Group** (not shown).

7.3.4.1 Endpoint Policy Group for Windstream

The following screen shows **WS_PG** created for Windstream:

- Set Application Rule to **WS_AR** as created in **Section 7.3.1**.
- Set Media Rule to **WS_MR** as created **Section 7.3.2**.
- Set Signaling Rule to **WS_SR** as created in **Section Error! Reference source not found.**
- Set Border Rule to **default**.
- Set Time of Day Rule to **default**.
- Set Security Rule to **default-high**.

Policy Groups: WS-PG

Buttons: Add, Filter By Device..., Rename, Delete

Policy Groups:

- default-low
- default-low-enc
- default-med
- default-med-e...
- default-high
- WS-PG**

Click here to add a description.

Hover over a row to see its description.

Policy Group

Buttons: Summary, Add

Order	Application	Border	Media	Security	Signaling	Time of Day	
1	WS_AR	default	WS_MR	default-high	WS_SR	default	Edit Clone

7.3.4.2 Endpoint Policy Group for Session Manager

The following screen shows **SM63_WS_PG** created for Session Manager:

- Set Application Rule to **WS_AR** as created in **Section 7.3.1**.
- Set Media Rule to **WS_MR** as created **Section 7.3.2**.
- Set Signaling Rule to **SM63_WS_SR** as created in **Section Error! Reference source not found**.
- Set Border Rule to **default**.
- Set Time of Day Rule to **default**.
- Set Security Rule to **default-low**.

The screenshot shows the 'Policy Groups: SM63_WS_PG' configuration page. On the left is a navigation menu with options like Dashboard, Administration, Backup/Restore, System Management, SIP Cluster, and Domain Policies. The 'Domain Policies' section is expanded, showing 'End Point Policy Groups' selected. The main area displays a list of policy groups: default-low, default-low-enc, default-med, default-med-e..., SM63_WS_PG (highlighted in red), and WS-PG. Below this list is a table for the selected 'Policy Group'. The table has columns: Order, Application, Border, Media, Security, Signaling, Time of Day, and actions (Edit, Clone). The first row shows Order 1, Application WS_AR, Border default, Media WS_MR, Security default-low, Signaling SM63_WS_SR, Time of Day default, and Edit/Clone buttons. Above the table are buttons for 'Add', 'Filter By Device...', 'Rename', and 'Delete'. There are also instructions to 'Click here to add a description' and 'Hover over a row to see its description'.

7.3.5. Session Policy

Session Policy is applied based on the source and destination of a media session i.e., which codec is to be applied to the media session between its source and destination. The source and destination are defined in URI Group in **Section 7.2.1**.

In the compliance testing, a Session Policy named **SM-WS-SP** was created to allow Avaya SBCE to anchor media in off-net call forward or off-net call transfer scenarios. It is applied to both Server Configurations for Communication Manager and Windstream.

To clone a Session Policy, navigate to **Domain Policies → Session Policies**. With the **default** rule chosen, click on **Clone** button (not shown).

Enter a descriptive name **SM_WS_SP** for the new policy and click **Finish** (not shown).

Session Policies: SM-WS-SP

Media Anchoring ☒

Media Forking Profile

7.4. Device Specific Settings

Device Specific Settings feature allows aggregate system information to be viewed and various device-specific parameters to be managed to determine how a particular device will function when deployed in the network. Specifically, it gives the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality and protocol scrubber rules, end-point and session call flows, as well as the ability to manage system logs and control security features.

7.4.1. Network Management

Network Management screen is where the network interface settings are configured and enabled. During the installation process of the Avaya SBCE, certain network-specific information was defined such as device IP address(es), public IP address(es), netmask, gateway, etc. to interface the device to the network. This information populates the various **Network Management** tab, which can be edited as needed to optimize device performance and network efficiency.

Navigate to **Device Specific Settings → Network Management** and under **Network Configuration** tab verify the IP addresses assigned to the interfaces and that the interfaces are enabled. The following screen shows the private interface is assigned to **A1** and the public interface is assigned to **B1**.

