



Avaya Solution & Interoperability Test Lab

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

Abstract

These Application Notes describe the steps to configure 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 Session Border Controller for Enterprise 6.2 and various Avaya endpoints. This documented solution does not extend to configurations without 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.

Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing	4
2.2.	Test Results	6
2.3.	Support.....	6
3.	Reference Configuration	7
4.	Equipment and Software Validated	9
5.	Configure Communication Manager	10
5.1.	Licensing and Capacity.....	10
5.2.	System Features	11
5.3.	IP Node Names	12
5.4.	Codecs.....	12
5.5.	IP Network Region	13
5.6.	Signaling Group.....	14
5.7.	Trunk Group.....	16
5.8.	Calling Party Information	18
5.9.	Inbound Routing	19
5.10.	Outbound Routing.....	19
5.11.	Saving Communication Manager Configuration Changes	20
6.	Configure Avaya Session Border Controller for Enterprise	21
6.1.	Avaya Session Border Controller for Enterprise Login.....	21
6.2.	Global Profiles	21
6.2.1.	Uniform Resource Identifier (URI) Groups.....	22
6.2.2.	Routing Profiles	23
6.2.3.	Topology Hiding	25
6.2.4.	Server Interworking	26
6.2.5.	Signaling Manipulation.....	31
6.2.6.	Server Configuration.....	32
6.3.	Domain Policies	34
6.3.1.	Application Rules.....	34
6.3.2.	Media Rules	35
6.3.3.	Signaling Rules	36
6.3.4.	Endpoint Policy Groups.....	36
6.3.5.	Session Policy	38
6.4.	Device Specific Settings	38
6.4.1.	Network Management.....	38
6.4.2.	Media Interface	39
6.4.3.	Signaling Interface	40
6.4.4.	End Point Flows - Server Flow	40
6.4.5.	Session Flows.....	42
7.	Windstream SIP Trunking Service Configuration.....	44
8.	Verification and Troubleshooting	44
8.1.	Verification Steps.....	44
8.2.	Protocol Traces	44

8.3.	Troubleshooting:	45
8.3.1.	The Avaya SBCE.....	45
8.3.2.	Communication Manager.....	49
9.	Conclusion	49
10.	References.....	49

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 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 include 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 include the following:

- T38 Fax.

2.2. Test Results

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

- **OPTIONS** - Windstream Communications SIP Trunking platform sent an OPTIONS message with request line header containing “SIP:ping@110.10.98.111”. This will not work with CM. The fix or workaround is to use a signalling manipulation script in the Avaya SBCE to convert to [SIP:110.10.98.111](http://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, an inbound call was made to the enterprise PBX. A vector redirected the call to another PSTN endpoint using REFER redirection message, when that was busy, the caller heard a busy tone. 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 include:

- Avaya S8800 Servers 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)
- Avaya one-X® Communicator soft phones (H.323)
- 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 Avaya Aura® Communication Manager is TCP.

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.

