Avaya Solution & Interoperability Test Lab

Application Notes for Windstream SIP Trunking Service (Metaswitch) with Avaya Communication Server 1000 Release 7.6 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) Trunking between Windstream SIP Trunking Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Communication Server 1000 Release 7.6, Avaya Session Border Controller for Enterprise Release 6.2 and various Avaya endpoints.

Windstream SIP Trunking Service provides PSTN access via a SIP Trunk between the enterprise and Windstream networks as an alternative to traditional PSTN trunks such as analog or ISDN-PRI. This approach generally results in lower cost for the 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

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Windstream SIP Trunking Service (Windstream) and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Communication Server 1000 (CS1000) Release 7.6, Avaya Session Border Controller for Enterprise (Avaya SBCE) Release 6.2 and various Avaya endpoints.

Windstream SIP Trunking Service referenced within these Application Notes is designed for enterprise business customers. Customers using Windstream SIP Trunking Service with the Avaya SIP-enabled enterprise solution are able to place and receive PSTN calls via a broadband WAN connection using the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks such as analog or ISDN-PRI.

2. General Test Approach and Test Results

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 public Internet and exercise the features and functionalities listed in **Section 2.1**.

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

2.1. Interoperability Compliance Testing

To verify Windstream SIP Trunking interoperability, the following features and functionalities were covered during the compliance testing:

- Incoming PSTN calls to various phone types including UNIStim, SIP, digital and analog telephones at the enterprise. All incoming calls from PSTN are routed to the enterprise across the SIP Trunk from the service provider.
- Outgoing PSTN calls from various phone types including UNIStim, SIP, digital and analog telephones at the enterprise. All outgoing calls to PSTN are routed from the enterprise across the SIP Trunk to the service provider.
- Incoming and outgoing PSTN calls to/from 2050 IP softphones.
- Dialing plans including local, long distance, international, outgoing toll-free, etc.
- Calling Party Number presentation and Calling Party Number restriction.
- Proper codec negotiation with G.711MU codec and G.729 codec.
- Proper early media transmission using G.711MU codec.
- Proper media transmission using G.711MU codec.
- Incoming and outgoing fax calls using G.711MU codec.
- DTMF tone transmission as out-of-band RTP events as per RFC 2833.
- Voicemail navigation for incoming and outgoing calls.

- Call Pilot voicemail hosted on the CS1000.
- Telephony features such as Hold and Resume, Call Waiting, Call Park, Call Transfer, Call Forward and Conferencing.
- Music on Hold.
- Off-net call transfer using subsequent INVITE method.
- Response to OPTIONS heartbeat.
- Response to incomplete call attempts and trunk errors.

Items that are not supported by Windstream on the test environment or not tested as part of the compliance testing, are listed as following:

- Inbound toll-free and outgoing emergency calls (E911) are supported but were not tested as part of the compliance testing.
- T.38 is not supported.
- Off-net calls transfer using REFER method is not supported.
- Call forward from PSTN back to PSTN is not supported.

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.

1. **For off-net blind transfer call**, **the calling PSTN does not hear ring back when the called PSTN is ringing**. When the CS1000 transfers off-net an incoming PSTN call back to PSTN, the transfer is successfully completed but after the transfer the calling PSTN does not hear ringback tone. This issue can be fixed by removing SDP in the 180 Ringing message coming to CS1000 from Windstream, this can be done in Avaya SBCE in Section **6.2.4.2** Server Interworking Profile for CS1000.
2. **No ring back tone on CS1000 UNIStim phone when it is blindly transferred by another CS1000 UNIStim phone to PSTN.** This is also a known issue in the CS1000. This issue can be fixed by removing SDP in the 180 Ringing message coming to CS1000 from Windstream, this can be done in Avaya SBCE in Section **6.2.4.2** Server Interworking Profile for CS1000.
3. **For off-net call transfer**, **Calling Party Name and Calling Party Number are not updated to PSTN parties**. When the CS1000 transfers off-net an incoming call back to PSTN, it does not update the true connected Calling Party Name and Calling Party Number to PSTN parties. It results both PSTN parties still display Calling Party Name and Calling Party Number of the CS1000 extension. This is a known issue of the CS1000 when it interoperates with Windstream where the proprietary signaling of the CS1000 is not supported. This issue has low user impact, it is listed here simply as an observation.
4. **The 501 plug-in** must be enabled in the CS1000 for the call blind transfer to be executed successfully. This configuration is documented in **Section 5.7**.
5. **CS1000 UNIStim phone places an external call on hold then retrieves the held call**, **it causes Calling Party Number to change**. After retrieving a held external call, Calling Party Number previously displayed on the CS1000 UNIStim phone is replaced by "Route ACOD" – "Trunk Channel ID". This is a known behavior of the CS1000 with no

resolution available at this time. This issue has low user impact, it is listed here simply as an observation.

6. **CS1000 UNIStim phone calls to an internal SIP phone which Call Forward All Call to PSTN**, **the UNIStim phone does not display Calling Party Name and Number of the PSTN party**. After the call was successfully forwarded to PSTN, the PSTN party properly displayed DID number associated with the UNIStim or DID pilot number. However, the UNIStim phone still displayed local extension of the SIP phone which is not expected. It should display Calling Party Name and Number of the PSTN which is the true connected party. This is a known behavior of the CS1000 with no resolution available at this time. This issue has low user impact, it is listed here simply as an observation.
7. **CS1000 UNIStim phone calls to PSTN then blind transfers to an internal SIP phone, the SIP phone does not display Calling Party Name and Number of the PSTN party**. After the call was successfully transferred, the SIP phone displayed Calling Party Name and Number of the UNIStim which is not expected. It should display Calling Party Name and Number of the PSTN which is the true connected party. This is a known behavior of the CS1000 with no resolution available at this time. This issue has low user impact, it is listed here simply as an observation.
8. **MIME Multipart** in SIP INVITE message sent from Avaya CS1000 is not supported by Windstream and it causes outbound call to PSTN dropped immediately after the call answered. This issue is fixed by applying a Signaling Manipulation script in Avaya SBCE in Section **6.2.5**.
9. **Call Forward from PSTN back to PSTN** is not supported by Windstream (using Metaswitch). There is a workaround for this issue by applying a Signaling Manipulation script in Avaya SBCE in Section **6.2.5**.

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 at http://www.windstream.com/Support/

3. Reference Configuration

Figure 1 illustrates the sample Avaya SIP-enabled enterprise solution connected to Windstream SIP Trunking Service (Vendor Validation Circuit) through the Internet. For confidentiality and privacy purposes, the actual public IP addresses and PSTN routable phone numbers used in the certification testing have been replaced with fictitious parameters throughout the Application Notes.

The Avaya SBCE is located at the edge of the enterprise network. The Avaya SBCE has two connection points, a public side connecting to Windstream via the Internet and a private side connecting to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise network flow through the Avaya SBCE which can protect the enterprise against any outside SIP-based attacks. In the compliance testing, Windstream provided the service provider public IP address **64.xx.xxx.174**. This public IP address will be used for the public SIP traffic between the Avaya SBCE and Windstream. The Avaya lab was configured with a SIP domain **avayalab.com** for the enterprise, the Topology-Hiding feature of the Avaya SBCE (see **Section 6.2.3.1**) was used to adapt the enterprise SIP domain to the service provider SIP domains known to Windstream.

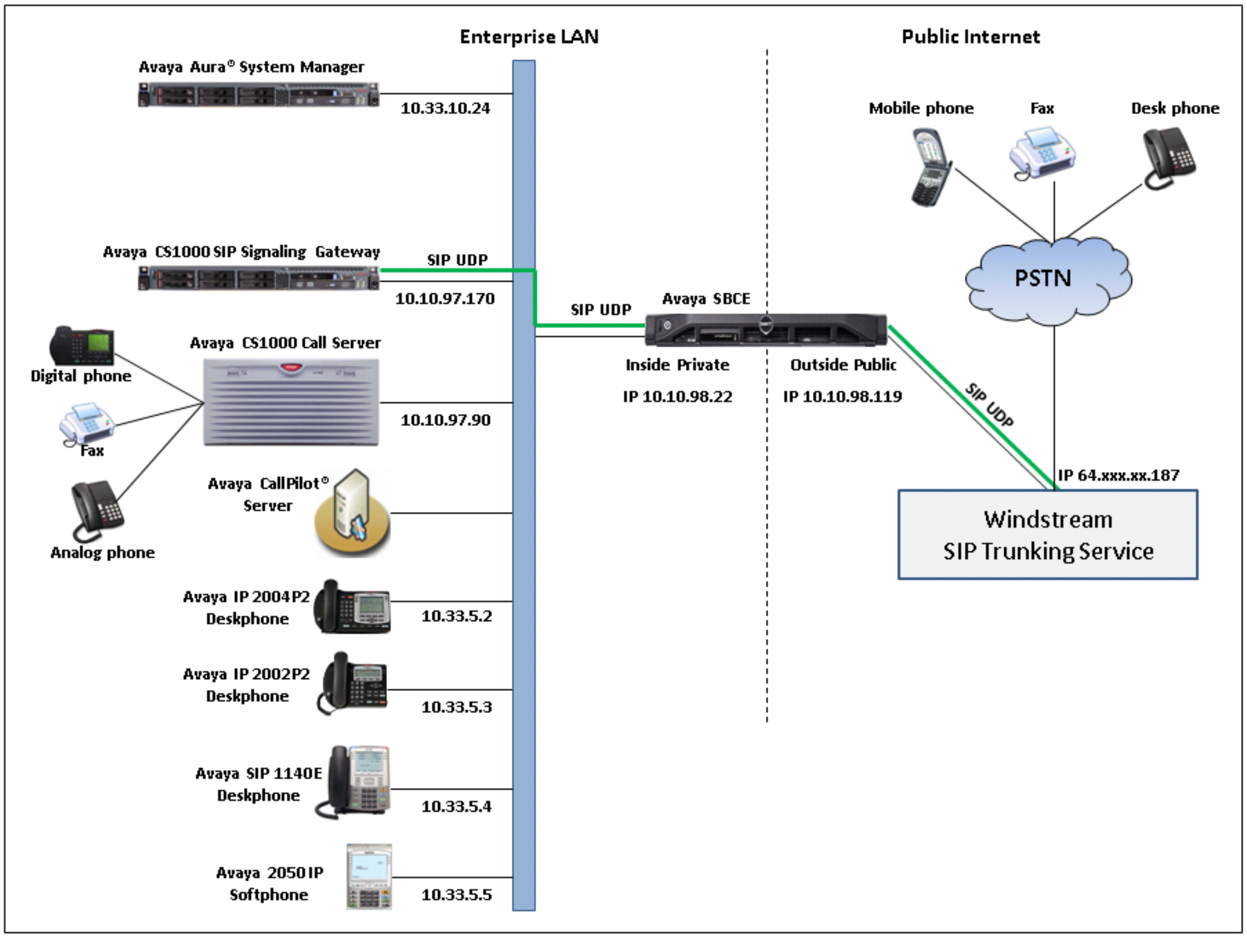


Figure 1: **Avaya IP Telephony Network connecting to Windstream SIP Trunking Service**

4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Equipment/Software	**Release/Version**
Avaya CS1000 7.6 (CPPM)	• Call Server: 7.65 P GA plus latest DEPLIST Issue: 01 Release: 2013-12-17 (est) • SSG and SLG Server: 7.65.16 GA plus latest Service Pack 4 SP_7.6_4.ntl
Avaya Media Gateway Controller (MGC) Avaya DSP	• MGCCDC02 • DSP1AB07
Avaya Aura® System Manager running on Avaya S8800 Server	6.3.4 – FP3 （6.3.4.0.634014）
Avaya Call Pilot	05.00.41.141
Avaya IP Telephone	• 2002 p2: 0604DCO (UNIStim) • 2004 p2: 0604DCO (UNIStim) • 1140: 0625C8Q (UNIStim) • 1120: 0624C6Q (UNIStim) • 2007: 0621C8Q (UNIStim) • SIP 1140: SIP11x0e04.03.12.00
Avaya 2050 IP Softphone	4.3
Avaya Digital Telephone 3904	024
Avaya Analog Telephone	n/a
Avaya Session Border Controller for Enterprise (running on Dell R210 platform)	6.2.1 Q07
Windstream SIP Trunking Service Components	
Equipment/Software	**Release/Version**
Metaswitch	8.1.0 Patch B
EdgeWater EM 11.6.13	11.6.13

Table 1: **Equipment and Software Tested**

5. Configure Avaya Communication Server 1000

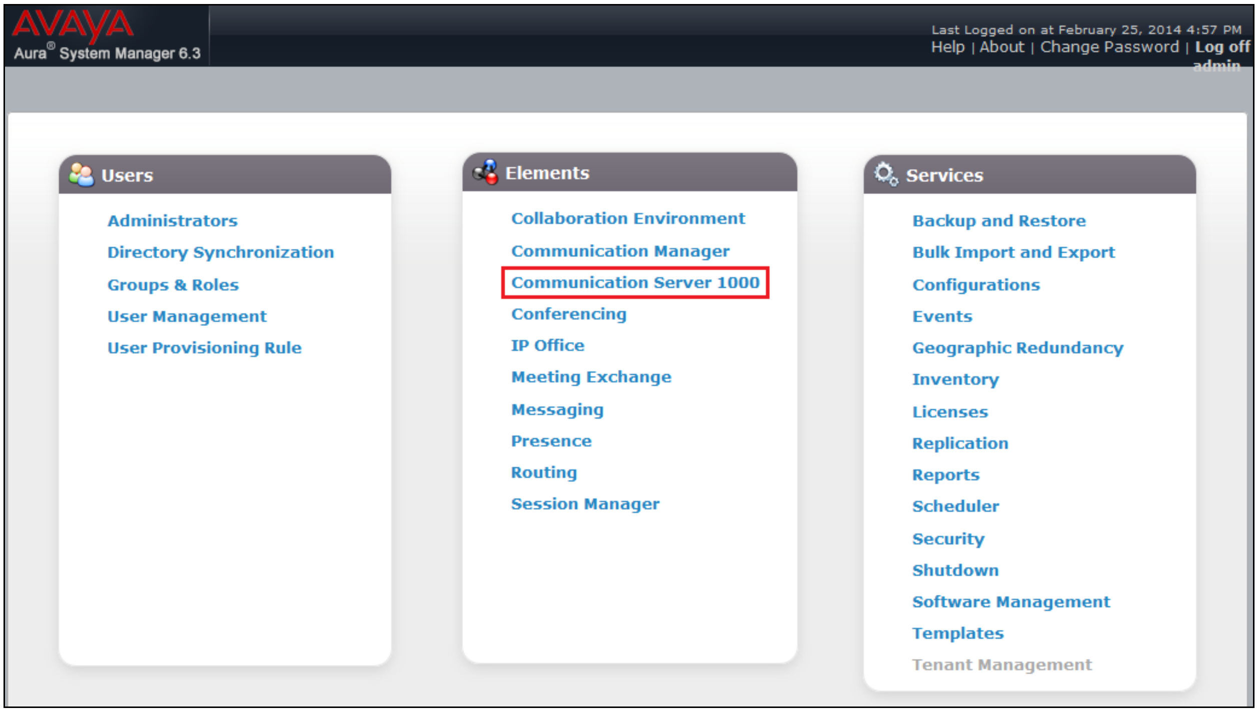
This section describes the procedure for configuring the CS1000 for interoperating with Windstream. A two-way SIP Trunk was created between the CS1000 and Avaya SBCE to carry traffic to and from the service provider respectively. Incoming calls flow from the Windstream network to the Avaya SBCE to the CS1000. Incoming calls into the CS1000 may undergo call treatments such as incoming digit translations and class of service restrictions. Outgoing calls to PSTN are first processed by the CS1000 for call treatments such as route selection and class of service. Once the CS1000 selects the proper SIP Trunk, the call is routed to the Avaya SBCE for egress to the Windstream network.

These Application Notes assume the basic configuration has already been administered and it is not discussed here. For further information on the CS1000, see **References** in **Section 10**.