Session Border Controller for Enterprise AVAYA

Network Management: SBCE62

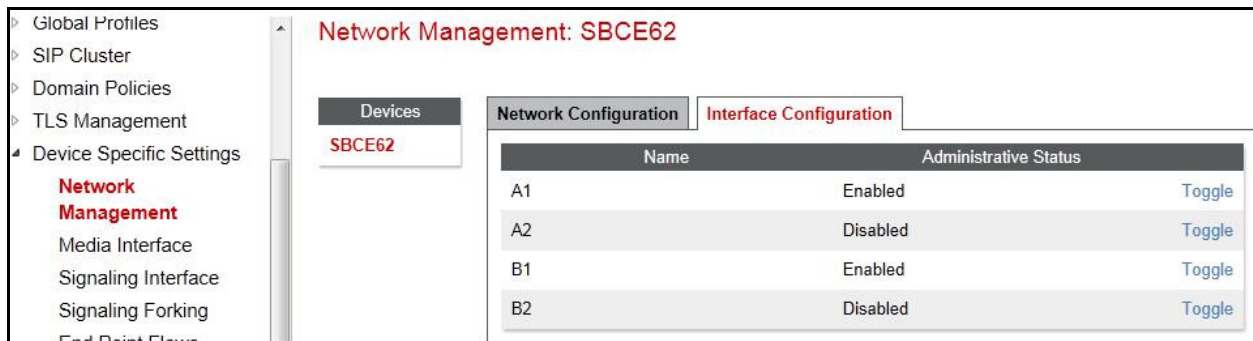
SBCE62

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

A1 Netmask	A2 Netmask	B1 Netmask	B2 Netmask
255.255.255.192		255.255.255.224	

IP Address	Public IP	Gateway	Interface
110.10.98.13		110.10.98.1	A1 <input type="button" value="Delete"/>
110.10.98.111		110.10.98.97	B1 <input type="button" value="Delete"/>

Enable the interfaces used to connect to the inside and outside networks on the **Interface Configuration** tab. The following screen shows interface **A1** and **B1** are **Enabled**. To enable an interface click it's **Toggle** button.



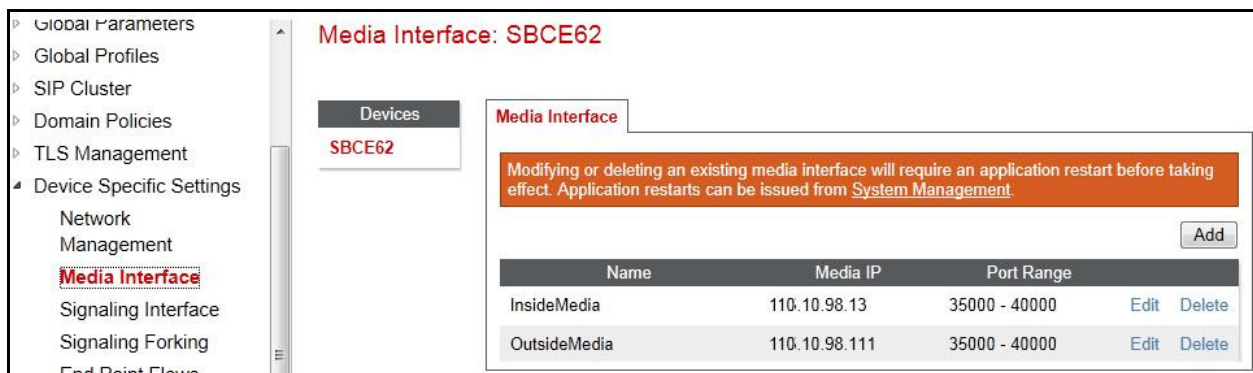
7.4.2. Media Interface

Media Interface screen is where the media ports are defined. The Avaya SBCE will open connection for RTP on the defined ports.