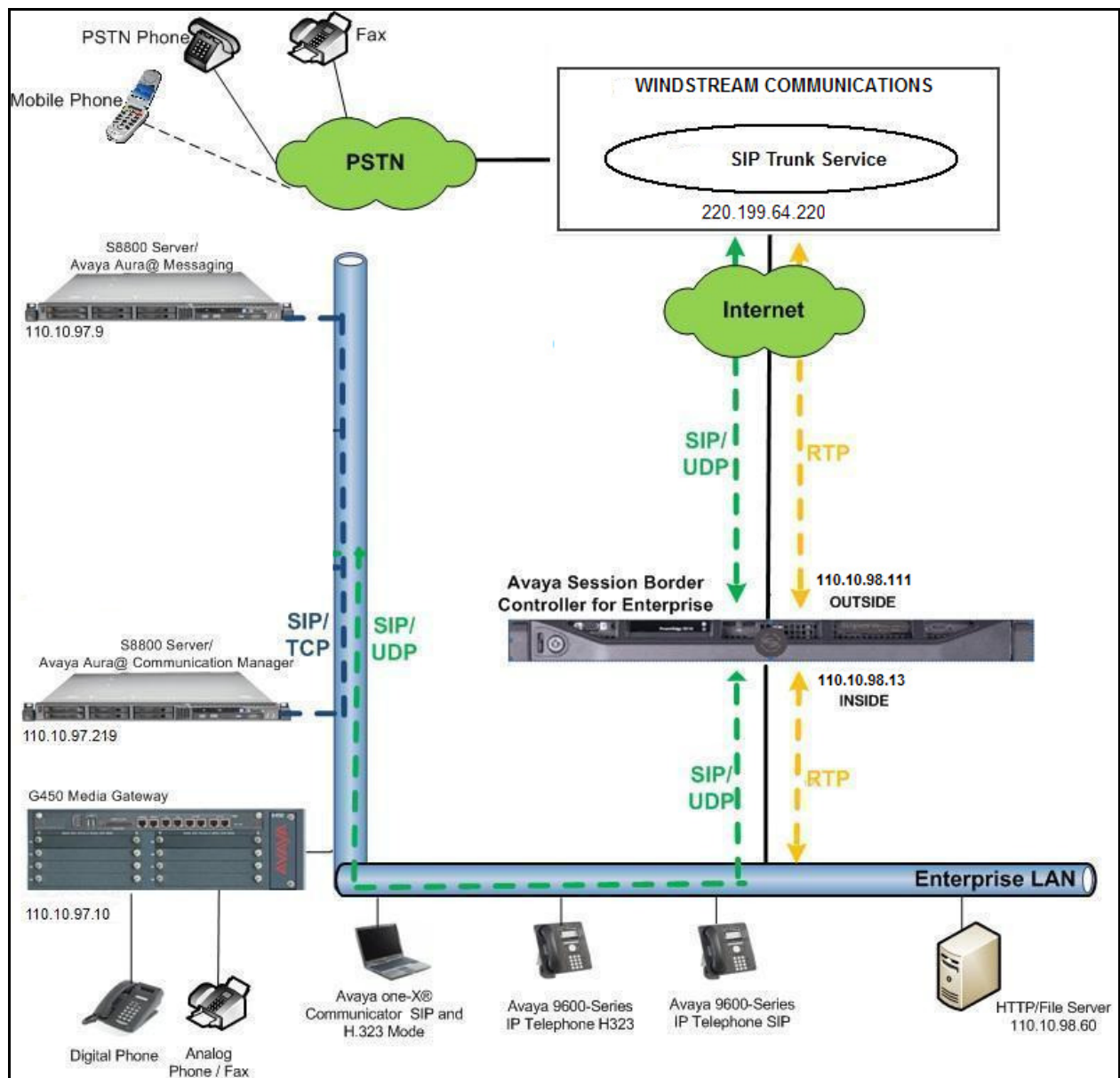


Figure 1: Avaya IP Telephony Network connecting to Windstream SIP Trunking Service

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® 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 one-X Communicator (H.323)	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	17sp4

Table 1: Equipment and Software Tested

Note: This solution will be compatible with other Avaya Server and Media Gateway platforms running similar versions 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 and Avaya G450 Media 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 calls from 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 calls and unavailable calls.

```
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 Avaya Session Border Controller for Enterprise (**ASBCE62**). 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	
ASBCE62	110.10.97.26	
DevAAM	110.33.10.9	
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 1. 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	Packet Size(ms)
1: G.729A	n	2	20
2: G.711MU	n	2	20
	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
	Mode	Redundancy
FAX	off	0
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 calls between the enterprise and the service provider versus calls 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 *bwvdev7.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: bwvdev7.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 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 calls 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 t
dst codec direct	WAN-BW-limits Video Intervening	Dyn A G c
rgn set WAN Units Total Norm Prio Shr Regions	CAC R L e	
1 1		all
2 1 y NoLimit	n	t
3 1 y NoLimit	n	t

Non-IP telephones (e.g., analog, digital) derive network region from the IP interface of 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 Avaya Session Border Controller (ASBCE) 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 ASBCE.
- 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 **ASBCE62**. This node name maps to the IP address of Avaya SBCE 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 ASBCE 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: ASBCE62	
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 the service provider. This value defines the interval a re-INVITE 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 5.98**).

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		
UI 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 4 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. Inbound Routing

In general, the incoming call handling treatment for a trunk group can be used to manipulate the digits received for an incoming call if necessary. DID number sent by Windstream can be mapped to an extension using the incoming call handling treatment of the receiving trunk-group. Use the **change inc-call-handling-trmt trunk-group** command to create an entry for each DID.

change inc-call-handling-trmt trunk-group 50					Page	1 of	3
INCOMING CALL HANDLING TREATMENT							
Service/ Feature	Number Len	Number Digits	Del	Insert			
public-ntwrk	10	4693418165	10	1130			
public-ntwrk	10	4693418166	10	1131			
public-ntwrk	10	4693418167	10	1132			
...							

5.10. 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 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:		
...				

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	Call	Node	ANI
		Min	Max	Pattern	Type	Num	Reqd
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 5.8**.