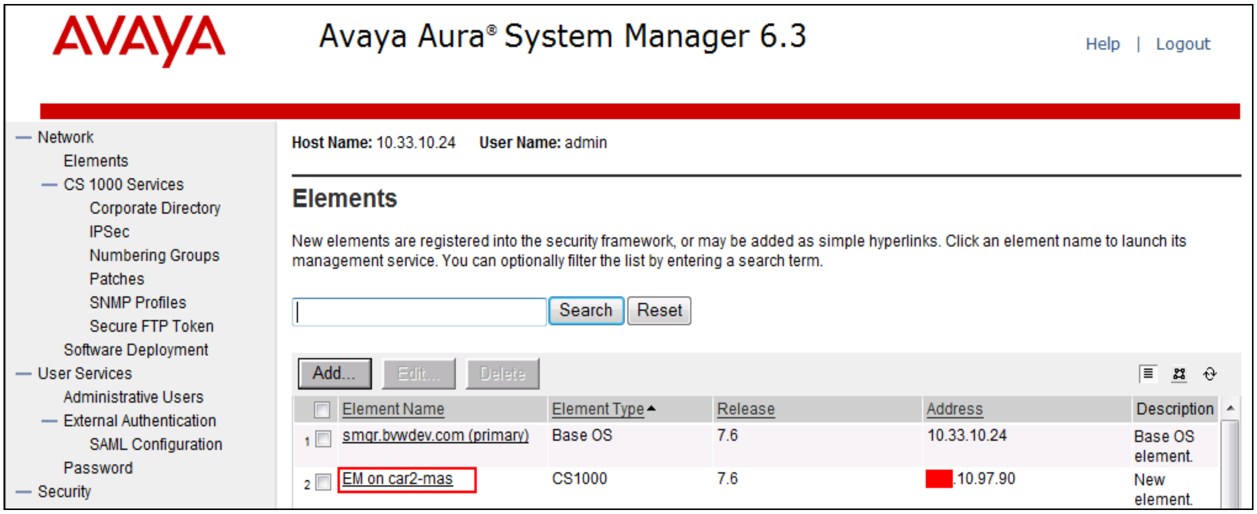
5.1. Log into the CS1000

5.1.1. Log into Unified Communications Management (UCM) and Element Manager (EM)

Since release 7.6 Avaya CS1000 UCM was integrated with System Manager, it depends on how the CS1000 system is deployed as to whether it is managed by its own UCM or from within System Manager. In the compliance testing, the CS1000 UCM was accessed via System Manager. The screen below shows the System Manager home page with the Communication Server 1000 entry in the Elements table. Click on the Communication Server 1000 link to access the CS1000 UCM. The UCM webpage will be opened in anew window.



The **Avaya Unified Communications Management** is shown in the following screenshot. Click **Element Name** of the CS1000 Element as highlighted in the red box.



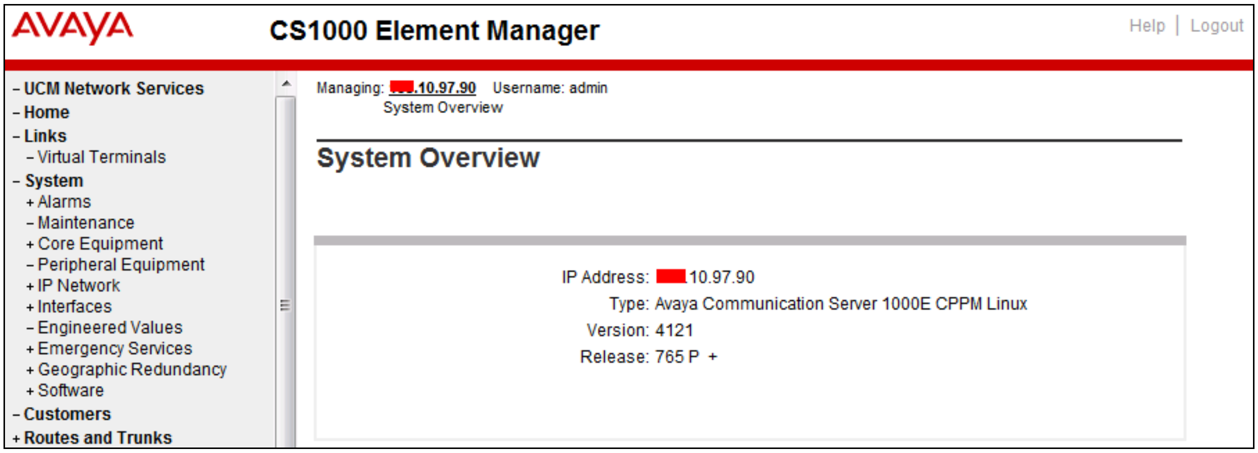
Host Name: 10.33.10.24 **User Name:** admin

Elements

New elements are registered into the security framework, or may be added as simple hyperlinks. Click an element name to launch its management service. You can optionally filter the list by entering a search term.

	□	Element Name	Element Type	Release	Address	Description
1	□	smgr.bvwdev.com (primary)	Base OS	7.6	10.33.10.24	Base OS element.
2	□	EM on car2-mas	CS1000	7.6	[redacted].10.97.90	New element.

The following screenshot shows the CS1000 Element Manager **System Overview** page.



Managing: [redacted].10.97.90 Username: admin
System Overview

System Overview

IP Address: [redacted].10.97.90
Type: Avaya Communication Server 1000E CPPM Linux
Version: 4121
Release: 765 P +

5.1.2. Log into Call Server Command Line Interface (CLI)

Using Putty, SSH to the IP address of the SIP Signaling Gateway (SSG) Server with the ***admin*** account then run the command ***cslogin*** and login with the appropriate admin account and password. The following screenshot are the logs.

```
login as: admin

               Avaya Inc. Linux Base   7.65
The software and data stored on this system are the property of,
or licensed to, Avaya Inc. and are lawfully available only
to authorized users for approved purposes. Unauthorized access
to any software or data on this system is strictly prohibited and
punishable under appropriate laws. If you are not an authorized
user then do not try to login. This system may be monitored for
operational purposes at any time.
```

```
admin@10.10.97.90's password:
Last login: Tue Oct  8 16:12:37 2013 from 10.10.98.86

SEC054 A device has connected to, or disconnected from, a pseudo tty without
authenticating
```

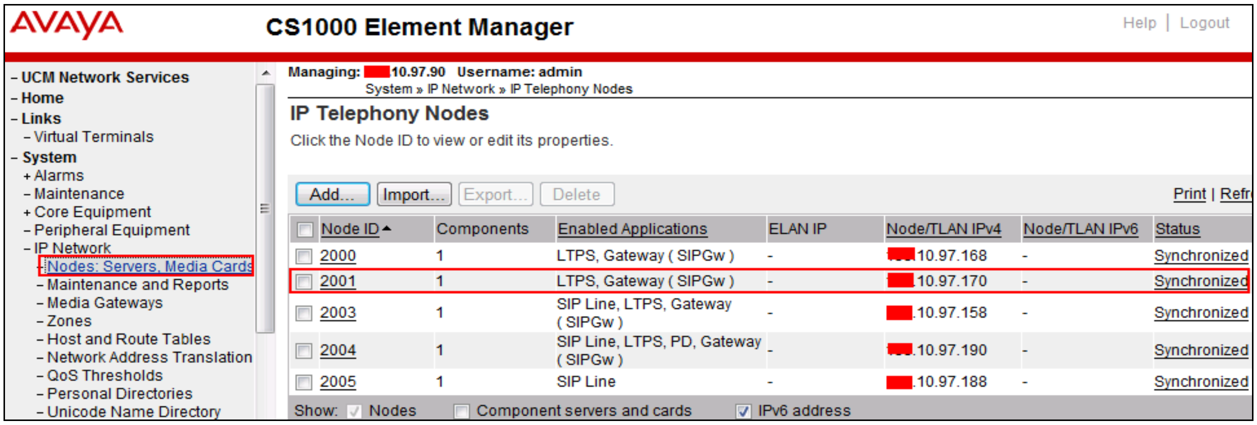
5.2. Administer Node IP Telephony

This section describes how to configure a Node IP Telephony on the CS1000.

5.2.1. Obtain Node IP Address

These Application Notes assume the basic configuration has already been administered and that a Node has already been created. This section describes configuration steps for Node ID 2001.

To configure an IP Node, select **System → IP Network → Nodes: Servers, Media Cards**. In the **IP Telephony Nodes** page as shown in the screenshot below, click the Node ID of the CS1000.



Managing: [redacted]10.97.90 Username: admin

System » IP Network » IP Telephony Nodes

IP Telephony Nodes

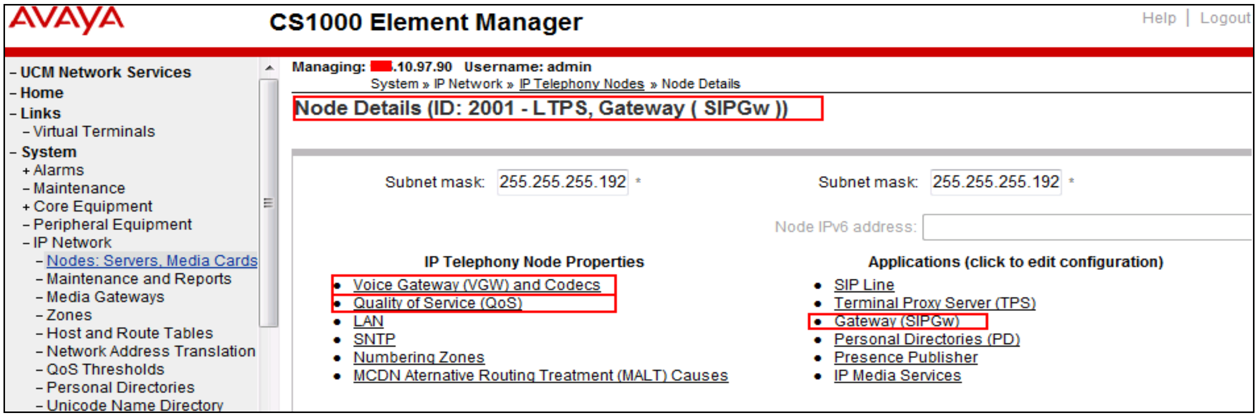
Click the Node ID to view or edit its properties.

Add... | Import... | Export... | Delete | Print | Refr

□ Node ID ▲	Components	Enabled Applications	ELAN IP	Node/TLAN IPv4	Node/TLAN IPv6	Status
□ 2000	1	LTPS, Gateway (SIPGw)	-	[redacted]10.97.168	-	Synchronized
□ 2001	1	LTPS, Gateway (SIPGw)	-	[redacted]10.97.170	-	Synchronized
□ 2003	1	SIP Line, LTPS, Gateway (SIPGw)	-	[redacted]10.97.158	-	Synchronized
□ 2004	1	SIP Line, LTPS, PD, Gateway (SIPGw)	-	[redacted]10.97.190	-	Synchronized
□ 2005	1	SIP Line	-	[redacted]10.97.188	-	Synchronized

Show: ☑ Nodes □ Component servers and cards ☑ IPv6 address

The **Node Details** page is shown in the screenshot below with the IP address of the Node ID 2001. The SIP Signaling Gateway uses the **Node IP Address** to connect to the Avaya SBCE for the SIP Trunk to Windstream. The three links highlighted in the screen shot below will be configured in the next sections.



Managing: [redacted].10.97.90 Username: admin

System » IP Network » IP Telephony Nodes » Node Details

Node Details (ID: 2001 - LTPS, Gateway (SIPGw))

Subnet mask: 255.255.255.192 *

Subnet mask: 255.255.255.192 *

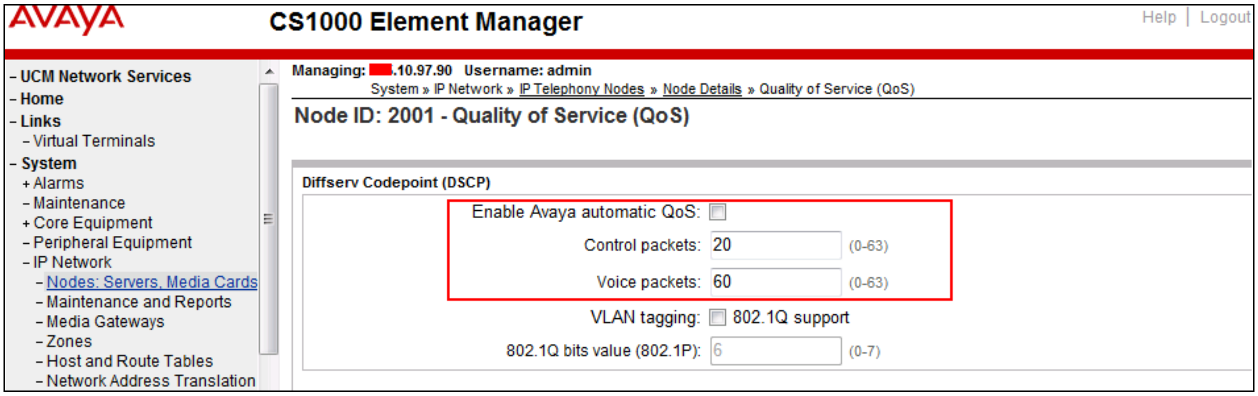
Node IPv6 address:

IP Telephony Node Properties
- Voice Gateway (VGW) and Codecs
- Quality of Service (QoS)
- LAN
- SNTP
- Numbering Zones
- MCDN Aternative Routing Treatment (MALT) Causes

Applications (click to edit configuration)
- SIP Line
- Terminal Proxy Server (TPS)
- Gateway (SIPGw)
- Personal Directories (PD)
- Presence Publisher
- IP Media Services

5.2.2. Administer Quality of Service (QoS)

To configure the QoS, click the **Quality of Service (QoS)** link in the Node Details page shown in **Section 5.2.1**. Verify that the default Diffserv values were used as shown in the screenshot below, then click the **Save** button (not shown).



Managing: [redacted].10.97.90 Username: admin

System » IP Network » IP Telephony Nodes » Node Details » Quality of Service (QoS)

Node ID: 2001 - Quality of Service (QoS)

Diffserv Codepoint (DSCP)

Enable Avaya automatic QoS: □

Control packets: 20 (0-63)

Voice packets: 60 (0-63)

VLAN tagging: □ 802.1Q support

802.1Q bits value (802.1P): 6 (0-7)

5.2.3. Synchronize the new configuration

In order for the changes to take effect, the Node Details page needs to be saved and synchronized by following the steps below.

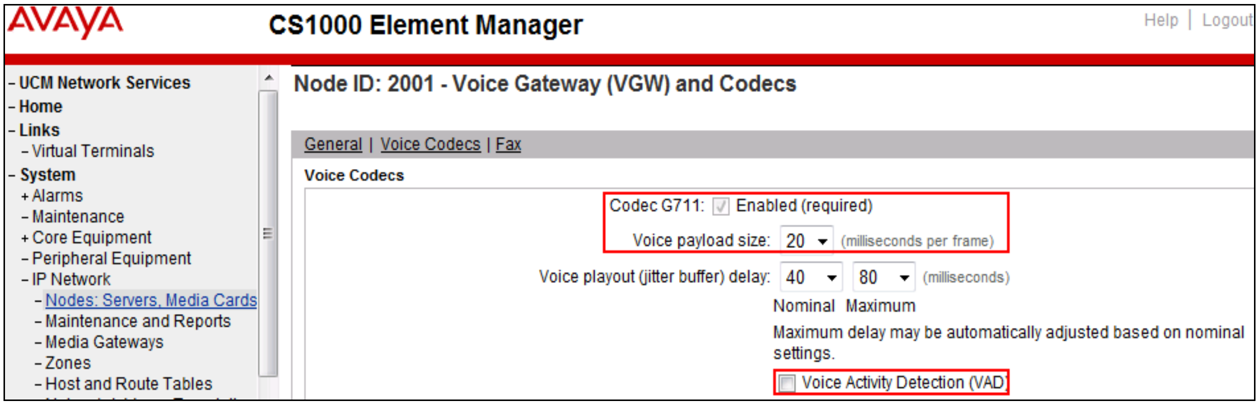
- Return to the **Node Details** page shown in **Section 5.2.1** and click **Save** button (not shown).
- The **Node Saved** screen is displayed. Click **Transfer Now** button (not shown).
- The **Synchronize Configuration Files** screen is displayed. Check the **Signaling Server** checkbox and click **Start Sync** button (not shown).
- When the synchronization completes, check the **Signaling Server** check box and click **Restart Applications** button (not shown).