To create a new Media Interface, navigate to **Device Specific Settings → Media Interface** and click **Add Media Interface** (not shown).

Separate Media Interfaces were created for both inside and outside interfaces. The following screen shows the Media Interfaces created in the compliance testing.

Note: After the media interfaces are created, an application restart is necessary before the changes will take effect.

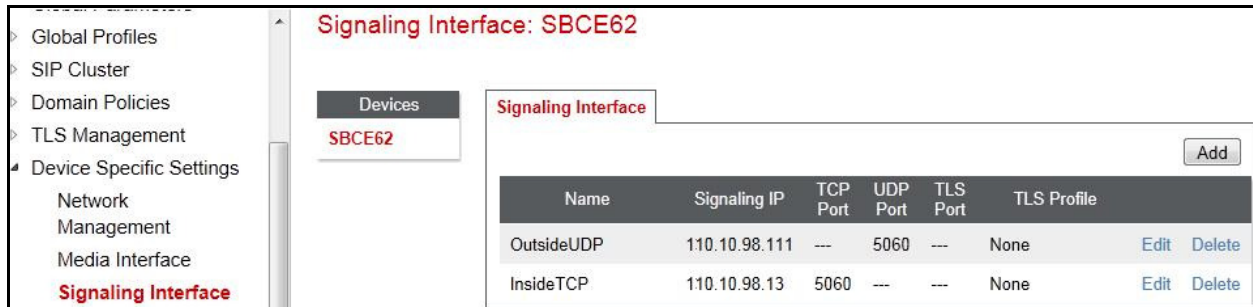


7.4.3. Signaling Interface

Signaling Interface screen is where the SIP signaling port is defined. The Avaya SBCE will listen for SIP requests on the defined port.

To create a new Signaling Interface, navigate to **Device Specific → Settings → Signaling Interface** and click **Add Signaling Interface** (not shown).

Separate Signaling Interface was created for both inside and outside interfaces. The following screen shows the Signaling Interfaces were created in the compliance testing with UDP/5060 for outside interface to Windstream and TCP/5060 for the inside interface to SM.



Signaling Interface: SBCE62						
Signaling Interface						
Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
OutsideUDP	110.10.98.111	---	5060	---	None	Edit Delete
InsideTCP	110.10.98.13	5060	---	---	None	Edit Delete

7.4.4. End Point Flows - Server Flow

When a packet is received by UC-Sec, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow. The following screen illustrates the flow through the Avaya SBCE to secure a SIP Trunk call.

In the compliance testing, separate Server Flows were created for Windstream and Session Manager. To create a Server Flow, navigate to **Device Specific Settings → End Point Flows**. Select the **Server Flows** tab and click **Add Flow** (not shown). In the new window that appears, enter the following values. The other fields are kept default.

- **Flow Name:** Enter a descriptive name.
- **Server Configuration:** Select a Server Configuration created in **Section 7.2.5** to assign to the Flow.
- **URI Group:** Select the URI Group created in **Section 7.2.1** to assign to the Flow.
- **Received Interface:** Select the Signaling Interface created in **Section 7.4.3** the Server Configuration is allowed to receive SIP messages from.
- **Signaling Interface:** Select the Signaling Interface created in **Section 7.4.3** used to communicate with the Server Configuration.
- **Media Interface:** Select the Media Interface created in **Section 7.4.2** used to communicate with the Server Configuration.
- **End Point Policy Group:** Select the End Point Policy Group created in **Section 7.3.4** to assign to the Server Configuration.
- **Routing Profile:** Select the Routing Profile created in **Section 7.2.2** the Server Configuration will use to route SIP messages to.
- **Topology Hiding Profile:** Select the Topology-Hiding profile created in **Section 7.2.3** to apply to the Server Configuration.
- Click **Finish**.

The following screen shows the Server Flow **WS_SF** configured for Windstream.