```

change route-pattern 50
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: 2      0
2:
....
      BCC VALUE  TSC CA-TSC      ITC BCIE Service/Feature PARM No. Numbering LAR
      0 1 2 M 4 W      Request      Dgts Format
1: y y y y y n  n      rest      lev0-pvt  none
...

```

5.11. 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 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.

6.1. Avaya Session Border Controller for Enterprise Login

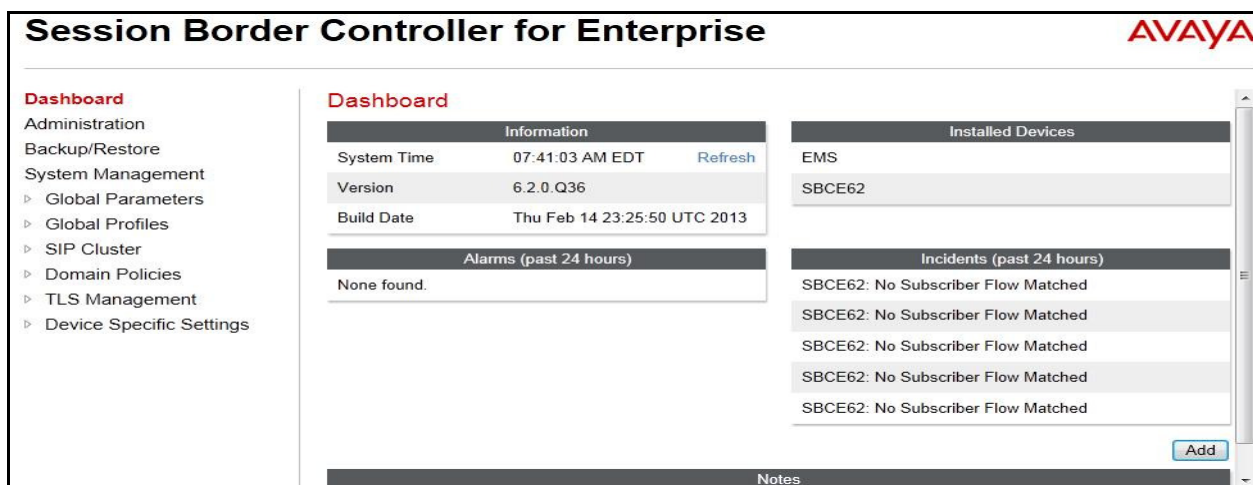
Use a Web browser to access the Unify Communication Security (UC-Sec) web interface, enter `https://<ip-addr>/ucsec` in the address field of the web browser (not shown), where `<ip-addr>` is the management LAN IP address of UC-Sec.

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



The login page features the Avaya logo in red at the top left. Below it, the text "Session Border Controller for Enterprise" is displayed. To 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. The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials. All users must comply with all corporate instructions regarding the protection of information assets." At the bottom right, it says "© 2011 - 2013 Avaya Inc. All rights reserved."

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



The dashboard is titled "Session Border Controller for Enterprise" with the Avaya logo in the top right. On the left is a "Dashboard" sidebar menu with options: Administration, Backup/Restore, System Management (Global Parameters, Global Profiles, SIP Cluster, Domain Policies, TLS Management, Device Specific Settings). The main content area is divided into several sections: "Information" (System Time: 07:41:03 AM EDT, Version: 6.2.0.Q36, Build Date: Thu Feb 14 23:25:50 UTC 2013), "Installed Devices" (EMS, SBCE62), "Alarms (past 24 hours)" (None found), and "Incidents (past 24 hours)" (Five entries, all stating "SBCE62: No Subscriber Flow Matched"). There is a "Refresh" button next to the System Time, and an "Add" button at the bottom right of the Incidents section. A "Notes" section is at the very bottom.

6.2. Global Profiles

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

6.2.1. 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.

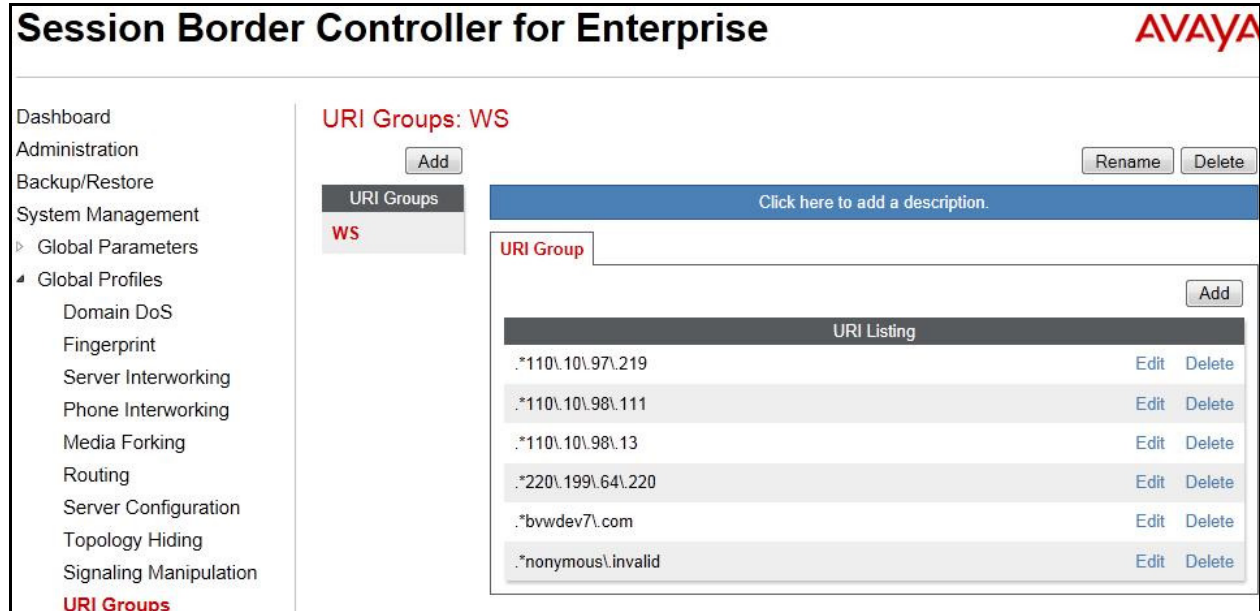
To add a URI Group, select **Global Profiles → URI Groups**. Click on **Add** button (not shown).

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**).
- **.*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\98\13**: IP address based URI-Host, defined to support routing for the outbound OPTIONS heartbeat originated by Communication Manager to the Avaya SBCE. 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 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 6.2.2** and **Section 6.4.4**.

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



6.2.2. 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 **CM52-to-WS** was created to use in conjunction with the server flow defined for Communication Manager. This entry is to route the outbound call from the enterprise to Windstream.

In the opposite direction, a Routing Profile named **WS-to-CM52** 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.

6.2.2.1 Routing Profile for Windstream

The screenshot below illustrates the routing profile from Avaya SBCE to Windstream network, **Global Profiles → Routing: CM52-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 6.2.1**, 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: CM52-to-WS'. It features a list of routing profiles on the left: 'default', 'WS-to-CM52', and 'CM52-to-WS' (selected). To the right of this list is a table for the selected profile. The table has columns: Priority, URI Group, Next Hop Server 1, and Next Hop Server 2. The first row shows Priority 1, URI Group WS, and Next Hop Server 1 as 220.199.64.220:5060. There is also a 'View' and 'Edit' link for this entry. Above the table, there is a button 'Add' and a description field with the text 'Click here to add a description.'.

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

6.2.2.2 Routing Profile for Communication Manager