5.3. Administer Voice Codec

5.3.1. Enable Voice Codec, Node IP Telephony

To configure Voice Codec, select **IP Network → Nodes**: **Servers, Media Cards** from the left pane, and in the **IP Telephony Nodes** screen, select the **Node ID** of the CS1000 system. The **Node Details** screen is displayed as described in **Section 5.2.1**.

On the **Node Details** page (not shown), click on **Voice Gateway (VGW) and Codecs**. Windstream supports voice codec G.711 and G.729, payload size 20 ms, with Voice Activity Detection (VAD) disabled. The following screenshot shows appropriate voice codec profile configured on the CS1000.



Node ID: 2001 - Voice Gateway (VGW) and Codecs

Voice Codecs

Codec G711: ☑ Enabled (required)

Voice payload size: 20 (milliseconds per frame)

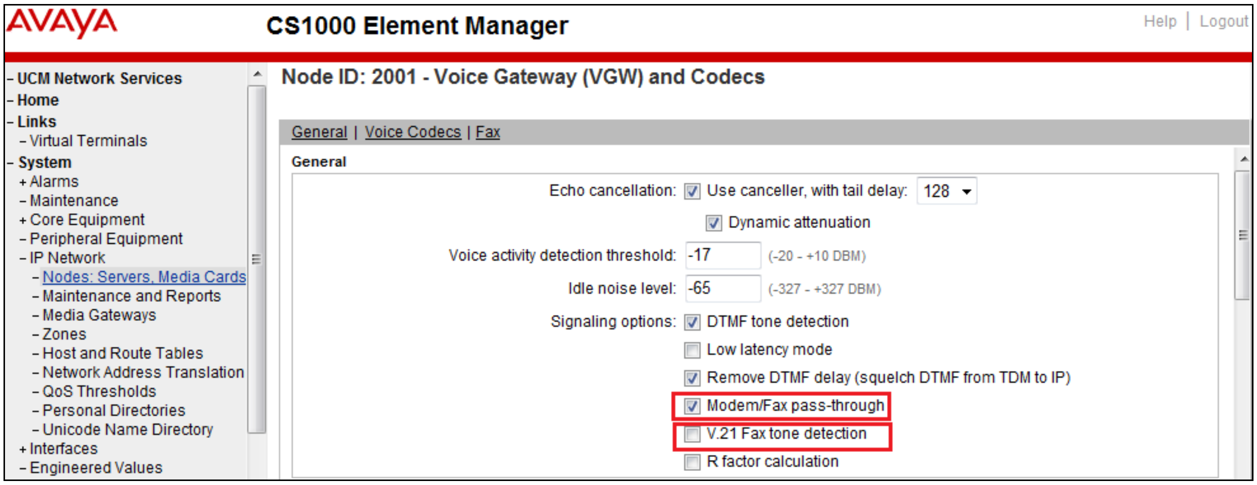
Voice playout (jitter buffer) delay: 40 80 (milliseconds)

Nominal Maximum

Maximum delay may be automatically adjusted based on nominal settings.

□ Voice Activity Detection (VAD)

For Fax over IP, Windstream supports G.711 codec as default and does not support T.38. The following screenshot shows **Modem/Fax pass-through** is selected for Node **2001**, this enables G.711 codec to be used for fax call between the CS1000 and Windstream. **Note**: The **V.21 Fax tone detection** should not be checked because **T.38 fax** is not supported.



Node ID: 2001 - Voice Gateway (VGW) and Codecs

General

Echo cancellation: ☑ Use canceller, with tail delay: 128

☑ Dynamic attenuation

Voice activity detection threshold: -17 (-20 - +10 DBM)

Idle noise level: -65 (-327 - +327 DBM)

Signaling options: ☑ DTMF tone detection

□ Low latency mode

☑ Remove DTMF delay (squelch DTMF from TDM to IP)

☑ Modem/Fax pass-through

□ V.21 Fax tone detection

□ R factor calculation

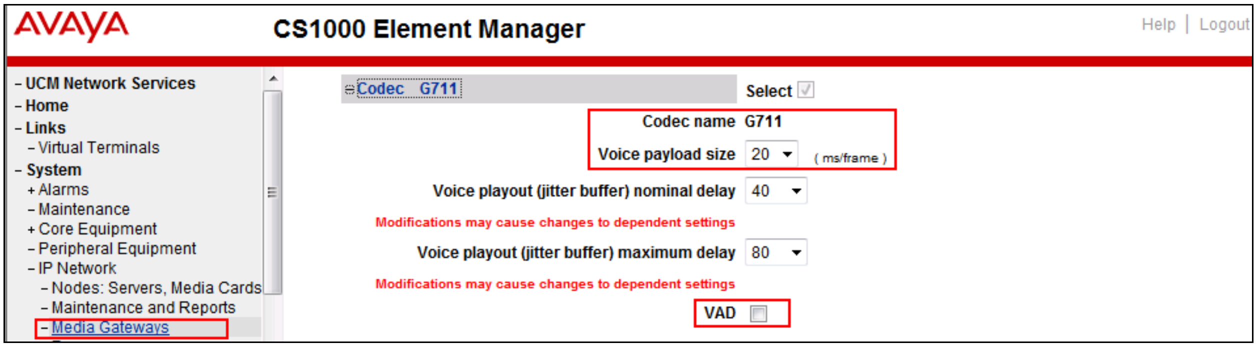
Click **Save** (not shown) then synchronize the new configuration (see **Section 5.2.3**).

5.3.2. Administer Voice Codec on Media Gateways

The CS1000 uses Media Gateways to support traditional analog and digital phones for voice calls over a SIP Trunk. Media Gateways are also needed to support analog terminals to send fax over IP.

To configure Voice Codec on Media Gateways, from the left menu of the Element Manager page (not shown), select the **IP Network → Media Gateways** menu item. The Media Gateways page will appear (not shown). Click on the **MGC** which is located on the right of the page (not shown).

Windstream supports voice codec G.711, payload size 20 ms, with VAD disabled. The screenshot below shows appropriated codec profile configured for Media Gateways.



Codec G711 — Select ☑

Codec name G711

Voice payload size 20 (ms/frame)

Voice playout (jitter buffer) nominal delay 40

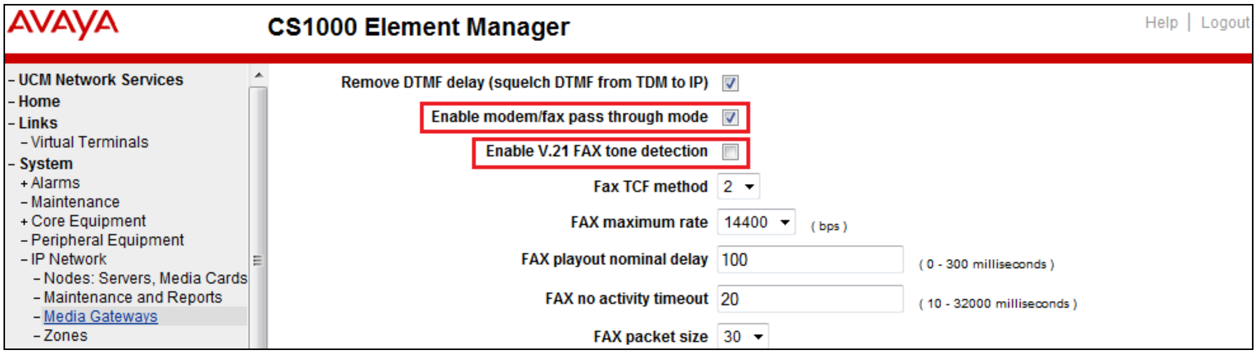
Modifications may cause changes to dependent settings

Voice playout (jitter buffer) maximum delay 80

Modifications may cause changes to dependent settings

VAD ☐

For Fax over IP, Windstream supports G.711 codec as default and does not support T.38. The following screenshot shows **Enable modem/fax pass through mode** is selected for Media Gateway, this enables G.711MU codec to be used for fax calls between the CS1000 and Windstream. **Note**: The **Enable V.21 FAX tone detection** should not be checked to disable T.38 fax capability on the Media Gateway.



Remove DTMF delay (squelch DTMF from TDM to IP) ☑

Enable modem/fax pass through mode ☑

Enable V.21 FAX tone detection ☐

Fax TCF method 2

FAX maximum rate 14400 (bps)

FAX playout nominal delay 100 (0 - 300 milliseconds)

FAX no activity timeout 20 (10 - 32000 milliseconds)

FAX packet size 30

5.4. Administer Zones and Bandwidth

This section describes the steps to create two zones: zone **10** for VGW and IP phone and zone **255** for SIP virtual trunk. The CS1000 uses zone configuration for bandwidth management purposes.

Windstream supports G.711 and G.729 codec on the test environment. In the sample configuration as shown in the screenshots below, the **MO** zone **10** and **VTRK** zone **255** were configured with **Strategy Best Quality (BQ)** to allow the CS1000 to prioritize the G.711 codec for both voice and fax calls. **Note**: In the fax call scenario, the call has to be established with G.711 codec; otherwise, it will fail because the CS1000 cannot switch the codec over to G.711.

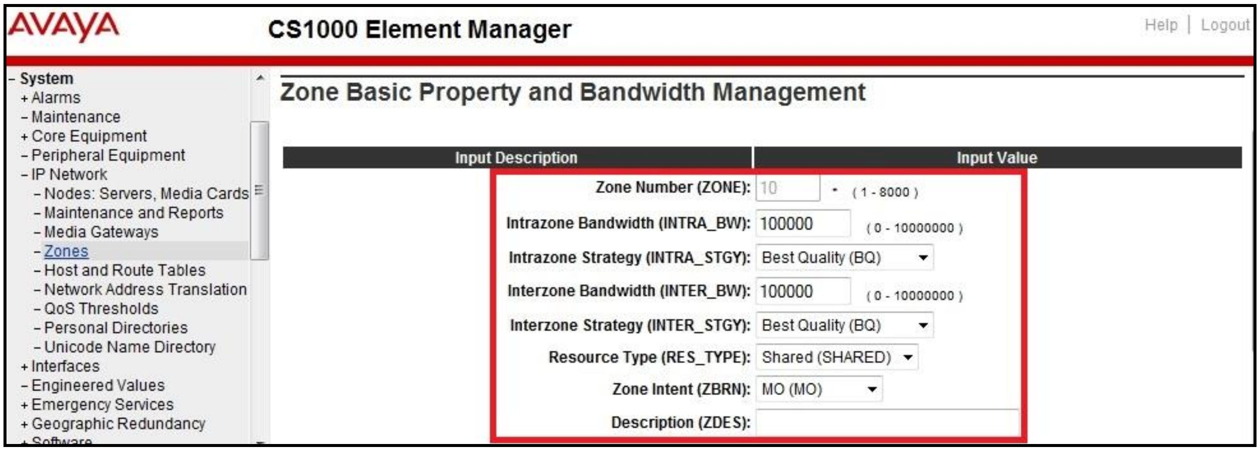
In general, a bandwidth zone is configured with parameters described as following:

- **INTRA_STGY**: Bandwidth configuration for local calls.
- **INTER_STGY**: Bandwidth configuration for the calls over the SIP Trunk.
- **BQ**: G.711 is first choice and G.729 is second choice.
- **BB**: G.729 is first choice and G.711 is second choice.
- **MO**: The zone type which is used for IP phones and VGW.
- **VTRK**: The zone type which is used for the SIP Trunk.

5.4.1. Create Zone for VGW and IP phones

To create a MO zone **10** for VGW and IP phone, select **IP Network → Zones** from the left pane then configure as following:

- Click **Bandwidth Zones** link (not shown).
- In **Bandwidth Zones** screen, click **Add** button (not shown).
- In the **Add Bandwidth Zone** screen, click on **Zone Basic Property and Bandwidth Management**, select the values as shown (in red box) in the screenshot below and click on the **Submit** button (not shown).

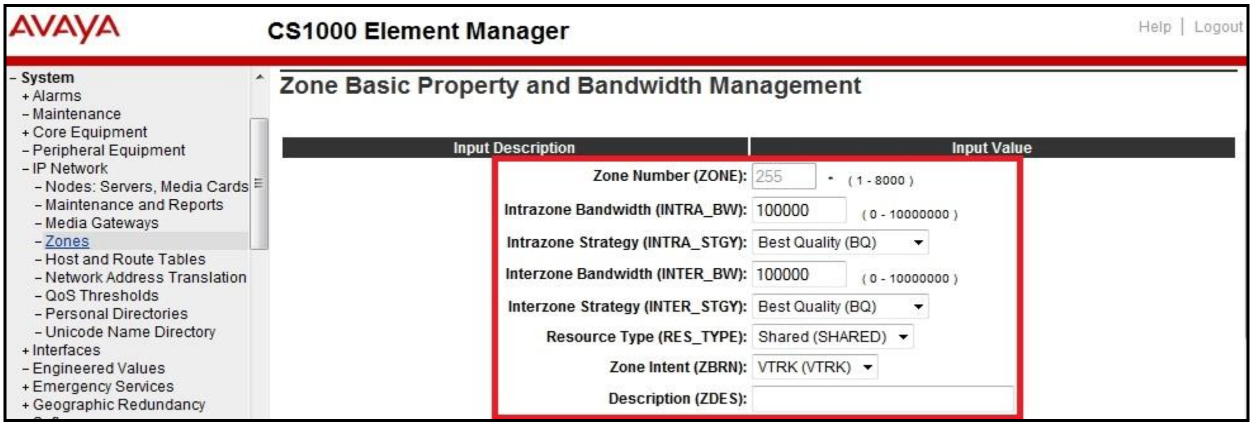


Zone Basic Property and Bandwidth Management

Input Description	Input Value
Zone Number (ZONE):	10 * (1 - 8000)
Intrazone Bandwidth (INTRA_BW):	100000 (0 - 10000000)
Intrazone Strategy (INTRA_STGY):	Best Quality (BQ)
Interzone Bandwidth (INTER_BW):	100000 (0 - 10000000)
Interzone Strategy (INTER_STGY):	Best Quality (BQ)
Resource Type (RES_TYPE):	Shared (SHARED)
Zone Intent (ZBRN):	MO (MO)
Description (ZDES):	

5.4.2. Create Zone for Virtual SIP Trunk

Follow **Section 5.4.1** to create a VTRK zone **255** for the virtual trunk. The difference is in the **Zone Intent (ZBRN)** field, select **VTRK** for virtual trunk as shown in the screenshot below then click **Submit** button (not shown).



Zone Basic Property and Bandwidth Management

Input Description	Input Value
Zone Number (ZONE):	255 * (1 - 8000)
Intrazone Bandwidth (INTRA_BW):	100000 (0 - 10000000)
Intrazone Strategy (INTRA_STGY):	Best Quality (BQ)
Interzone Bandwidth (INTER_BW):	100000 (0 - 10000000)
Interzone Strategy (INTER_STGY):	Best Quality (BQ)
Resource Type (RES_TYPE):	Shared (SHARED)
Zone Intent (ZBRN):	VTRK (VTRK)
Description (ZDES):	

5.5. Administer SIP Trunk Gateway

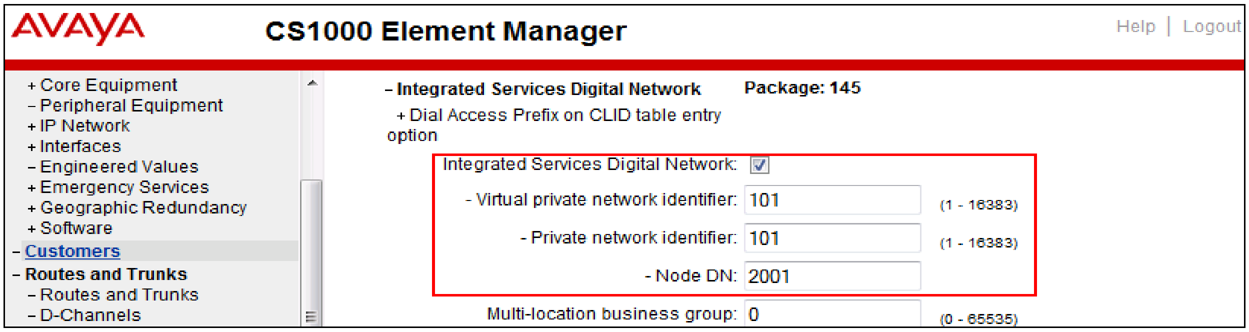
This section describes the steps for establishing a SIP Trunk between the CS1000 SIP Signaling Gateway (SSG) to the Avaya SBCE.