Edit Flow: WS_SF	
Flow Name	WS_SF
Server Configuration	WS_SC
URI Group	WS
Transport	*
Remote Subnet	*
Received Interface	InsideTCP
Signaling Interface	OutsideUDP
Media Interface	OutsideMedia
End Point Policy Group	WS-PG
Routing Profile	WS-to-SM63
Topology Hiding Profile	SM63-to-WS
File Transfer Profile	None
Finish	

The following screen shows the Server Flow **SM63_WS_SF** configured for Session Manager.

Edit Flow: SM63_WS_SF	
Flow Name	SM63_WS_SF
Server Configuration	SM63_SC
URI Group	WS
Transport	*
Remote Subnet	*
Received Interface	OutsideUDP
Signaling Interface	InsideTCP
Media Interface	InsideMedia
End Point Policy Group	WS-PG
Routing Profile	SM63-to-WS
Topology Hiding Profile	WS-to-SM63
File Transfer Profile	None
Finish	

7.4.5. Session Flows

Session Flows feature allows defining certain parameters that pertain to the media portions of a call, whether it originates from the enterprise or outside the enterprise. This feature provides the complete and unparalleled flexibility to monitor, identify and control very specific types of calls based upon these user-definable parameters. Session Flows profiles SDP media parameters, to completely identify and characterize a call placed through the network.

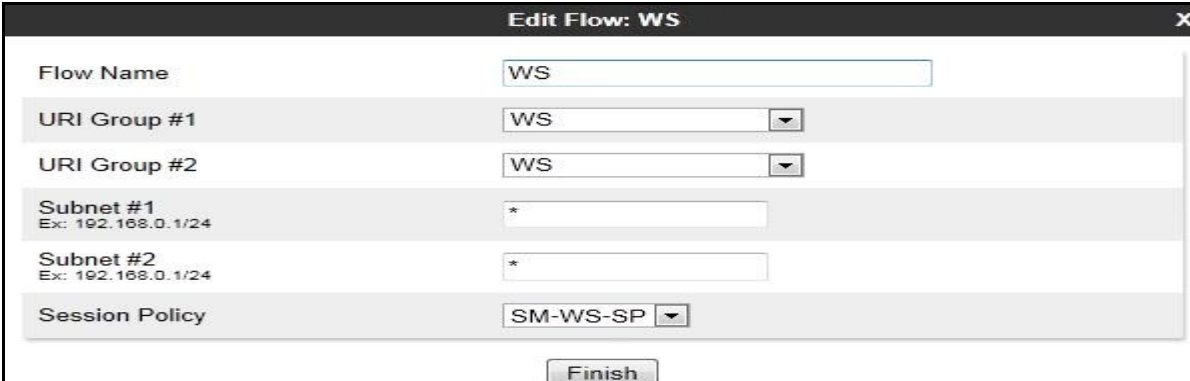
To create a session flow, navigate to **Device Specific Settings → Session Flows**. Click **Add Flow** (not shown).

A common Session Flow was created for both Windstream and Communication Manager. In the new window that appears, enter the following values. Use default values for the remaining fields:

- **Flow Name:** Enter a descriptive name.
- **URI Group #1:** Select the URI Group created in **Section 7.2.1** to assign to the Session Flow as the source URI Group.
- **URI Group #2:** Select the URI Group created in **Section 7.2.1** to assign to the Session Flow as the destination URI Group.
- **Session Policy:** Select the session policy created in **Section 7.3.5** to assign to the Session Flow.
- Click **Finish**.

Note: A unique URI Group is used for source and destination, since it contains multiple URIs defined for the source as well as for the destination.

The following screen shows the Session Flow named **WS** was created.