The Routing Profile, Windstream to Communication Manager 5.2.1, **WS-to-CM52** was defined to route calls where the “To” header matches the URI Group **WS** defined in **Section 6.2.1** to **Next Hop Server 1** which is the IP address of Communication Manager, on port 5060 as a destination. As shown in **Figure 1**, SIP trunk between Communication 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-CM52'. It features a list of routing profiles on the left: 'default', 'WS-to-CM52' (selected), and 'CM52-to-WS'. To the right of this list is a table for the selected profile. The table has columns: Priority, URI Group, Next Hop Server 1, and Next Hop Server 2. The first row shows Priority 1, URI Group WS, and Next Hop Server 1 as 110.33.10.26:5060. There is also a 'View' and 'Edit' link for this entry. Above the table, there is a button 'Add' and a description field with the text 'Click here to add a description.'.

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

6.2.3. 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 **CM52-to-WS** and **WS-to-CM52** were created.

6.2.3.1 Topology Hiding Profile for Windstream

Profile **CM52-to-WS** was defined to mask the enterprise SIP domain `bwvdev7.com` in "Request-URI" and "To" headers to IP **220.199.64.220** (the IP address Windstream uses as URI-Host portion for "Request-URI" and "To" headers to meet the SIP specification requirement of Windstream); mask the enterprise SIP domain `bwvdev7.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 **CM52-to-WS**.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar shows the navigation menu with 'Topology Hiding' selected. The main content area is titled 'Topology Hiding Profiles: CM52-to-WS'. It features a list of profiles with 'CM52-to-WS' selected. Below the list, there is a table titled 'Topology Hiding' with the following data:

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	---

6.2.3.2 Topology Hiding Profile for Communication Manager

Profile **WS-to-CM52** 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-CM52**.

The screenshot displays the Avaya Session Border Controller for Enterprise (SBCE) web interface. The left sidebar shows the navigation menu with 'Global Profiles' expanded, and 'Topology Hiding' selected. The main content area is titled 'Topology Hiding Profiles: WS-to-CM52'. It features a table with the following data:

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	---

Buttons for 'Add', 'Rename', 'Clone', 'Delete', and 'Edit' are visible. The 'WS-to-CM52' profile is highlighted in the list on the left.

6.2.4. 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 Communication Manager respectively.

6.2.4.1 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 = Unchecked. The Avaya SBCE will not handle REFER. It will keep the REFER message unchanged from Communication Manager to Windstream.
- T.38 Support = Unchecked. Windstream does not support T.38 fax in the compliance testing.
- Privacy Enabled = Unchecked. 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 = Checked. The Avaya SBCE will modify “Call-ID” header for the call toward Windstream.
- Change Max Forwards: Checked. 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: Checked. 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

RenameCloneDelete

Click here to add a description.

GeneralTimersURI ManipulationHeader ManipulationAdvanced

General

Hold Support	NONE
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: **WS_SI**

Add

Interworking Profiles

SM63_WS_SI

WS_SI

RenameCloneDelete

Click here to add a description.

GeneralTimersURI ManipulationHeader ManipulationAdvanced

Advanced

Record Routes	Both
Topology Hiding: Change Call-ID	Yes
Call-Info NAT	No
Change Max Forwards	Yes
Include End Point IP for Context Lookup	No
OCS Extensions	No
AVAYA Extensions	No
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

6.2.4.2 Server Interworking profile for Communication Manager

Profile **CM_DH_ACME** 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 = Unchecked. The Avaya SBCE will not handle REFER, it will keep the REFER messages unchanged from Windstream to Communication Manager.
- T.38 Support = Unchecked. Windstream does not support T.38 fax in the compliance testing.
- Privacy Enabled = Unchecked. 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 = Checked. The Avaya SBCE will modify “Call-ID” header for the call toward Communication Manager.
- Change Max Forwards: Checked. 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: Checked. 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 **CM52_WS_SI**.