5.5.1. Integrated Services Digital Network (ISDN)

To configure ISDN, select **Customers** in the left pane. The **Customers** screen is displayed (not shown). Click on the link associated with the appropriate customer, in this case is **01**. The system can support more than one customer with different network settings and options. The **Customer 01 Edit** page will appear (not shown). Select the **Feature Packages** option from this page (not shown).

The screen is populated with a list of **Feature Packages**. Select **Integrated Services Digital Network** to edit its parameters. The screen is populated with **Integrated Services Digital Network** parameters as follows.

- Virtual private network identifier: Enter a valid value, e.g. **101**.
- Private network identifier: Enter a valid value, e.g. **101**.
- Node DN: Enter the Node DN, e.g. **2001**.



- Integrated Services Digital Network Package: 145

+ Dial Access Prefix on CLID table entry option

Integrated Services Digital Network: ☑

- Virtual private network identifier: 101 (1 - 16383)

- Private network identifier: 101 (1 - 16383)

- Node DN: 2001

Multi-location business group: 0 (0 - 65535)

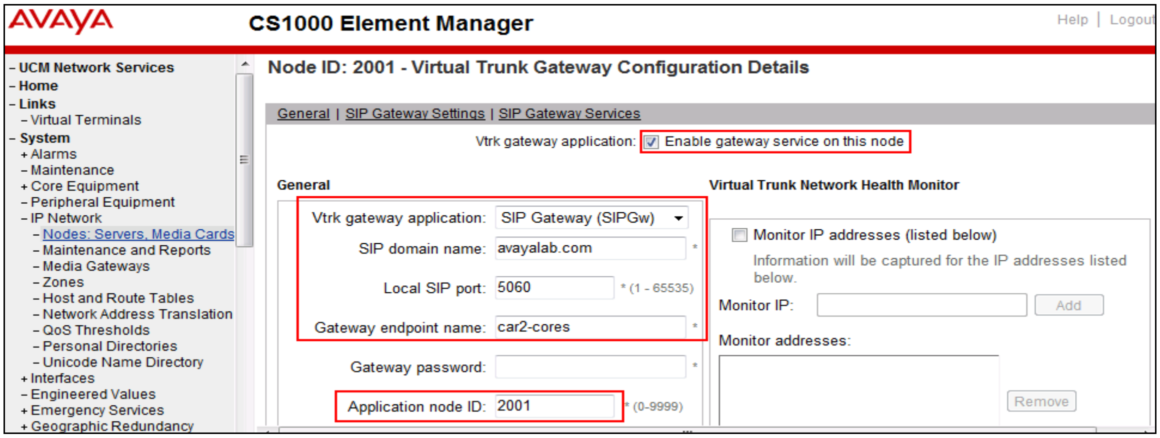
Retain the default values for all remaining fields. Scroll down to the bottom of the screen then click **Save** button (not shown).

5.5.2. Administer SIP Trunk Gateway to the Avaya SBCE

To configure SIP Trunk Gateway, select **IP Network → Nodes: Servers, Media Cards** configuration from the left pane, and in the **IP Telephony Nodes** screen, select the **Node ID 2001**. The **Node Details** screen is displayed as shown in **Section 5.2.1**.

On the **Node Details** screen, select **Gateway (SIPGw)** (not shown). Check on the check box "**Enable gateway service on this node**". Under **General** tab of the **Virtual Trunk Gateway Configuration Details** screen, enter the following values which are highlighted in red boxes as shown in screenshot below.

- **Vtrk gateway application**: Select **SIP Gateway (SIPGw)**.
- **SIP domain name**: An enterprise SIP Domain name, e.g., **avayalab.com**.
- **Local SIP port**: A port open to receive SIP traffic, e.g., **5060**.
- **Gateway endpoint name**: A descriptive name for SIP Gateway, e.g., **car2-cores**.
- **Application node ID**: An available node ID, e.g., **2001**.



Node ID: 2001 - Virtual Trunk Gateway Configuration Details

Vtrk gateway application: ☑ Enable gateway service on this node

Vtrk gateway application: SIP Gateway (SIPGw)

SIP domain name: avayalab.com *

Local SIP port: 5060 * (1 - 65535)

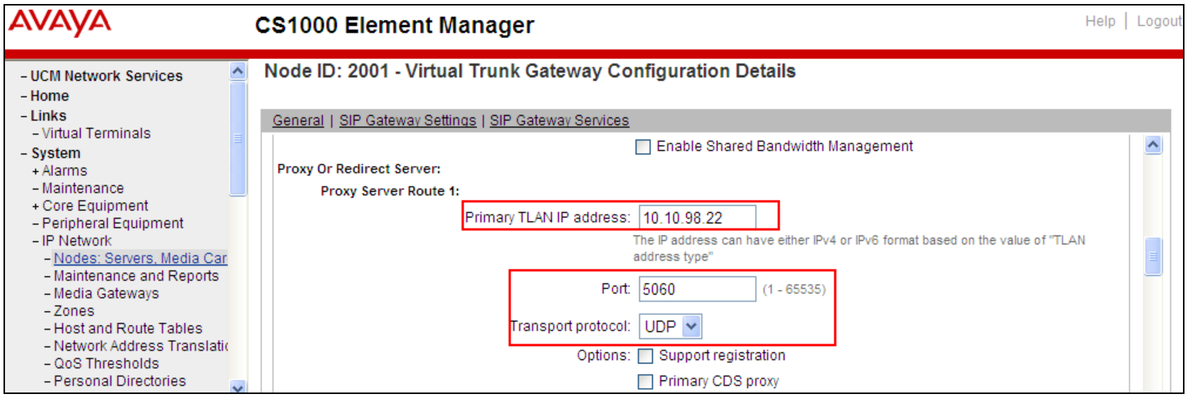
Gateway endpoint name: car2-cores *

Gateway password: *

Application node ID: 2001 * (0-9999)

□ Monitor IP addresses (listed below)

Click on the **SIP Gateway Settings** tab, under **Proxy or Redirect Server**, enter the internal IP address of Avaya SBCE as shown in the screenshot below, and retain the default values for the remaining fields.



Node ID: 2001 - Virtual Trunk Gateway Configuration Details

□ Enable Shared Bandwidth Management

Proxy Or Redirect Server:

Proxy Server Route 1:

Primary TLAN IP address: 10.10.98.22

The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"

Port: 5060 (1 - 65535)

Transport protocol: UDP

Options: □ Support registration

□ Primary CDS proxy

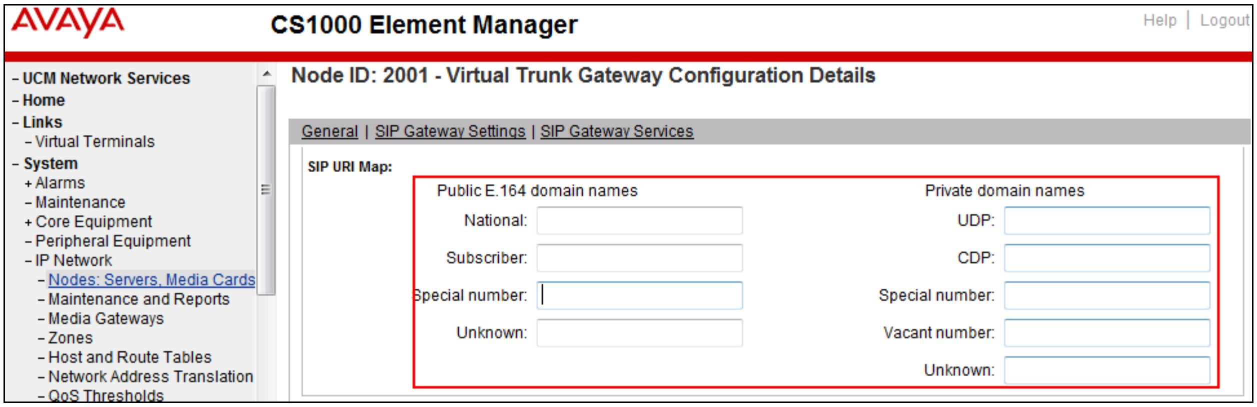
On the same page, scroll down to the **SIP URI Map** section as shown in the screenshot below. The URI Map settings were set to blank to disable the "phone-context" from being sent because it is not required by Windstream.

Under the **Public E.164 Domain Names**:

- **National**: Set the field to blank.
- **Subscriber**: Set the field to blank.
- **Special Number**: Set the field to blank.
- **Unknown**: Set the field to blank.

Under the **Private Domain Names**:

- **UDP**: Set the field to blank.
- **CDP**: Set the field to blank.
- **Special Number**: Set the field to blank.
- **Vacant number**: Set the field to blank.
- **Unknown**: Set the field to blank.



Node ID: 2001 - Virtual Trunk Gateway Configuration Details

SIP URI Map:

Public E.164 domain names		Private domain names	
National:		UDP:	
Subscriber:		CDP:	
Special number:		Special number:	
Unknown:		Vacant number:	
		Unknown:	

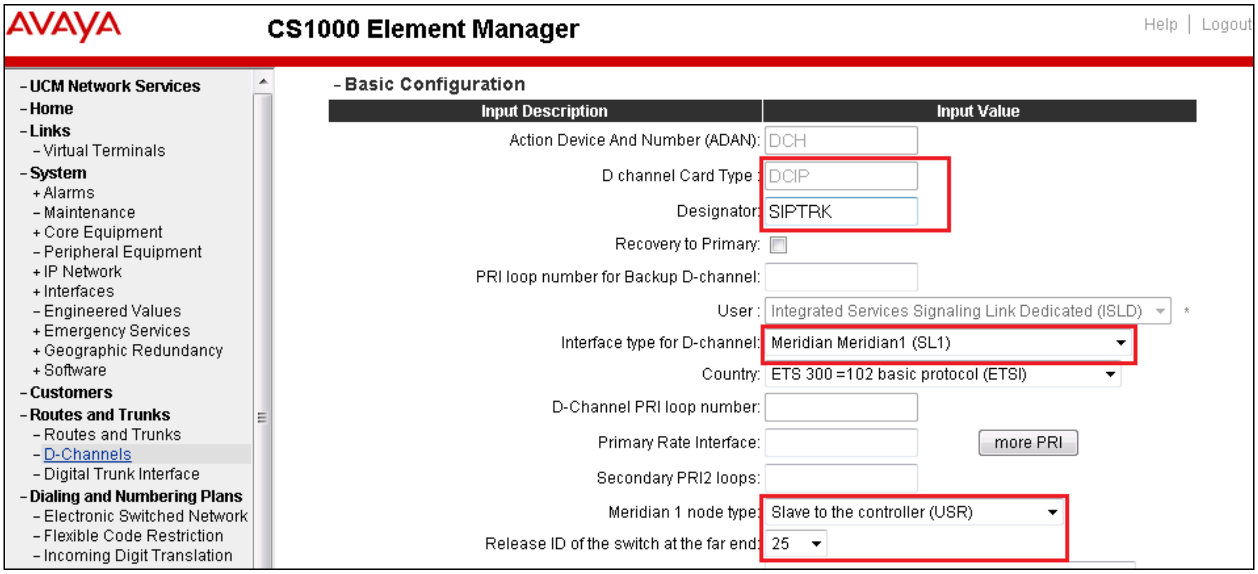
Then click **Save** button (not shown) and synchronize the new configuration (see **Section 5.2.3**).

5.5.3. Administer Virtual D-Channel

To create a D-Channel, select **Routes and Trunks → D-Channels** from the left pane to display the **D-Channels** screen (not shown). In the **Choose a D-Channel Number** field, select an available D-channel from the drop-down list (not shown). Click on **to Add** button (not shown)**.**

The **D-Channels Property Configuration** of DCH **101**is shown in the screenshot below. Enter the following values for the specified fields, and retain the default values for the remaining fields.

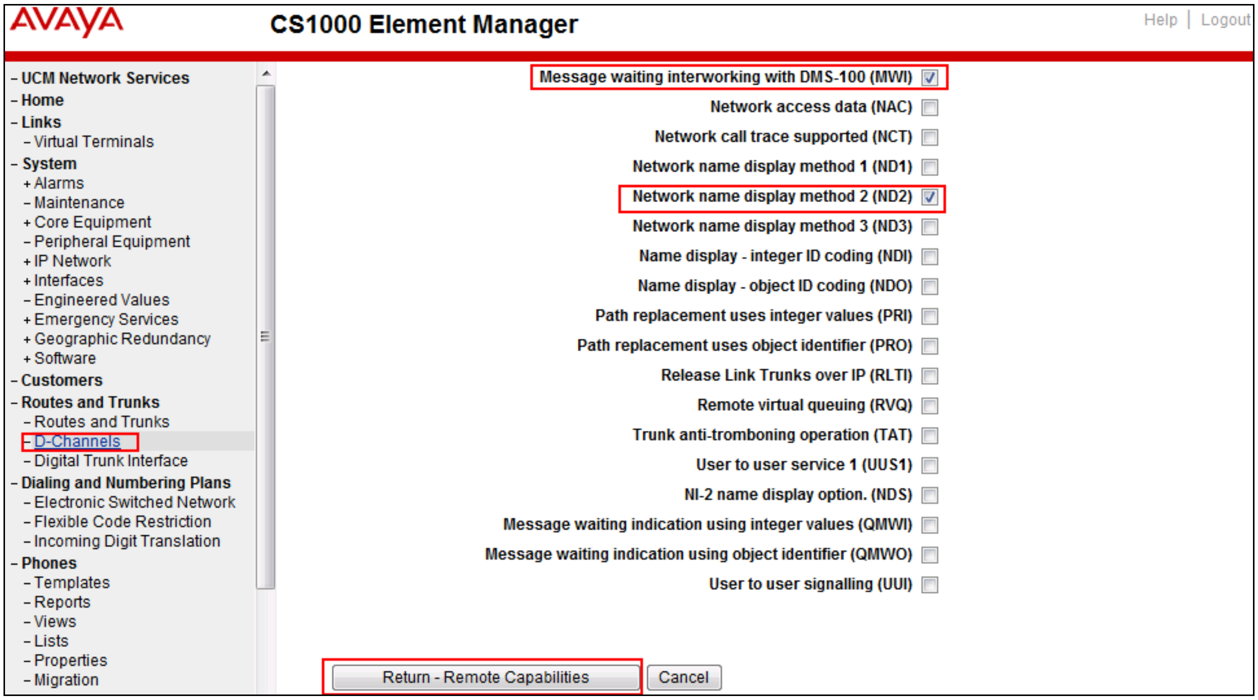
- **D channel Card Type (CTYP)**: D-Channel is over IP (DCIP).
- **Designator (DES)**: A descriptive name.
- **Interface type for D-channel (IFC)**: Meridian Meridian1 (SL1).
- **Meridian 1 node type**: Slave to the controller (USR).
- **Release ID of the switch at the far end (RLS)**: 25.



- Basic Configuration

Input Description	Input Value
Action Device And Number (ADAN):	DCH
D channel Card Type :	DCIP
Designator:	SIPTRK
Recovery to Primary:	□
PRI loop number for Backup D-channel:	
User :	Integrated Services Signaling Link Dedicated (ISLD) *
Interface type for D-channel:	Meridian Meridian1 (SL1)
Country:	ETS 300 =102 basic protocol (ETSI)
D-Channel PRI loop number:	
Primary Rate Interface:	
Secondary PRI2 loops:	
Meridian 1 node type:	Slave to the controller (USR)
Release ID of the switch at the far end:	25

Click on the **Basic Options** then click on the **Edit** button at the **Remote Capabilities** (**RCAP**) attribute (not shown). The **Remote Capabilities Configuration** page will appear. Then check on the **Message waiting interworking with DMS-100 (MWI)** and the **Network name display method 2 (ND2)** checkboxes as shown in the screenshot below.