The screenshot shows a window titled "Edit Flow: WS" with a close button (X) in the top right corner. The window contains several configuration fields:

- Flow Name:** A text input field containing "WS".
- URI Group #1:** A dropdown menu with "WS" selected.
- URI Group #2:** A dropdown menu with "WS" selected.
- Subnet #1:** A text input field with a placeholder "*" and an example "Ex: 192.168.0.1/24".
- Subnet #2:** A text input field with a placeholder "*" and an example "Ex: 192.168.0.1/24".
- Session Policy:** A dropdown menu with "SM-WS-SP" selected.

At the bottom of the window is a "Finish" button.

8. Windstream SIP Trunking Service Configuration

Windstream is responsible for the configuration of its SIP Trunking Service. The customer will need to provide the IP address used to reach the Avaya SBCE at enterprise side. Windstream will provide the customer with the necessary information to configure the SIP connection from enterprise to the Windstream. The information provided by Windstream includes:

- IP address and port number used for signaling through security devices (if any).
- IP address and port number used for media through security devices (if any).
- Windstream SIP domain. In the compliance testing, Windstream preferred to use IP address as an URI-Host.
- CPE SIP domain. In the compliance testing, Windstream preferred to use IP address of the Avaya SBCE as an URI-Host.
- Supported codecs.
- DID numbers.

The sample configuration between Windstream and the enterprise for the compliance testing is a static configuration. There is no registration on the SIP trunk implemented on either Windstream or enterprise side.

9. Verification and Troubleshooting

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

9.1. Verification Steps

- Verify that endpoints at the enterprise site can place call to PSTN and that the call remains active for more than 35 seconds. This time period is included to satisfy SIP protocol timers.
- Verify that endpoints at the enterprise site can receive call from PSTN and that the call can remain active for more than 35 seconds. This time period is included satisfy SIP protocol timers.
- Verify that the user on PSTN can end an active call by hanging up.
- Verify that an endpoint at the enterprise site can end an active call by hanging up.

9.2. Protocol Traces

The following SIP headers are inspected using Wireshark trace analysis:

- Request-URI: verify the called party number and SIP domain.
- From: verify the calling party name and number.
- To: verify the called party name and number.
- P-Asserted-Identity: verify the calling party name and number.
- Privacy: verify the value “user” and/or “id” presents the private call scenario.

The following attributes in SIP message body are inspected using Wireshark trace analysis:

- Connection Information (c line): verify IP address of near end and far end endpoints.
- Time Description (t line): verify session timeout value of near end and far end endpoints.
- Media Description (m line): verify audio port, codec, DTMF event description.
- Media Attribute (a line): verify specific audio port, codec, ptime, send/ receive ability, DTMF event and fax attributes.

9.3. Troubleshooting:

9.3.1. The Avaya SBCE

Using a network sniffing tool (e.g. Wireshark) to monitor the SIP signaling messages between Windstream and the Avaya SBCE

Following is an example inbound call from Windstream to the enterprise

- Inbound INVITE request from Windstream:

```
INVITE sip:4693418165@110.10.98.111:5060;transport=udp SIP/2.0
Via: SIP/2.0/UDP 220.199.64.220:5060;branch=z9hG4bKn3rtgf006gghnm4j24s0.1
From: "BELLEVILLE
ON"<sip:6139675258@220.199.64.220;user=phone;broadworks=BWWESTSIGIS-
1ecpqcalh9ba>;tag=1589544696-1373644040784-
To: "4693418165 4693418165"<sip:4693418165@220.199.64.220;interopis=interopis-
h3bnp35pc3i58>
Call-ID: BW154720784120713224114444@220.199.51.199
CSeq: 700994857 INVITE
Contact: <sip:6139675258@220.199.64.220:5060;broadworks=BWWESTSIGIS-
o6i7c69dv2579;transport=udp>
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY
Accept: application/media_control+xml,application/sdp,multipart/mixed
Supported: timer
Min-SE: 60
Max-Forwards: 47
Content-Type: application/sdp
Content-Length: 283

v=0
o=BroadWorks 413524 1 IN IP4 220.199.64.220
s=-
c=IN IP4 220.199.64.220
t=0 0
m=audio 39002 RTP/AVP 18 0 8 101
a=sendrecv
a=ptime:20
a=rtpmap:18 G729/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=fmtp:18 annexb=no
```