Interworking Profiles: CM52_WS_SI

Buttons: Add, Rename, Clone, Delete

Click here to add a description.

Tabs: General, Timers, URI Manipulation, Header Manipulation, Advanced

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: CM52_WS_SI

Add
Rename
Clone
Delete

Interworking Profiles

CM52_WS_SI

WS_SI

Click here to add a description.

General
Timers
URI Manipulation
Header Manipulation
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

6.2.5. 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).

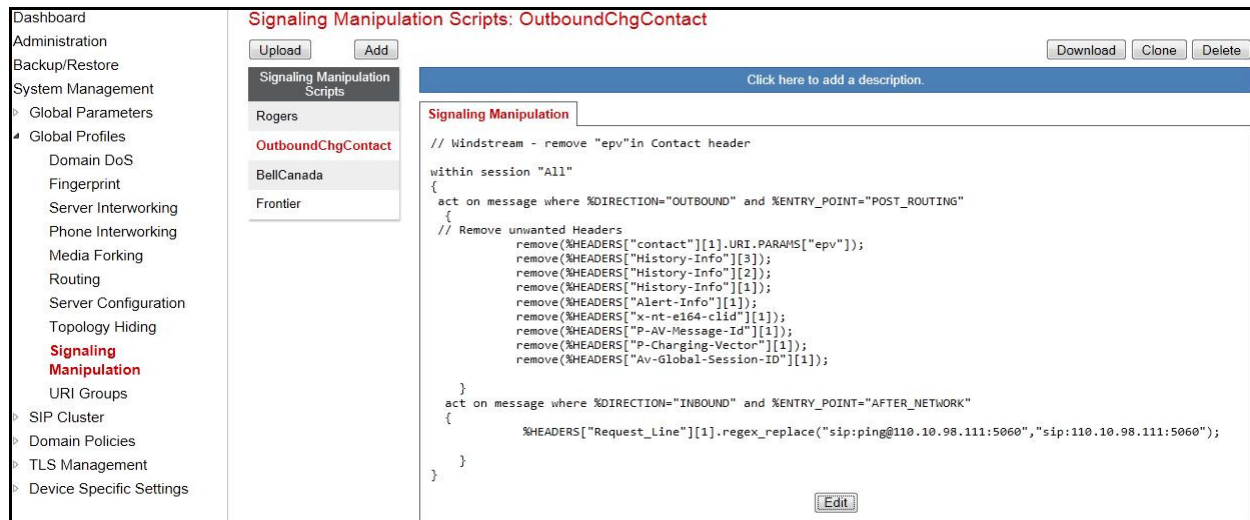
In the compliance testing, SigMa script **OutboundChgContact** was created for Server Configuration for Windstream.

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.



6.2.6. 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 **CM52_SC** for Communication Manager.

6.2.6.1 Server Configuration for Windstream

Server Configuration named **WS_SC** was created for Windstream. It will be discussed in detail 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 Communication 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.

Server Configuration: WS_SC

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

Buttons: Add, Edit, Rename, Clone, Delete

Tabs: **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

Under **Advanced** tab, check on **Enable DoS Protection** (not shown). For **Interworking Profile** drop down list, select **WS_SI** as defined in **Section 6.2.4**. For **Signaling Manipulation Script**, select **OutboundChgContact**, which is created in **Section 6.2.5**. This configuration applies the specific SIP profile to the Windstream traffic. The other settings are kept as default.

Server Configuration: WS_SC

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

Buttons: Add, Edit, Rename, Clone, Delete

Tabs: General, Authentication, Heartbeat, **Advanced**, DoS Whitelist, DoS Protection

Enable DoS Protection	<input checked="" type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	WS_SI
Signaling Manipulation Script	OutboundChgContact
UDP Connection Type	SUBID

6.2.6.2 Server Configuration for Communication Manager

Server Configuration named **CM52_SC** was created for Communication 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 Communication Manager to query the status of the SIP trunk.

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

The screenshot shows the 'Server Configuration: cm52_sc' window. On the left is a navigation menu with 'Server Configuration' selected. The main area has tabs for 'General', 'Authentication', 'Heartbeat', and 'Advanced'. The 'General' tab is active, showing a table with the following data:

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

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

Under **Advanced** tab, click on **Edit** button (not shown), for **Interworking Profile** drop down list select **CM52_WS_SI** as defined in **Section 6.2.4** and for **Signaling Manipulation Script** drop down list select **None**. The other settings are kept as default.

The screenshot shows the 'Server Configuration: cm52_sc' window with the 'Advanced' tab selected. The settings are as follows:

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	CM52_WS_SI
Signaling Manipulation Script	None
TCP Connection Type	SUBID

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

6.3. 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.

6.3.1. 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 sessions. The sample configuration is cloned and modified to increase the number of **Maximum Concurrent Sessions** 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 Sessions 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. 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.

The screenshot shows the 'Application Rules: WS_AR' configuration page. On the left is a navigation menu with 'Domain Policies' expanded and 'Application Rules' selected. The main area has a title 'Application Rules: WS_AR' and buttons for 'Add', 'Filter By Device...', 'Rename', 'Clone', and 'Delete'. Below the title is a description field with the placeholder 'Click here to add a description.' A table titled 'Application Rule' lists the configured parameters:

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"/>		

Below the table is a 'Miscellaneous' section with two rows:

Miscellaneous	
CDR Support	None
RTCP Keep-Alive	No

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

6.3.2. 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 packets 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** was cloned 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).

6.3.3. 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 **CM52_WS_SR**, were created from **default** Signaling Rules for Windstream and Communication Manager respectively (not shown).

6.3.4. 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 Communication 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).

Endpoint Policy Group for Windstream

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

- Set Application Rule to **WS_AR** as created in **Section 6.3.1**.
- Set Media Rule to **WS_MR** as created **Section 6.3.2**.
- 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**.

The screenshot shows the 'Policy Groups: WS-PG' configuration page. On the left is a navigation menu with categories like Dashboard, Administration, Backup/Restore, System Management, and Domain Policies. Under Domain Policies, 'Application Rules', 'Border Rules', 'Media Rules', and 'Security Rules' are listed. The main area shows a list of policy groups: 'default-low', 'default-low-enc', 'default-med', 'default-med-e...', and 'default-high'. The 'WS-PG' group is selected and highlighted. To the right of this list is a detailed view for the selected group, which includes a 'Filter By Device...' dropdown, 'Rename' and 'Delete' buttons, and a table of rules. The table has columns for Order, Application, Border, Media, Security, Signaling, and Time of Day. The first row shows Order 1, Application WS_AR, Border default, Media WS_MR, Security default-high, Signaling WS_SR, and Time of Day default. There are 'Edit' and 'Clone' buttons for each row. Above the table are 'Summary' and 'Add' buttons.

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

Endpoint Policy Group for Communication Manager

The following screen shows **CM52_WS_PG** created for Communication Manager:

- Set Application Rule to **WS_AR** as created in **Section 6.3.1**.
- Set Media Rule to **WS_MR** as created **Section 6.3.2**.
- Set Signaling Rule to **CM52_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**.

6.3.5. 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 6.2.1**.

In the compliance testing, a Session Policy named **CM52-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 **CM52_WS_SP** for the new policy and click **Finish** (not shown).

6.4. 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.

6.4.1. 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 **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. The following screen shows the private interface is assigned to **A1** and the public interface is assigned to **B1**.

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.

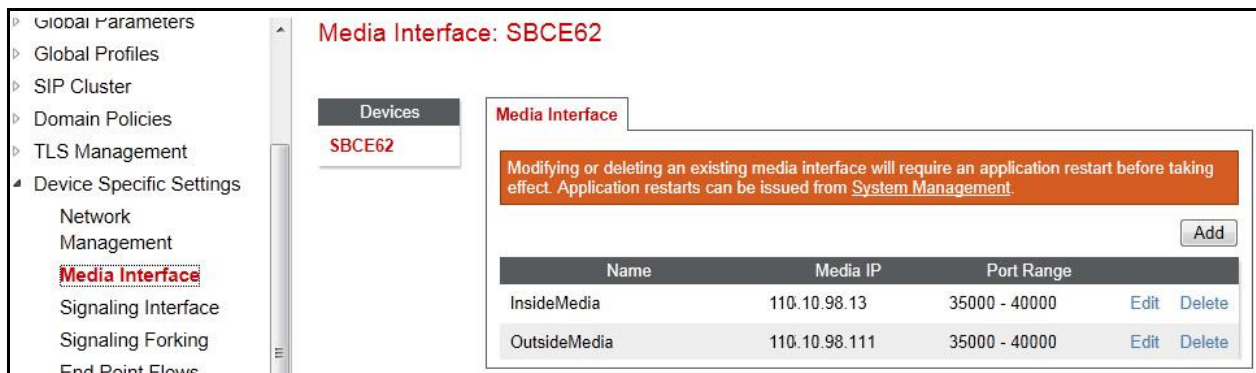
6.4.2. Media Interface

Media Interface screen is where the media ports are defined. The Avaya SBCE will open a 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.

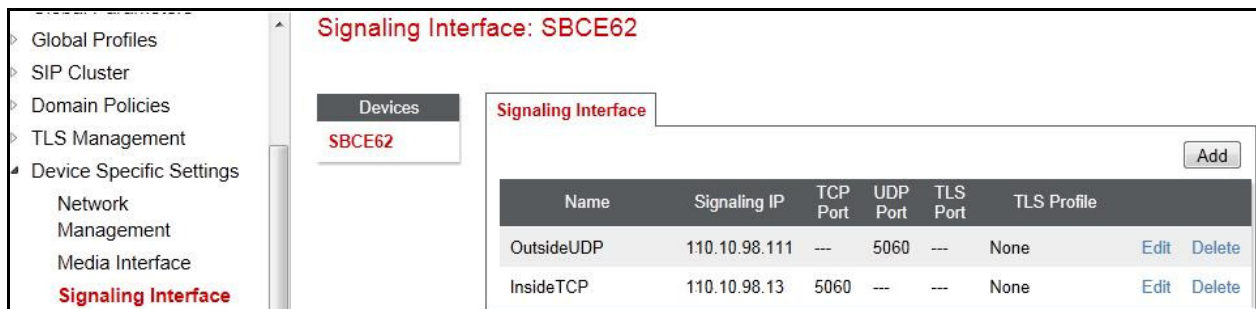


6.4.3. Signaling Interface

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



6.4.4. 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 Communication 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 6.2.5** to assign to the Flow.
- **URI Group:** Select the URI Group created in **Section 6.2.1** to assign to the Flow.
- **Received Interface:** Select the Signaling Interface created in **Section 6.4.3** the Server Configuration is allowed to receive SIP messages from.
- **Signaling Interface:** Select the Signaling Interface created in **Section 6.4.3** used to communicate with the Server Configuration.
- **Media Interface:** Select the Media Interface created in **Section 6.4.2** used to communicate with the Server Configuration.
- **End Point Policy Group:** Select the End Point Policy Group created in **Section 6.3.4** to assign to the Server Configuration.
- **Routing Profile:** Select the Routing Profile created in **Section 6.2.2** the Server Configuration will use to route SIP messages to.
- **Topology Hiding Profile:** Select the Topology-Hiding profile created in **Section 6.2.3** 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-CM52