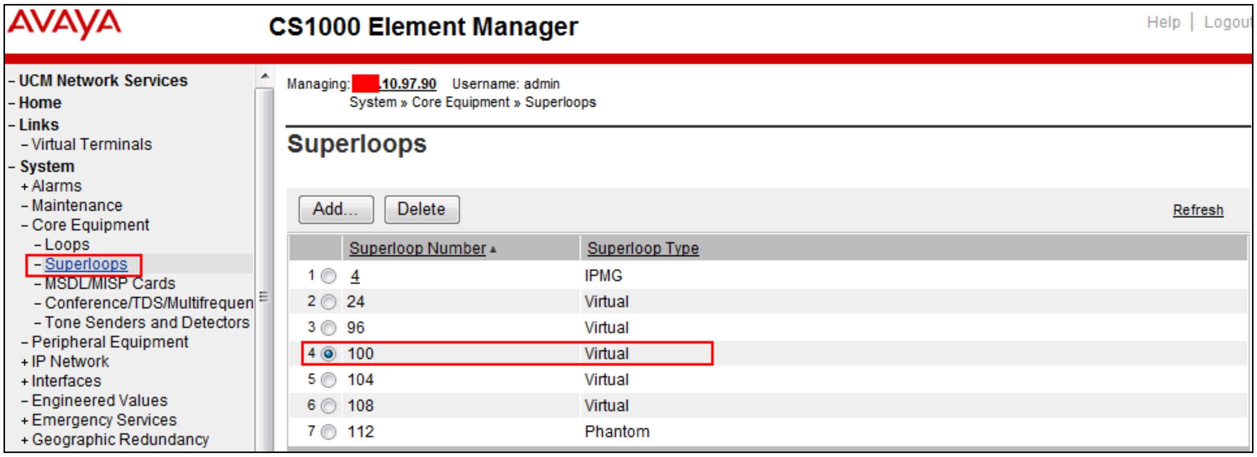


Message waiting interworking with DMS-100 (MWI) ☑
Network access data (NAC) □
Network call trace supported (NCT) □
Network name display method 1 (ND1) □
Network name display method 2 (ND2) ☑
Network name display method 3 (ND3) □
Name display - integer ID coding (NDI) □
Name display - object ID coding (NDO) □
Path replacement uses integer values (PRI) □
Path replacement uses object identifier (PRO) □
Release Link Trunks over IP (RLTI) □
Remote virtual queuing (RVQ) □
Trunk anti-tromboning operation (TAT) □
User to user service 1 (UUS1) □
NI-2 name display option. (NDS) □
Message waiting indication using integer values (QMWI) □
Message waiting indication using object identifier (QMWO) □
User to user signalling (UUI) □

Click **Return – Remote Capabilities** button then click **Submit** button (not shown).

5.5.4. Administer Virtual Super-Loop

To add a virtual loop, select **System → Core Equipment → Superloops** from the left pane to display the **Superloops** screen. If the Superloop does not exist, click **Add** button to create a new one as shown in the screenshot below. In this example, Superloop **100** was added.



Managing: [redacted].10.97.90 Username: admin
System » Core Equipment » Superloops

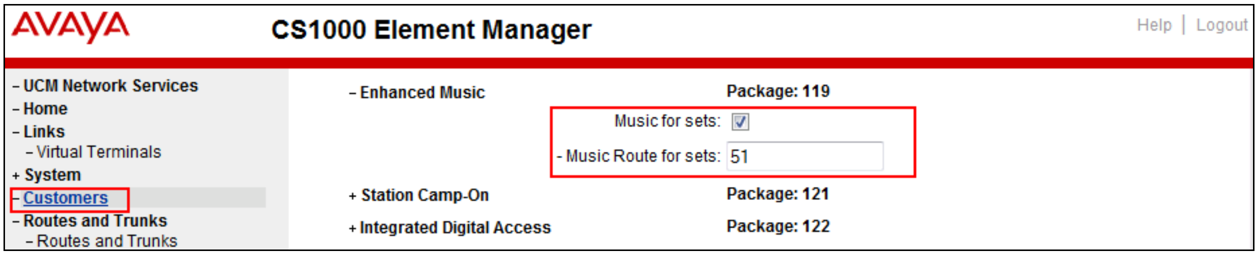
Superloops

	Superloop Number ▴	Superloop Type
1 ○	4	IPMG
2 ○	24	Virtual
3 ○	96	Virtual
4 ●	100	Virtual
5 ○	104	Virtual
6 ○	108	Virtual
7 ○	112	Phantom

5.5.5. Enable Music for Customer Data Block

To enable music for a customer, select **Customers** in the left pane. The **Customers** screen is displayed (not shown). Click on the link associated with the appropriate customer, in this case is **01**. The **Customer 01 Edit** page will appear (not shown). Select the **Feature Packages** option from this page (not shown).

The screen is populated with a list of F**eature Packages**. Select **Enhanced Music** to edit its parameters. Check **Music for sets** to enable music for Customer **01**, define **Music Route for sets 51** as shown in the red box of the screenshot below. The CS1000 has been pre-configured with music route **51**.

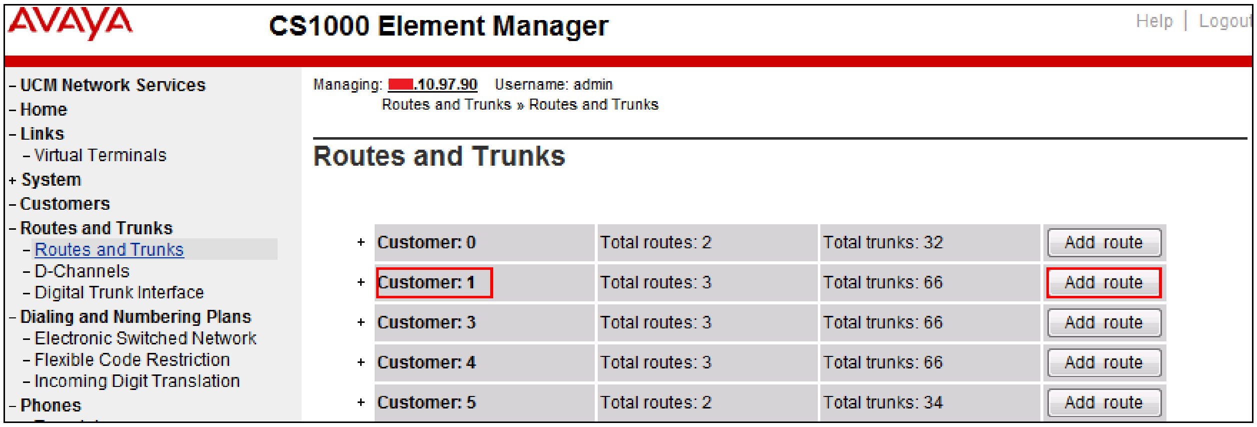


- Enhanced Music Package: 119
Music for sets: ☑
- Music Route for sets: 51
+ Station Camp-On Package: 121
+ Integrated Digital Access Package: 122

Scroll down to the bottom of the screen and click **Save** button (not shown).

5.5.6. Administer Virtual SIP Route

To create a SIP Route, select **Routes and Trunks** → **Routes and Trunks** from the left pane to display the **Routes and Trunks** screen. In this example, the new route is added under **Customer 1**. Click **Add route** button as shown in the screenshot below.



Managing: [redacted].10.97.90 Username: admin
Routes and Trunks » Routes and Trunks

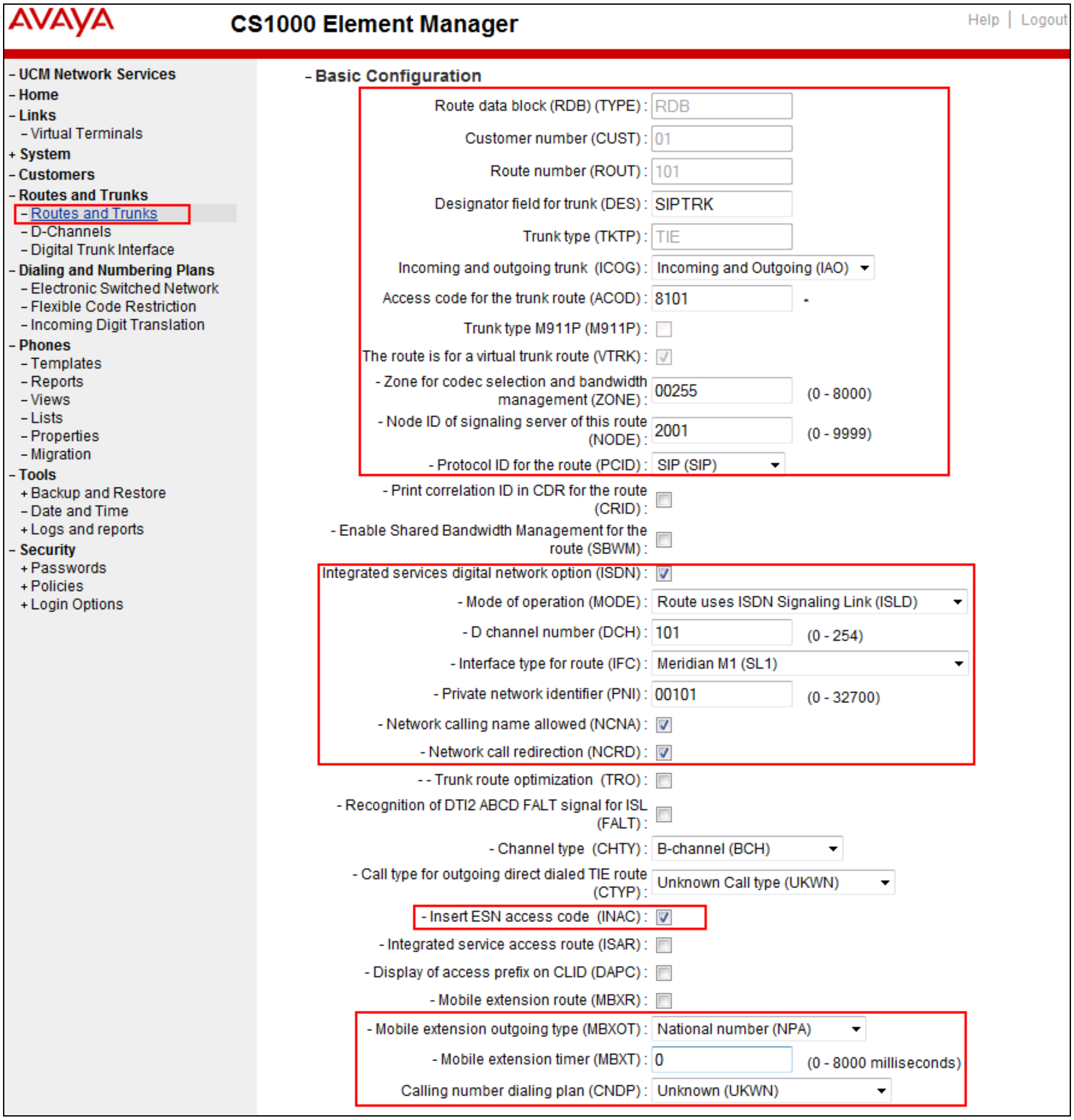
Routes and Trunks

+	Customer: 0	Total routes: 2	Total trunks: 32	Add route
+	Customer: 1	Total routes: 3	Total trunks: 66	Add route
+	Customer: 3	Total routes: 3	Total trunks: 66	Add route
+	Customer: 4	Total routes: 3	Total trunks: 66	Add route
+	Customer: 5	Total routes: 2	Total trunks: 34	Add route

The **Customer 1**, New **Route Configuration** screen is displayed (not shown). Scroll down until the **Basic Configuration** section is displayed and enter the following values for the specified fields, and retain the default values for the remaining fields as shown in the screenshot below.

- **Route Number (ROUT)**: Select an available route number, e.g., **101**.
- **Designator field for trunk (DES)**: A descriptive text.
- **Trunk Type (TKTP)**: **TIE trunk data block (TIE)**.
- **Incoming and Outgoing trunk (ICOG)**: **Incoming and Outgoing (IAO)**.
- **Access Code for the trunk route (ACOD)**: An available access code.
- Check the field **The route is for a virtual trunk route (VTRK**), to enable additional fields to appear.
- For the **Zone for codec selection and bandwidth management (ZONE)** field, enter zone **255** (created in **Section 5.4.2**).
- For the **Node ID of signalling server of this route (NODE)** field, enter the node number **2001** (created in **Section 5.2.1**).
- Select **SIP (SIP)** from the drop-down list for **the Protocol ID for the route (PCID)** field.
- Check the **Integrated Services Digital Network option (ISDN)** checkbox to enable additional fields to appear. Enter the following values for the specified fields, and retain the default values for the remaining fields.
  - **Mode of operation (MODE)**: **Route uses ISDN Signalling Link (ISLD)**.
  - **D channel number (DCH)**: D-Channel number **101** (created in **Section 5.5.3**).
  - **Network calling name allowed (NCNA)**: Checked.
  - **Network call redirection (NCRD)**: Checked.
  - **Insert ESN access code (INAC):** Checked.
  - **Mobile extension outgoing type (MBXOT)**: Select **National number (NPA)**.

- ○ **Mobile extension timer (MBXT)**: Define an appropriate value to meet the certain deployment at the enterprise network. For this compliance test, the default value of 0 ms is used.
- ○ **Calling number dialling plan (CNDP)**: Unknown (UKWN).



- Basic Configuration

Route data block (RDB) (TYPE) : RDB

Customer number (CUST) : 01

Route number (ROUT) : 101

Designator field for trunk (DES) : SIPTRK

Trunk type (TKTP) : TIE

Incoming and outgoing trunk (ICOG) : Incoming and Outgoing (IAO)

Access code for the trunk route (ACOD) : 8101

Trunk type M911P (M911P) : □

The route is for a virtual trunk route (VTRK) : ☑

- Zone for codec selection and bandwidth management (ZONE) : 00255 (0 - 8000)

- Node ID of signaling server of this route (NODE) : 2001 (0 - 9999)

- Protocol ID for the route (PCID) : SIP (SIP)

- Print correlation ID in CDR for the route (CRID) : □

- Enable Shared Bandwidth Management for the route (SBWM) : □

Integrated services digital network option (ISDN) : ☑

- Mode of operation (MODE) : Route uses ISDN Signaling Link (ISLD)

- D channel number (DCH) : 101 (0 - 254)

- Interface type for route (IFC) : Meridian M1 (SL1)

- Private network identifier (PNI) : 00101 (0 - 32700)

- Network calling name allowed (NCNA) : ☑

- Network call redirection (NCRD) : ☑

- - Trunk route optimization (TRO) : □

- Recognition of DTI2 ABCD FALT signal for ISL (FALT) : □

- Channel type (CHTY) : B-channel (BCH)

- Call type for outgoing direct dialed TIE route (CTYP) : Unknown Call type (UKWN)

- Insert ESN access code (INAC) : ☑

- Integrated service access route (ISAR) : □

- Display of access prefix on CLID (DAPC) : □

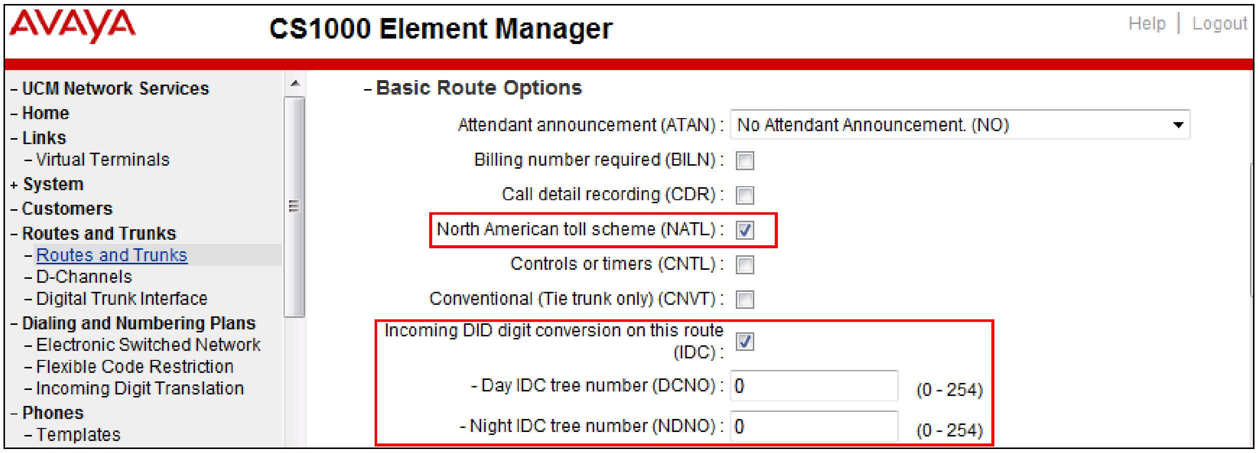
- Mobile extension route (MBXR) : □

- Mobile extension outgoing type (MBXOT) : National number (NPA)

- Mobile extension timer (MBXT) : 0 (0 - 8000 milliseconds)

Calling number dialing plan (CNDP) : Unknown (UKWN)

Click on **Basic Route Options**, check **North American toll scheme (NATL)** and **Incoming DID digit conversion on this route (IDC)**. Enter a value of **0** for both **Day IDC Tree Number (DCN0)** and **Night IDC Tree Number (NDCN0)** as shown in the screenshot below. The IDC is discussed in **Section 5.6.5**.