- 200OK/SDP response by the enterprise:

```
SIP/2.0 200 OK
From: "BELLEVILLE ON"
<sip:6139675258@220.199.64.220;user=phone;broadworks=BWWESTSIGIS-
1ecpqcalh9ba>;tag=1589544696-1373644040784-
To: "4693418165 4693418165" <sip:4693418165@220.199.64.220;interopis=interopis-
h3bnp35pc3i58>;tag=80c8641611f9e21c2251f8fd3b00
CSeq: 700994857 INVITE
Call-ID: BW154720784120713224114444@220.199.51.199
Contact: "H323 9611" <sip:4693418165@110.10.98.111:5060;transport=udp;gsid=8eabf2d0-
eb0a-11e2-af59-e41f13b32ca8>
Record-Route: <sip:110.10.98.111:5060;ipcs-line=21565;lr;transport=udp>
Allow: INVITE, CANCEL, BYE, ACK, PRACK, SUBSCRIBE, NOTIFY, REFER, OPTIONS, INFO,
PUBLISH
Supported: timer, replaces, join
Via: SIP/2.0/UDP 220.199.64.220:5060;branch=z9hG4bKn3rtgf006gghnm4j24s0.1
Accept-Language: en
Require: timer
Server: Avaya CM/R015x.02.1.016.4 AVAYA-SM-6.3.2.0.632023
Session-Expires: 7200;refresher=uas
Content-Type: application/sdp
P-Location:
SM;origlocname="Belleville";origsiglocname="Belleville";origmedialocname="Belleville"
;termlocname="Belleville";termsiglocname="Belleville";termmedialocname="Belleville";s
maccounting="true"
Content-Length: 189

v=0
o=- 1 2 IN IP4 110.10.98.111
s=-
c=IN IP4 110.10.98.111
b=AS:64
t=0 0
m=audio 35052 RTP/AVP 18 101
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
```

Following is an example outbound call from the enterprise to Windstream.

- Outbound INVITE request from the enterprise:

```
INVITE sip:4693418165@110.10.98.111:5060;transport=udp SIP/2.0
Via: SIP/2.0/UDP 220.199.64.220:5060;branch=z9hG4bKgqqc1g1008qg7og1q4s1.1
From: "BELLEVILLE
ON"<sip:6139675258@220.199.64.220;user=phone;broadworks=BWWESTSIGIS-
1ecpqqcalh9ba>;tag=1360258443-1373649593464-
To: "4693418165 4693418165"<sip:4693418165@220.199.64.220;interopis=interopis-
h3bnp35pc3i58>
Call-ID: BW17195346412071360703@220.199.51.199
CSeq: 703771197 INVITE
Contact: <sip:6139675258@220.199.64.220:5060;broadworks=BWWESTSIGIS-
o6i7c69dv2579;transport=udp>
Diversion:
<sip:14693418165@220.199.51.199;user=phone>;reason=unavailable;counter=1,<sip:1469341
8165@220.199.51.199;user=phone>;reason=unavailable;counter=1
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY
Accept: application/media_control+xml,application/sdp,multipart/mixed
Supported: timer
Min-SE: 60
Max-Forwards: 47
Content-Type: application/sdp
Content-Length: 283

v=0
o=BroadWorks 413611 1 IN IP4 220.199.64.220
s=-
c=IN IP4 220.199.64.220
t=0 0
m=audio 39022 RTP/AVP 18 0 8 101
a=sendrecv
a=ptime:20
a=rtpmap:18 G729/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=fmtp:18 annexb=no
```

- 200OK/SDP response by Windstream:

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 220.199.64.220:5060;branch=z9hG4bKhale3q109040ln8ke481
From: <sip:ping@220.199.64.220>;tag=078cec2882d50a20112c71377df8506808060k1
To: <sip:ping@220.199.64.220>;tag=1e0c8bb65565d6c5
Call-ID: cac0ab4249c1289119703df97f46829008060k1@220.199.64.220
CSeq: 66408 OPTIONS
Allow: INVITE, ACK, CANCEL, OPTIONS, BYE, REFER, NOTIFY, INFO, UPDATE
Supported: timer
Server: IP Office 8.1 (69)
Content-Type: application/sdp
Content-Length: 189

v=0
o=UserA 3034237796 183833617 IN IP4 110.10.98.114
s=Session SDP
c=IN IP4 0.0.0.0
t=0 0
m=audio 8000 RTP/AVP 18 0
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:0 PCMU/8000
```

9.3.2. Communication Manager

- **list trace station** <extension number>. Traces call to and from a specific station.
- **list trace tac** <trunk access code number>. Trace call over a specific trunk group.
- **status station** <extension number>. Displays signaling and media information for an active call on a specific station.
- **status trunk** <trunk group number>. Displays trunk group information.
- **status trunk** <trunk group number/channel number>. Displays signaling and media information for an active trunk channel.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager 6.2, Avaya Aura® Session Manager 6.3 and Avaya Session Border Controller for Enterprise 6.2 to Windstream SIP Trunking Service. Windstream SIP Trunking Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large the enterprises. Windstream SIP Trunking Service provides a flexible, cost-saving alternative to traditional analog and ISDN-PRI trunks.

All of the test cases have been executed. Despite the number of observations seen during testing as noted in **Section 2.2**, the test results met the objectives outlined in **Section 2.1**. The Windstream SIP Trunking Service is considered **compliant** with Avaya Aura® Communication Manager 6.2, Avaya Aura® Session Manager 6.3 and Avaya Session Border Controller for Enterprise 6.2.

11. References

This section references the documentation relevant to these Application Notes. Additional Avaya product documentation is available at <http://support.avaya.com>.

- [1] *Installing and Configuring Avaya Aura® System Platform*, Release 6.2.1.0.9, December 2012.
- [2] *Administering Avaya Aura® System Platform*, Release 6.2.1, July 2012.
- [3] *Administering Avaya Aura® Communication Manager*, June 2010, Document Number 03-300509.
- [4] *Avaya Aura® Communication Manager Feature Description and Implementation*, June 2010, Document Number 555-245-205.
- [5] *Feature Description and Implementation for Avaya Communication Manager, Issue 5*, Document Number 555-245-205.
- [6] *Administrator Guide for Avaya Communication Manager*, February 2007, Issue 3, Document Number 03-300509.
- [7] *Implementing Avaya Aura® System Manager*, Release 6.3, December 2012.
- [8] *Upgrading Avaya Aura® System Manager to 6.3*, Release 6.3, January 2013.
- [9] *Administering Avaya Aura® System Manager*, Release 6.3, December 2012.
- [10] *Implementing Avaya Aura® Session Manager*, Release 6.3, Mar 2013.
- [11] *Administering Avaya Aura® Session Manager*, Release 6.3, December 2012.
- [12] *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Administrator Guide*, Release 3.1, November 2009, Document Number 16-300698.

- [13] *Avaya one-X® Deskphone SIP for 9600 Series IP Telephones Administrator Guide*, Release 2.6, June 2010, Document Number 16-601944.
- [14] *Administering Avaya one-X® Communicator*, April 2011.
- [15] *Using Avaya one-X® Communicator*, April 2011.
- [16] *UC-Sec Install Guide* (102-5224-400v1.01)
- [17] *UC-Sec Administration Guide* (010-5423-400v106)
- [18] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [19] *RFC 3515, The Session Initiation Protocol (SIP) Refer Method*, <http://www.ietf.org/>
- [20] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>

Product documentation for Windstream SIP Trunking Service is available from Windstream Communication.

©2013 Avaya Inc. All Rights Reserved.

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

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