Topology Hiding Profile	CM52-to-WS
File Transfer Profile	None
<input type="button" value="Finish"/>	

The following screen shows the Server Flow **CM52_WS_SF** configured for Communication Manager.

Flow Name	CM52_WS_SF
Server Configuration	CM52_SC
URI Group	WS
Transport	*
Remote Subnet	*
Received Interface	OutsideUDP
Signaling Interface	InsideTCP
Media Interface	InsideMedia
End Point Policy Group	WS-PG
Routing Profile	CM52-to-WS
Topology Hiding Profile	WS-to-CM52
File Transfer Profile	None

Finish

6.4.5. Session Flows

Session Flows feature allows definition of 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 6.2.1** to assign to the Session Flow as the source URI Group.
- **URI Group #2:** Select the URI Group created in **Section 6.2.1** to assign to the Session Flow as the destination URI Group.
- **Session Policy:** Select the session policy created in **Section 6.3.5** 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 web-based configuration 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 containing an asterisk (*). Below it is the example "Ex: 192.168.0.1/24".
- Subnet #2:** A text input field containing an asterisk (*). Below it is the example "Ex: 192.168.0.1/24".
- Session Policy:** A dropdown menu with "CM52-WS-SP" selected.

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

7. 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.

8. 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.

8.1. Verification Steps

- Verify that endpoints at the enterprise site can place a call to the 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 a call from the 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 the 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.

8.2. 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.

8.3. Troubleshooting:

8.3.1. 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=z9hG4bK2vkhgq102ge0lqolt041.1
From: "BELLEVILLE ON"<sip:6139675203@220.199.64.220;user=phone;
broadworks=BWWESTSIGIS-lecpqqcalh9ba>;tag=91284129-1376935659975-
To: "User-Avaya6 NDS4-TG1"<sip:4693418165@220.199.64.220;interopis=interopis-
h3bnp35pc3i58>
Call-ID: BW180739975190813-165340777@220.199.51.199
CSeq: 199320804 INVITE
Contact: <sip:6139675203@220.199.64.220:5060;broadworks=BWWESTSIGIS-o6i7c69dv2579;
transport=udp>
Diversion: <sip:4693418165@220.199.51.199;user=phone>;reason=unavailable;counter=1,
<sip:4693418165@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 446427 1 IN IP4 220.199.64.220
s=-
c=IN IP4 220.199.64.220
t=0 0
m=audio 39046 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:6139675203@220.199.51.199;user=phone;broadworks=BWWESTSIGIS-
1ecpqcalh9ba>;tag=91284129-1376935659975-
To: "User-Avaya6 NDS4-TG1" <sip:4693418165@220.199.64.220;interopis=interopis-
h3bnp35pc3i58>;tag=06527b5cee31757651fa9aaa00
CSeq: 199320804 INVITE
Call-ID: BW180739975190813-165340777@220.199.51.199
Contact: "H323 9611" <sip:4693418165@110.10.98.111:5060;transport=udp>
Record-Route: <sip:110.10.98.111:5060;ipcs-line=71861;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=z9hG4bK2vkhgq102ge0lqolt041.1
Accept-Language: en
Require: timer
Server: Avaya CM/R015x.02.1.016.4
P-Asserted-Identity: "H323 9611" <sip:4693418165@220.199.64.220>
Session-Expires: 7200;refresher=uas
Content-Type: application/sdp
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 35822 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:6139675203@220.199.64.220 SIP/2.0
From: "H323 9611" <sip:4693418165@110.10.98.111>;tag=8048d41f5dee31947651fa9aaa00
To: sip:6139675203@220.199.64.220
CSeq: 1 INVITE
Call-ID: 757bae6e9c61183a17789537b3e6533f
Contact: "H323 9611" <sip:4693418165@110.10.98.111:5060>
Record-Route: <sip:110.10.98.111:5060;ipcs-line=71904;lr;transport=udp>
Allow: INVITE, CANCEL, BYE, ACK, PRACK, SUBSCRIBE, NOTIFY, REFER, OPTIONS, INFO,
PUBLISH
Supported: timer, replaces, join, 100rel
User-Agent: Avaya CM/R015x.02.1.016.4
Max-Forwards: 70
Via: SIP/2.0/UDP 110.10.98.111:5060;branch=z9hG4bK-s1632-001993283232-1--s1632-
Accept-Language: en
P-Asserted-Identity: "H323 9611" <sip:4693418165@110.10.98.111>
Session-Expires: 7200;refresher=uac
Min-SE: 7200
Content-Type: application/sdp
Content-Length: 213

v=0
o=- 1 1 IN IP4 110.10.98.111
s=-
c=IN IP4 110.10.98.111
b=AS:64
t=0 0
m=audio 35830 RTP/AVP 0 18 101
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
```