- Basic Route Options

Attendant announcement (ATAN) : No Attendant Announcement. (NO)

Billing number required (BILN) : □

Call detail recording (CDR) : □

North American toll scheme (NATL) : ☑

Controls or timers (CNTL) : □

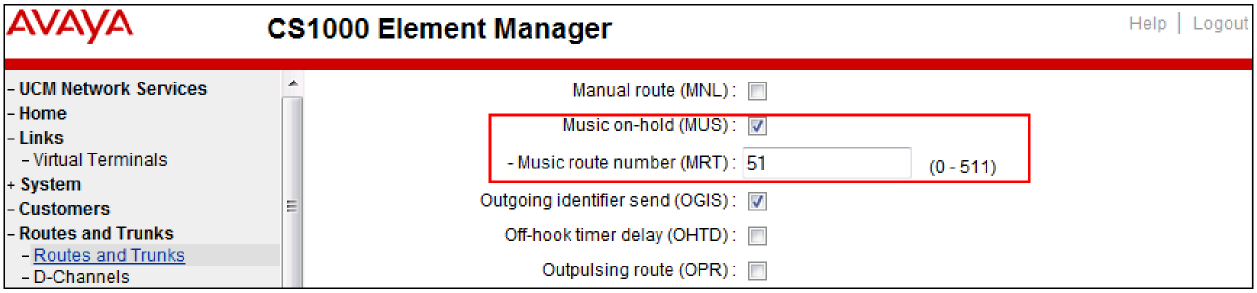
Conventional (Tie trunk only) (CNVT) : □

Incoming DID digit conversion on this route (IDC) : ☑

- Day IDC tree number (DCNO) : 0 (0 - 254)

- Night IDC tree number (NDNO) : 0 (0 - 254)

Click on **Advance Configurations** (not shown); check **Music-on-hold (MUS)** to enable music on hold on this route. Enter a value of **51** to the Music route number (MRT) box as shown in the screenshot below. The CS1000 has been pre-configured with route **51** as a music route.



Manual route (MNL) : □

Music on-hold (MUS) : ☑

- Music route number (MRT) : 51 (0 - 511)

Outgoing identifier send (OGIS) : ☑

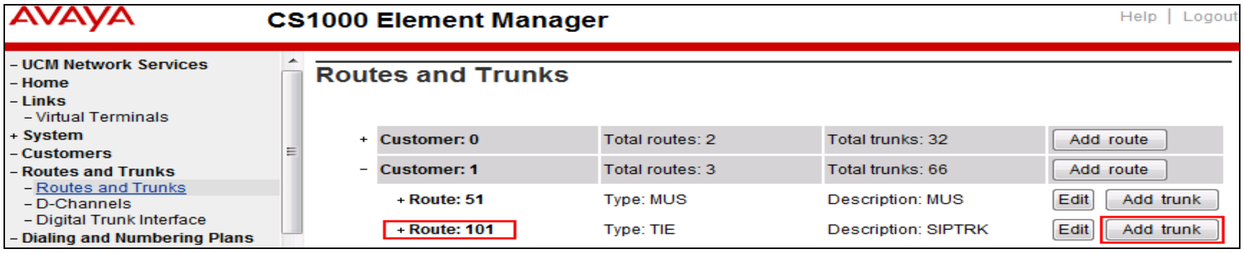
Off-hook timer delay (OHTD) : □

Outpulsing route (OPR) : □

Click **Submit** button (not shown).

5.5.7. Administer Virtual SIP Trunks

To configure the virtual SIP Trunks, select **Route 101** that was added in **Section 5.6.6** then click **Add trunk** button next to the newly added **Route 101** as shown in the screenshot below.

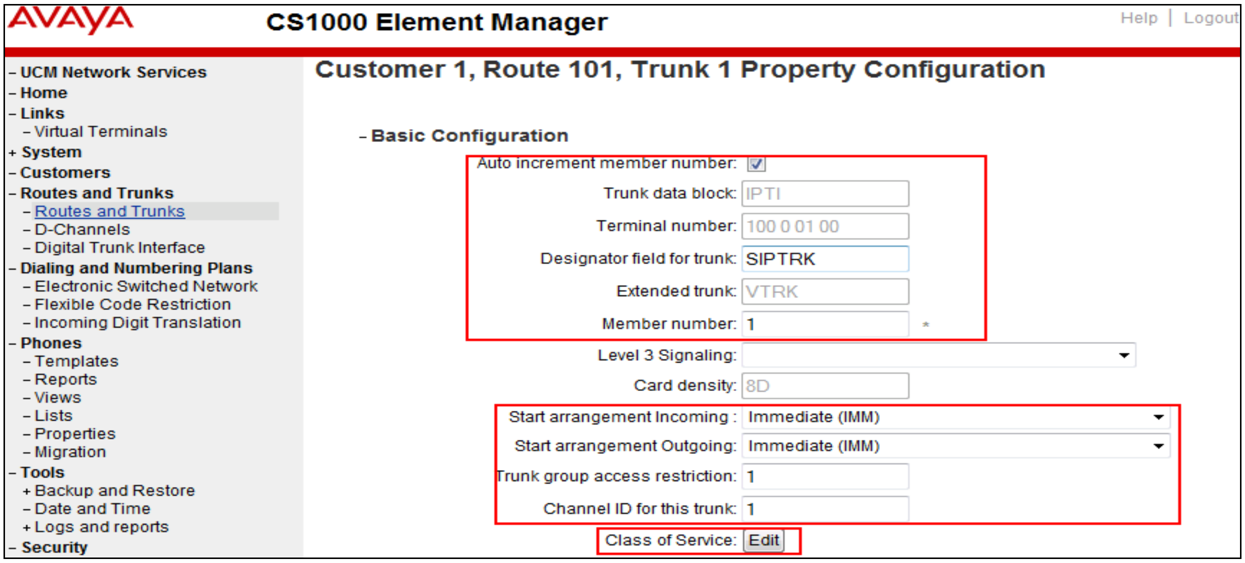


Routes and Trunks

+	Customer: 0	Total routes: 2	Total trunks: 32	Add route
–	Customer: 1	Total routes: 3	Total trunks: 66	Add route
	+ Route: 51	Type: MUS	Description: MUS	Edit Add trunk
	+ Route: 101	Type: TIE	Description: SIPTRK	Edit Add trunk

The **Customer 1, Route 101, Trunk 1 Property Configuration** is shown in the screenshot below. Enter **The Multiple trunk input number (MTINPUT)** field (not shown) to add multiple trunks in a single operation, or repeat the operation for each trunk. In the certification testing, 32 trunks were created (not shown). Enter the following values for the specified fields below and retain the default values for the remaining fields.

- **Trunk data block**: IP Trunk (IPTI).
- **Terminal Number**: Available terminal number (created in **Section 5.5.4**).
- **Designator field for trunk**: A descriptive text.
- **Extended Trunk**: Virtual trunk (VTRK).
- **Member number**: Current route number and starting member.
- **Start arrangement Incoming**: Immediate (IMM).
- **Start arrangement Outgoing**: Immediate (IMM).
- **Trunk Group Access Restriction**: Desired trunk group access restriction level, e.g., **1**.
- **Channel ID for this trunk**: An available starting channel ID, e.g., **1**.



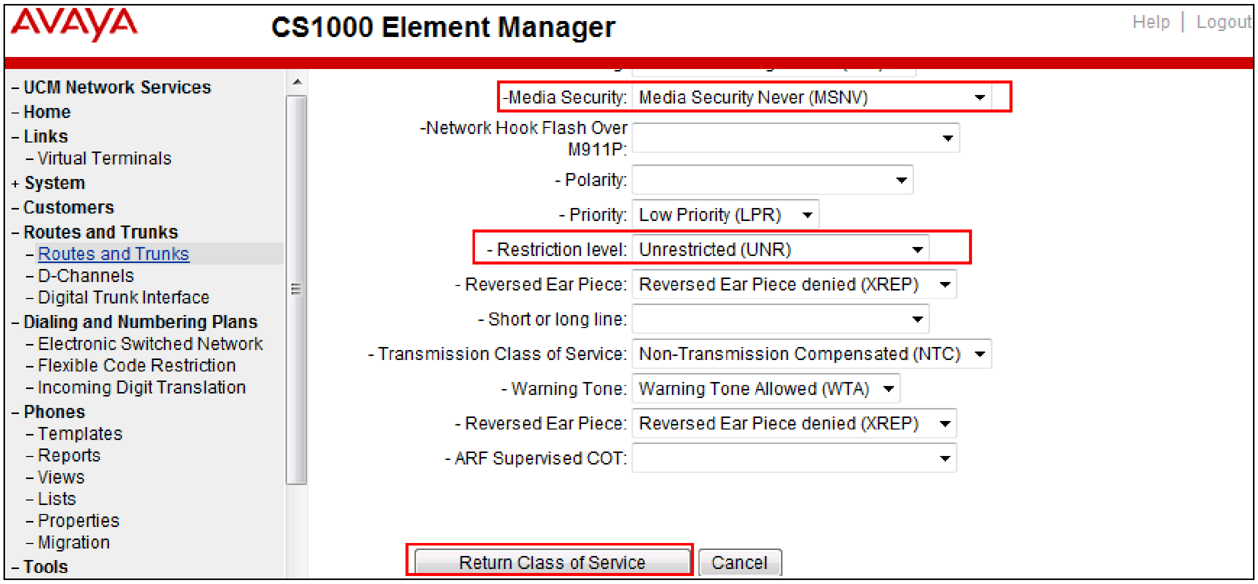
Customer 1, Route 101, Trunk 1 Property Configuration

– Basic Configuration

Auto increment member number: ☑
Trunk data block: IPTI
Terminal number: 100 0 01 00
Designator field for trunk: SIPTRK
Extended trunk: VTRK
Member number: 1 *
Level 3 Signaling:
Card density: 8D
Start arrangement Incoming : Immediate (IMM)
Start arrangement Outgoing: Immediate (IMM)
Trunk group access restriction: 1
Channel ID for this trunk: 1
Class of Service: Edit

Click the **Edit** button adjacent to **Class of Service** to configure the class of service parameters.

To disable SRTP at the trunk level, select **Media Security Never** (**MSNV)**. Select **Restriction level** as **Unrestricted (UNR)**. The remaining values are kept as default as shown in the screenshot below. Scroll down to the bottom of the screen and click **Return Class of Service** and then click **Save** button (not shown).



-Media Security: Media Security Never (MSNV)
-Network Hook Flash Over M911P:
- Polarity:
- Priority: Low Priority (LPR)
- Restriction level: Unrestricted (UNR)
- Reversed Ear Piece: Reversed Ear Piece denied (XREP)
- Short or long line:
- Transmission Class of Service: Non-Transmission Compensated (NTC)
- Warning Tone: Warning Tone Allowed (WTA)
- Reversed Ear Piece: Reversed Ear Piece denied (XREP)
- ARF Supervised COT:

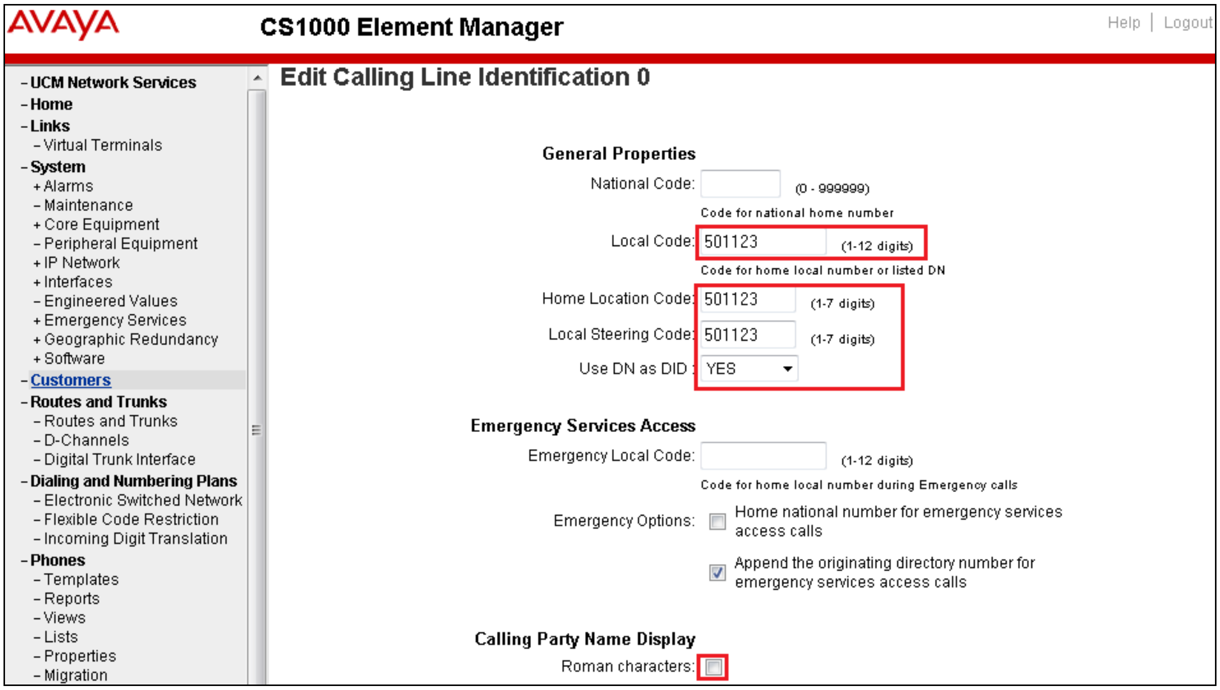
5.5.8. Administer Calling Line Identification Entry

To create Calling Line Identification Entry, select **Customers → 01 → ISDN and ESN Networking**. Click **Calling Line Identification Entries** link at the bottom of the page (not shown).

On the Calling Line Identification Entries page (not shown), click **Add**. Add entry **0** as shown in the screenshot below.

- **National Code**: Leave as blank.
- **Local Code**: Input the prefix what was assigned by the service provider, in this case it is 6 digits **501XXX**. This **Local Code** is used for call display purpose of outgoing call configuration in **Section 5.6.6** where the Special Number is associated with Call Type = NONE. Note that for security reasons the last 3 digits are hidden by XXX but in the real deployment, the local code should be entered with the full 6 digits, e.g., 501123.
- **Home Location Code**: Input the prefix that was assigned by the service provider, in this case it is 6 digits **501XXX**. This **Home Location Code** is used for call display purpose of outgoing call configuration in **Section 5.6.6** where the Special Number is associated with Call Type = National (NPA).
- **Local Steering Code**: Input the prefix that was assigned by the service provider, in this case it is 6 digits **501XXX**. This **Local Steering Code** is used for call display purpose of outgoing call configuration in **Section 5.6.6** where the Special Number is associated with Call Type = National (NXX).

- **Use DN as DID**: Select **YES**. Note that if selecting YES in this option, the local number of the CS1K system will be added at the end of the local code above to create DID numbers known by Windstream.
- **Calling Party Name Display**: Uncheck the **Roman characters** field.
- Click **Save** button (not shown).



Edit Calling Line Identification 0

General Properties

National Code: (0 - 999999)
Code for national home number

Local Code: 501123 (1-12 digits)
Code for home local number or listed DN

Home Location Code: 501123 (1-7 digits)

Local Steering Code: 501123 (1-7 digits)

Use DN as DID : YES

Emergency Services Access

Emergency Local Code: (1-12 digits)
Code for home local number during Emergency calls

Emergency Options: □ Home national number for emergency services access calls

☑ Append the originating directory number for emergency services access calls

Calling Party Name Display

Roman characters: □

5.5.9. Enable External Trunk to Trunk Transferring

This section shows how to enable **External Trunk to Trunk Transferring** feature which is a mandatory configuration to make call transfer and conference work properly over the SIP Trunk.

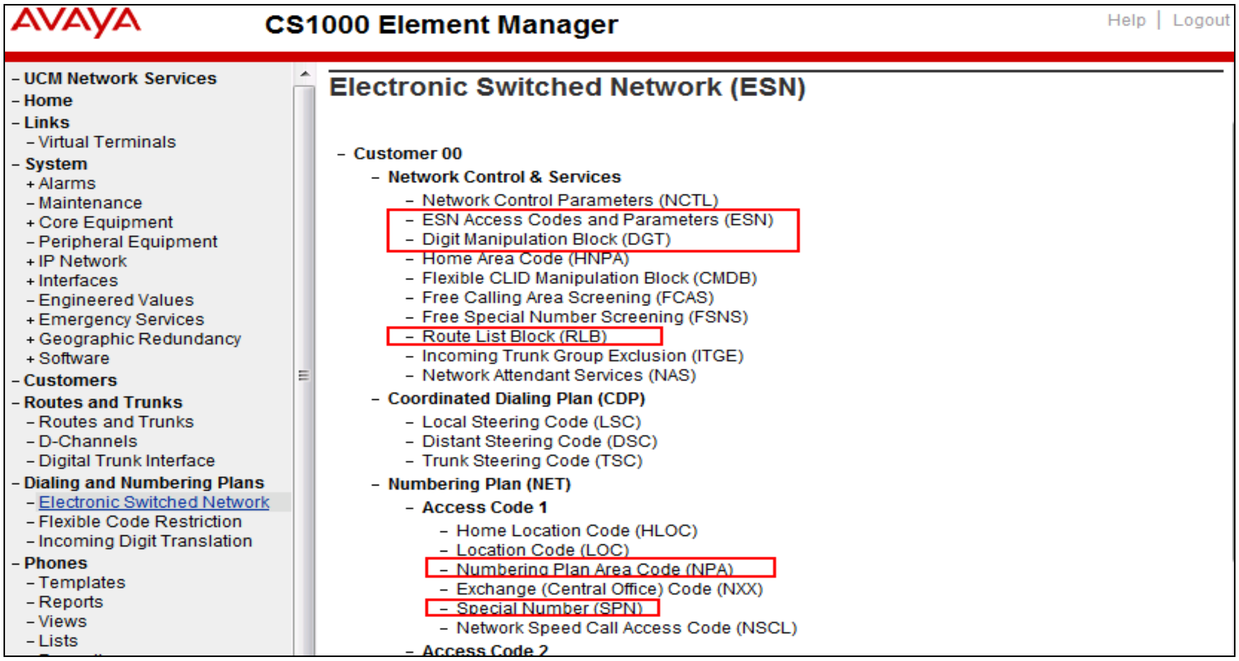
- Log into Call Server CLI (please refer to **Section 5.1.2** for more detail).
- Allow **External Trunk To Trunk Transferring** for **Customer Data Block** by using LD 15.

```
>ld 15
CDB000
MEM AVAIL: (U/P): 35600176    USED U P: 8325631 954062    TOT: 44879869
DISK SPACE NEEDED: 1722 KBYTES
REQ: chg
TYPE: net

TYPE NET_DATA
CUST 1
OPT
…
TRNX YES
EXTT YES
…
```

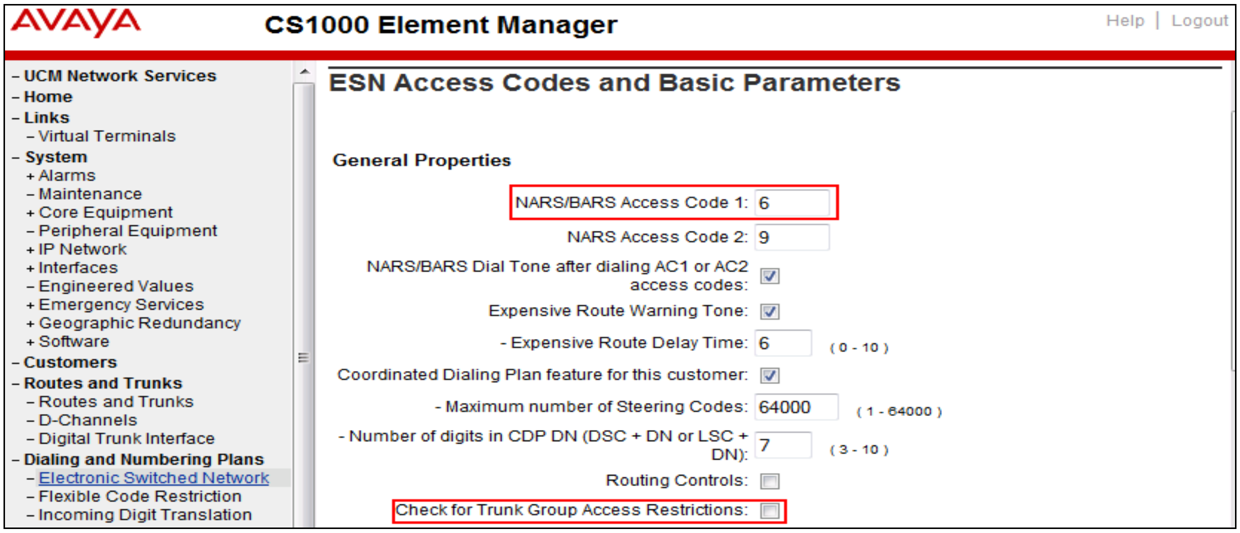
5.6. Administer Dialing Plans

5.6.1. Define ESN Access Codes and Parameters (ESN)

To configure Electronic Switched Network (ESN) parameters, select **Dialing and Numbering Plans → Electronic Switched Network** from the left pane to display the **Electronic Switched Network** (**ESN**) screen. Select **ESN Access Code and Parameters (ESN)** as shown in the screenshot below.


AVAYA
CS1000 Element Manager
Help | Logout
- UCM Network Services
- Home
- Links
- Virtual Terminals
- System
+ Alarms
- Maintenance
+ Core Equipment
- Peripheral Equipment
+ IP Network
+ Interfaces
- Engineered Values
+ Emergency Services
+ Geographic Redundancy
+ Software
- Customers
- Routes and Trunks
- Routes and Trunks
- D-Channels
- Digital Trunk Interface
- Dialing and Numbering Plans
- Electronic Switched Network
- Flexible Code Restriction
- Incoming Digit Translation
- Phones
- Templates
- Reports
- Views
- Lists
Electronic Switched Network (ESN)
- Customer 00
- Network Control & Services
- Network Control Parameters (NCTL)
- ESN Access Codes and Parameters (ESN)
- Digit Manipulation Block (DGT)
- Home Area Code (HNPA)
- Flexible CLID Manipulation Block (CMDB)
- Free Calling Area Screening (FCAS)
- Free Special Number Screening (FSNS)
- Route List Block (RLB)
- Incoming Trunk Group Exclusion (ITGE)
- Network Attendant Services (NAS)
- Coordinated Dialing Plan (CDP)
- Local Steering Code (LSC)
- Distant Steering Code (DSC)
- Trunk Steering Code (TSC)
- Numbering Plan (NET)
- Access Code 1
- Home Location Code (HLOC)
- Location Code (LOC)
- Numbering Plan Area Code (NPA)
- Exchange (Central Office) Code (NXX)
- Special Number (SPN)
- Network Speed Call Access Code (NSCL)
- Access Code 2

In the **ESN Access Codes and Basic Parameters** page, define **NARS/ BARS Access Code 1** and disable **Check for Trunk Group Access Restrictions** as shown in the screenshot below. Click **Submit** button (not shown).



ESN Access Codes and Basic Parameters

General Properties

NARS/BARS Access Code 1: 6

NARS Access Code 2: 9

NARS/BARS Dial Tone after dialing AC1 or AC2 access codes: ☑

Expensive Route Warning Tone: ☑

- Expensive Route Delay Time: 6 (0 - 10)

Coordinated Dialing Plan feature for this customer: ☑

- Maximum number of Steering Codes: 64000 (1 - 64000)

- Number of digits in CDP DN (DSC + DN or LSC + DN): 7 (3 - 10)

Routing Controls: □

Check for Trunk Group Access Restrictions: □

5.6.2. Associate Numbering Plan Area Code (NPA) and Special Number (SPN) calls to ESN Access Code 1

This section shows the configuration to associate the NPA and SPN to ESN Access Code 1.

- Log into Call Server CLI (refer to **Section 5.1.2** for more detail).
- In LD 15, change Customer **Net_Data** block by disabling NPA and SPN to be associated to Access Code 2. It means Access Code 1 will be used for NPA and SPN calls.

```
>ld 15
CDB000
MEM AVAIL: (U/P): 35600086    USED U P: 8325631 954152    TOT: 44879869
DISK SPACE NEEDED: 1722 KBYTES
REQ: chg
TYPE: net

TYPE NET_DATA
CUST 1
OPT
AC2 xNPA xSPN
FNP
CLID
…
```

Verify Customer Net_Data block by using LD 21. The NPA and SPN are now moved to ESN Access Code 1 (AC1).

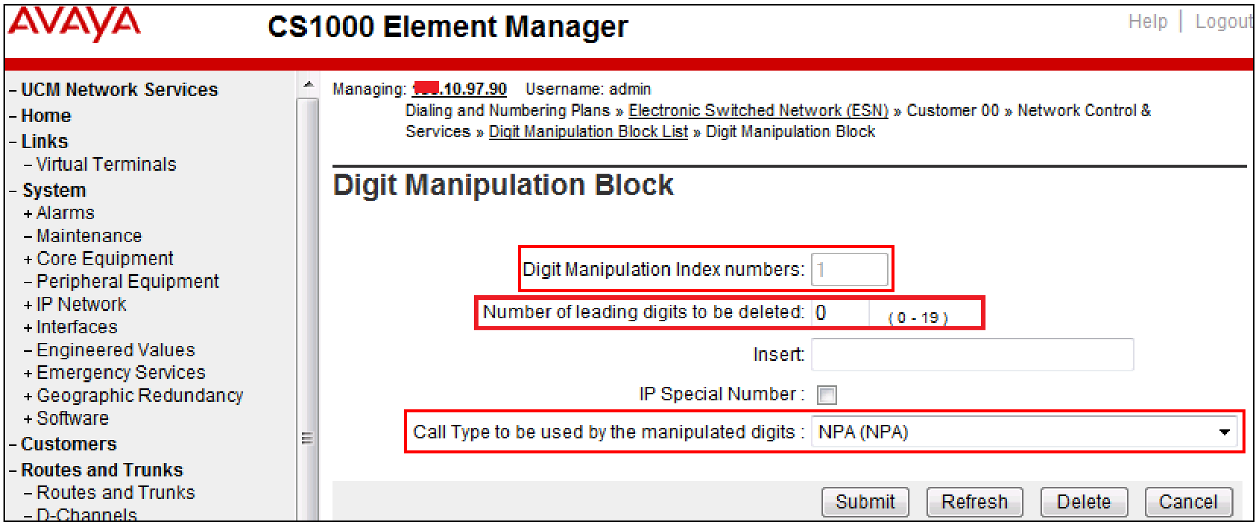
```
>ld 21
PT1000

REQ: prt
TYPE: net
TYPE NET_DATA
CUST 1

TYPE NET_DATA
CUST 01
OPT RTA
AC1 INTL NPA SPN NXX LOC
AC2
FNP YES
…
```

5.6.3. Administer Digit Manipulation Block (DMI)

To create a DMI entry, select **Dialing and Numbering Plans → Electronic Switched Network** from the left pane to display the **Electronic Switched Network** (**ESN**) screen (not shown). Then select **Digit Manipulation Block** (**DGT**) (not shown).

In the **Choose a DMI Number** field, select an available DMI from the drop-down list and click **to Add** (not shown). The screeshot below shows **DMI 1** was created with the following values.

- **Number of leading digits to be deleted** 0.
- **Call Type to be used by the manipulated digits**:NPA (NPA).
- Click **Submit** button.



Managing: [redacted].10.97.90 Username: admin

Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » Digit Manipulation Block List » Digit Manipulation Block

Digit Manipulation Block

Digit Manipulation Index numbers: 1

Number of leading digits to be deleted: 0 (0 - 19)

Insert:

IP Special Number : □

Call Type to be used by the manipulated digits : NPA (NPA)

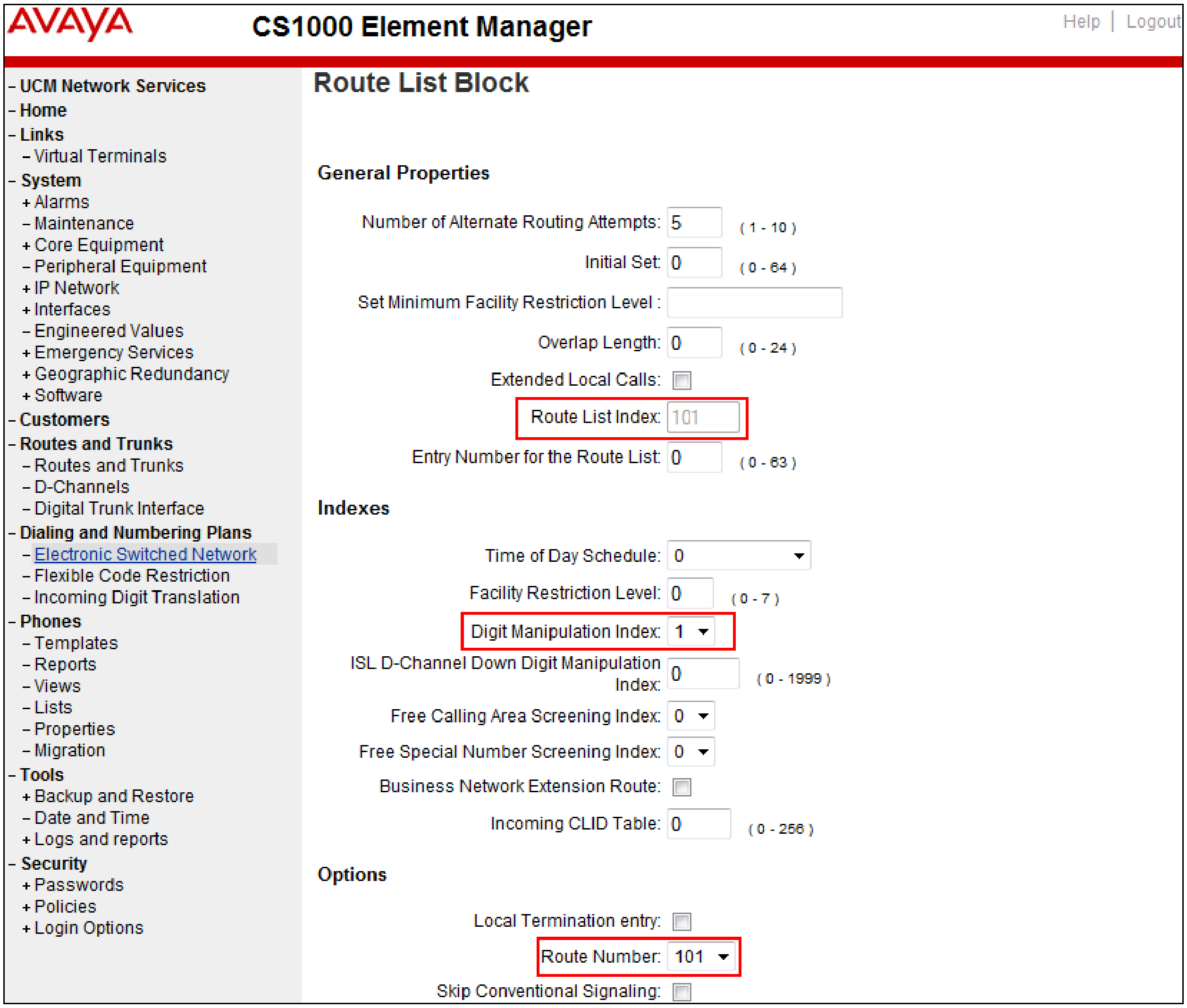
5.6.4. Administer Route List Block (RLB)

This section shows how to add a RLB associated with the DMI 1 created in **Section 0**.