- 200OK/SDP response by Windstream:

```
SIP/2.0 200 OK
From: "H323 9611" <sip:4693418165@110.10.98.111>;tag=8048d41f5dee31947651fa9aaa00
To: <sip:6139675203@220.199.64.220>;tag=229916331-1376935943091
CSeq: 1 INVITE
Call-ID: 757bae6e9c61183a17789537b3e6533f
Via: SIP/2.0/UDP 110.10.98.111:5060;branch=z9hG4bK-s1632-001993283232-1--s1632-
Record-Route: <sip:110.10.98.111:5060;ipcs-line=71904;lr;transport=udp>
Require: timer
Session-Expires: 7200;refresher=uac
Supported: timer
Contact: <sip:6139675203@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
Content-Type: application/sdp
Content-Length: 212

v=0
o=BroadWorks 446439 1 IN IP4 220.199.64.220
s=-
c=IN IP4 220.199.64.220
t=0 0
m=audio 39034 RTP/AVP 0 101
a=sendrecv
a=ptime:20
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```

8.3.2. 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.

9. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Manager 5.2.1 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 5.2.1 and Avaya Session Border Controller for Enterprise 6.2.

10. References

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

- [1] *Administering Avaya Aura® Communication Manager*, June 2010, Document Number 03-300509.
- [2] *Avaya Aura® Communication Manager Feature Description and Implementation*, June 2010, Document Number 555-245-205.
- [3] *Feature Description and Implementation for Avaya Communication Manager, Issue 5*, Document Number 555-245-205.
- [4] *Avaya one-X® Deskphone Edition for 9600 Series IP Telephones Administrator Guide*, Release 3.1, November 2009, Document Number 16-300698.
- [5] *Avaya one-X® Deskphone SIP for 9600 Series IP Telephones Administrator Guide*, Release 2.6, June 2010, Document Number 16-601944.
- [6] *Administering Avaya one-X® Communicator*, April 2011.
- [7] *Using Avaya one-X® Communicator*, April 2011.
- [8] *Avaya SBCE Install Guide (102-5224-400v1.01)*
- [9] *Avaya SBCE Administration Guide (010-5423-400v106)*
- [10] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [11] *RFC 3515, The Session Initiation Protocol (SIP) Refer Method*, <http://www.ietf.org/>
- [12] *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.