To create **RLB 101** for the certification testing, select **Dialing and Numbering Plans → Electronic Switched Network** from the left pane to display the **Electronic Switched Network** (**ESN**) screen then select **Route List Block** (**RLB**) as shown in **Section 5.6.1**.

Select an available value, e.g., **101** in the textbox for the **route list index** and click on the "**to Add"** button (not shown). Enter the following values for the specified fields as shown in the screenshot below, and retain the default values for the remaining fields.

- **Route number (ROUT)**: **101** (created in **Section 5.5.6**).
- **Digit Manipulation Index (DMI)**: **1** (created in **Section 0**).



Route List Block

General Properties

Number of Alternate Routing Attempts: 5 (1 - 10)

Initial Set: 0 (0 - 64)

Set Minimum Facility Restriction Level :

Overlap Length: 0 (0 - 24)

Extended Local Calls: □

Route List Index: 101

Entry Number for the Route List: 0 (0 - 63)

Indexes

Time of Day Schedule: 0

Facility Restriction Level: 0 (0 - 7)

Digit Manipulation Index: 1

ISL D-Channel Down Digit Manipulation Index: 0 (0 - 1999)

Free Calling Area Screening Index: 0

Free Special Number Screening Index: 0

Business Network Extension Route: □

Incoming CLID Table: 0 (0 - 256)

Options

Local Termination entry: □

Route Number: 101

Skip Conventional Signaling: □

On the same page, scroll down to the bottom of the screen, and click **Submit** button (not shown).

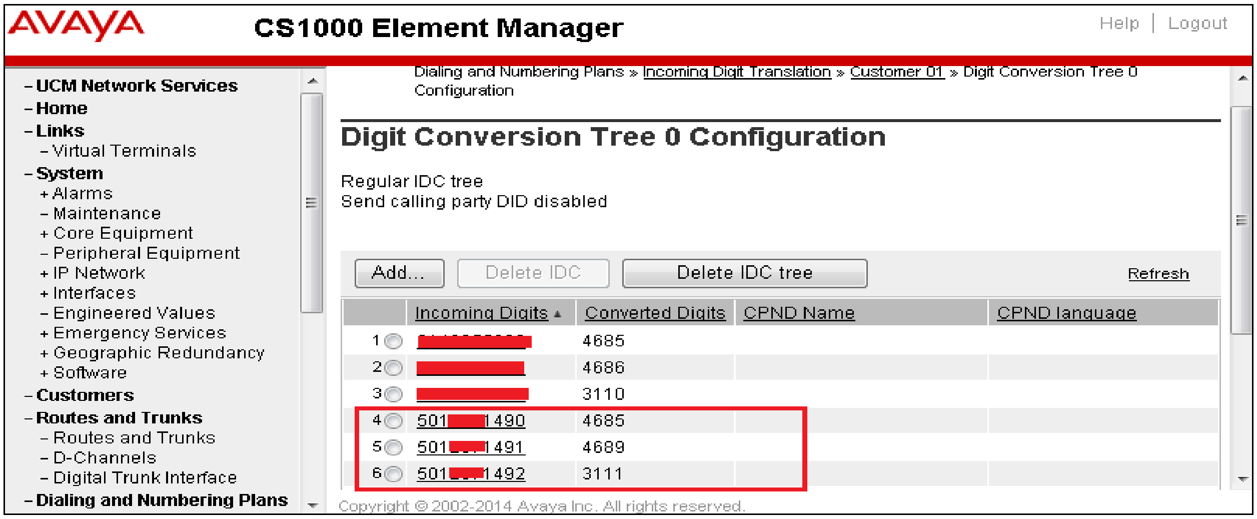
5.6.5. Administer Incoming Digit Translation (IDC)

This section describes the steps for receiving calls from PSTN via Windstream.

To create an IDC, select **Dialing and Numbering Plans → Incoming Digit Translation** from the left pane to display the **Incoming Digit Translation** screen then click on the **Edit IDC** button (not shown).

Click on **New DCNO** to create a digit translation entry (not shown). In this example, **Digit Conversion Tree Number** (**DCN0**) **0** was created. Detailed configuration of the DCNO is shown in the screenshot below. The **Incoming Digits** can be added to map to the **Converted Digits** which would be the CS1000 DN. This DCN0 has been assigned to Route 101 as shown in **Section 5.5.6**.

In the following configuration, incoming calls from PSTN with prefix **501XXX14XX** will be translated to CS1K DN **46XX**, including the DID **501XXX1492** which is translated to **3111** for the purpose of Call Pilot voice mail access.



Dialing and Numbering Plans » Incoming Digit Translation » Customer 01 » Digit Conversion Tree 0 Configuration

Digit Conversion Tree 0 Configuration

Regular IDC tree
Send calling party DID disabled

	Incoming Digits ▲	Converted Digits	CPND Name	CPND language
1 ○	[redacted]	4685		
2 ○	[redacted]	4686		
3 ○	[redacted]	3110		
4 ○	501[redacted]1490	4685		
5 ○	501[redacted]1491	4689		
6 ○	501[redacted]1492	3111		

Copyright © 2002-2014 Avaya Inc. All rights reserved.

5.6.6. Administer Outbound Call - Special Number

Special Number is configured to be used for this testing. For example, **0** to reach service provider operator, **0+10** digits to reach service provider operator assistance, **011** prefix for international call, **1** for national long distance call, **411** for directory assistance and so on.

To create a Special Number, select **Dialing and Numbering Plans → Electronic Switched Network** from the left pane to display the **Electronic Switched Network** (**ESN**) screen (not shown). Then select **Special Number** (**SPN**) (not shown).

Enter the SPN value and then click on the "**to Add**" button (not shown). The screenshot below shows all the Special Numbers used for this testing.

Special Number: **0**

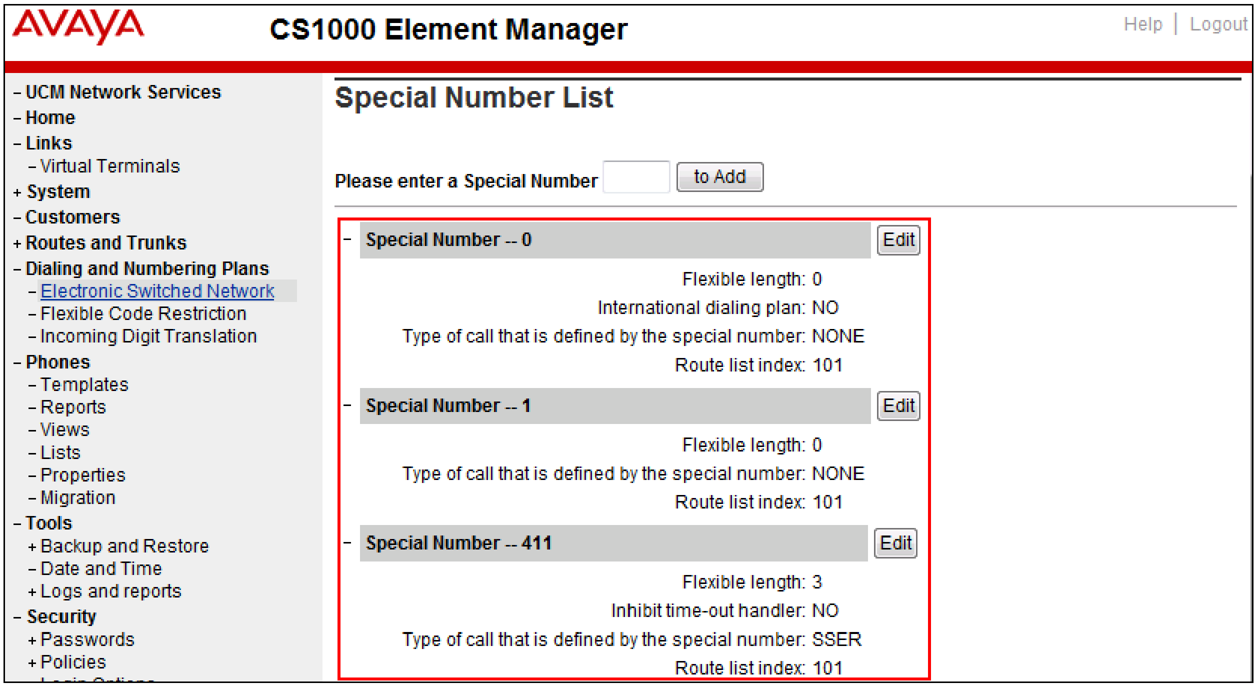
- **Flexible length**: 0 (flexible, unlimited and accept the character # to ending dial number).
- **Type of call that is defined by the special number**: NONE.
- **Route list index**: **101**, created in **Section 5.6.4**.

Special Number: **1**

- **Flexible length**: 0 (flexible, unlimited and accept the character # to ending dial number).
- **Type of call that is defined by the special number**: NONE.
- **Route list index**: **101**, created in **Section 5.6.4**.

Special Number: **411**

- **Flexible length**: 3.
- **Type of call that is defined by the special number**: SSER.
- **Route list index**: **101**, created in **Section 5.6.4**.



Special Number List

Please enter a Special Number

- Special Number -- 0

Flexible length: 0
International dialing plan: NO
Type of call that is defined by the special number: NONE
Route list index: 101

- Special Number -- 1

Flexible length: 0
Type of call that is defined by the special number: NONE
Route list index: 101

- Special Number -- 411

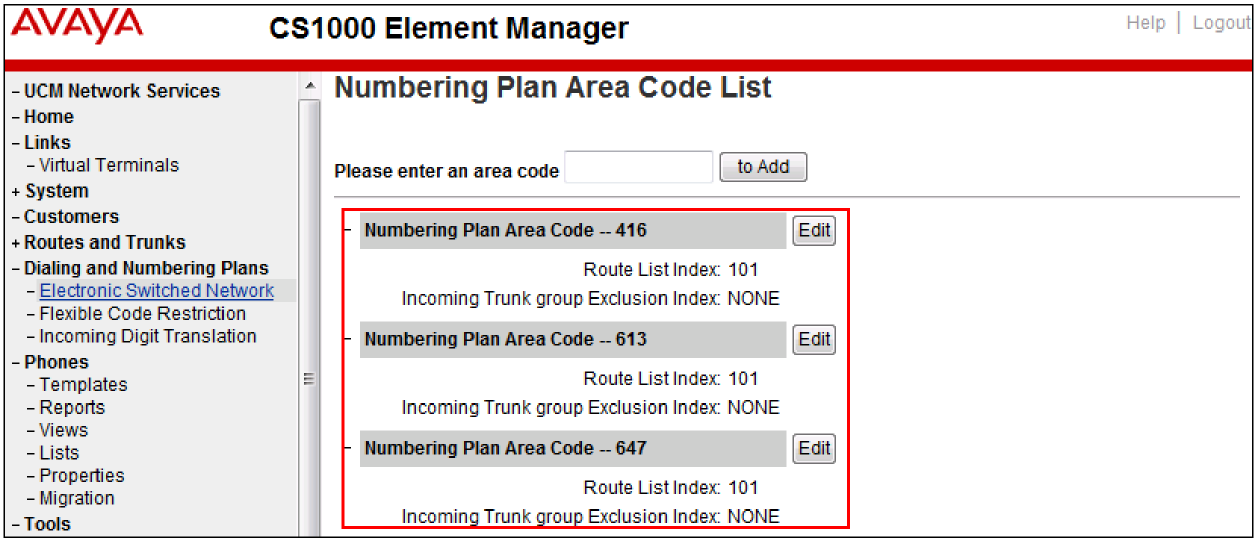
Flexible length: 3
Inhibit time-out handler: NO
Type of call that is defined by the special number: SSER
Route list index: 101

5.6.7. Administer Outbound Call - Numbering Plan Area (NPA)

This section describes the creation of NPA numbers used in this testing configuration.

To create a NPA number, select **Dialing and Numbering Plans → Electronic Switched Network** from the left pane to display the **Electronic Switched Network** (**ESN**) screen (not shown). Select **Numbering Plan Area Code** (**NPA**) (not shown).

Enter area code desired in the textbox and click "**to Add**" button (not shown). The screenshot below shows NPA numbers **416**, **613**, and **647** were configured for this testing. These NPA numbers are associated to the SIP Trunk for 10-digit outgoing local calls.



Numbering Plan Area Code List

Please enter an area code

Numbering Plan Area Code -- 416

Route List Index: 101

Incoming Trunk group Exclusion Index: NONE

Numbering Plan Area Code -- 613

Route List Index: 101

Incoming Trunk group Exclusion Index: NONE

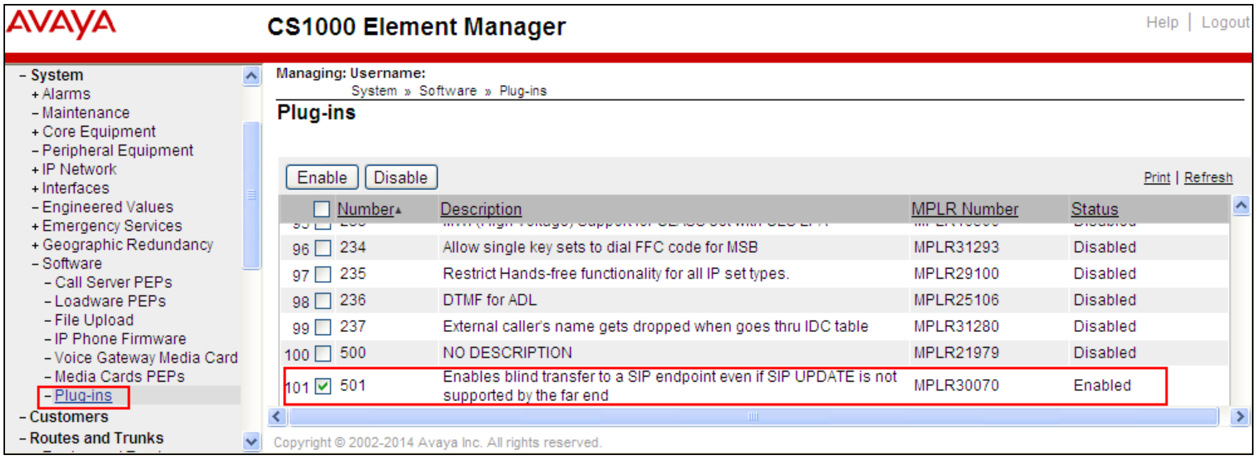
Numbering Plan Area Code -- 647

Route List Index: 101

Incoming Trunk group Exclusion Index: NONE

5.7. Administer Plug-ins

To enable the 501 plug-in, in the EM navigate to **System → Software → Plug-ins**. There is a list of plug-ins displayed in the right hand side. Scroll down to the 501 plug-in, check the check box of the 501 plug-in and click on the **Enable** button to enable the 501 plug-in.



Managing: Username:
System » Software » Plug-ins

Plug-ins

	☐	Number▲	Description	MPLR Number	Status
96	☐	234	Allow single key sets to dial FFC code for MSB	MPLR31293	Disabled
97	☐	235	Restrict Hands-free functionality for all IP set types.	MPLR29100	Disabled
98	☐	236	DTMF for ADL	MPLR25106	Disabled
99	☐	237	External caller's name gets dropped when goes thru IDC table	MPLR31280	Disabled
100	☐	500	NO DESCRIPTION	MPLR21979	Disabled
101	☑	501	Enables blind transfer to a SIP endpoint even if SIP UPDATE is not supported by the far end	MPLR30070	Enabled

6. Configure Avaya Session Border Controller for Enterprise

This section covers the configuration of the Avaya SBCE. It is assumed that the software has already been installed. For additional information on these configuration tasks, see **References** Error! Reference source not found. in **Section 10**.

The compliance testing comprised the configuration for two major components, Trunk Server for service provider and Call Server for enterprise. Each component consists of a set of Global Profiles, Domain Policies and Device Specific Settings. The configuration is defined in the Avaya SBCE web user interface as described in the following sections.

Trunk Server configuration elements for service provider Windstream:

- Global Profiles:
    - URI Groups
    - Routing
    - Topology Hiding
    - Server Interworking
    - Signaling Manipulation
    - Server Configuration
- Domain Policies:
    - Application Rules
    - Media Rules
    - Signaling Rules
    - Endpoint Policy Group
    - Session Policy
- Device Specific Settings:
    - Network Management
    - Media Interface
    - Signaling Interface
    - End Point Flows → Server Flows
    - Session Flows

Call Server configuration elements for enterprise CS1000:

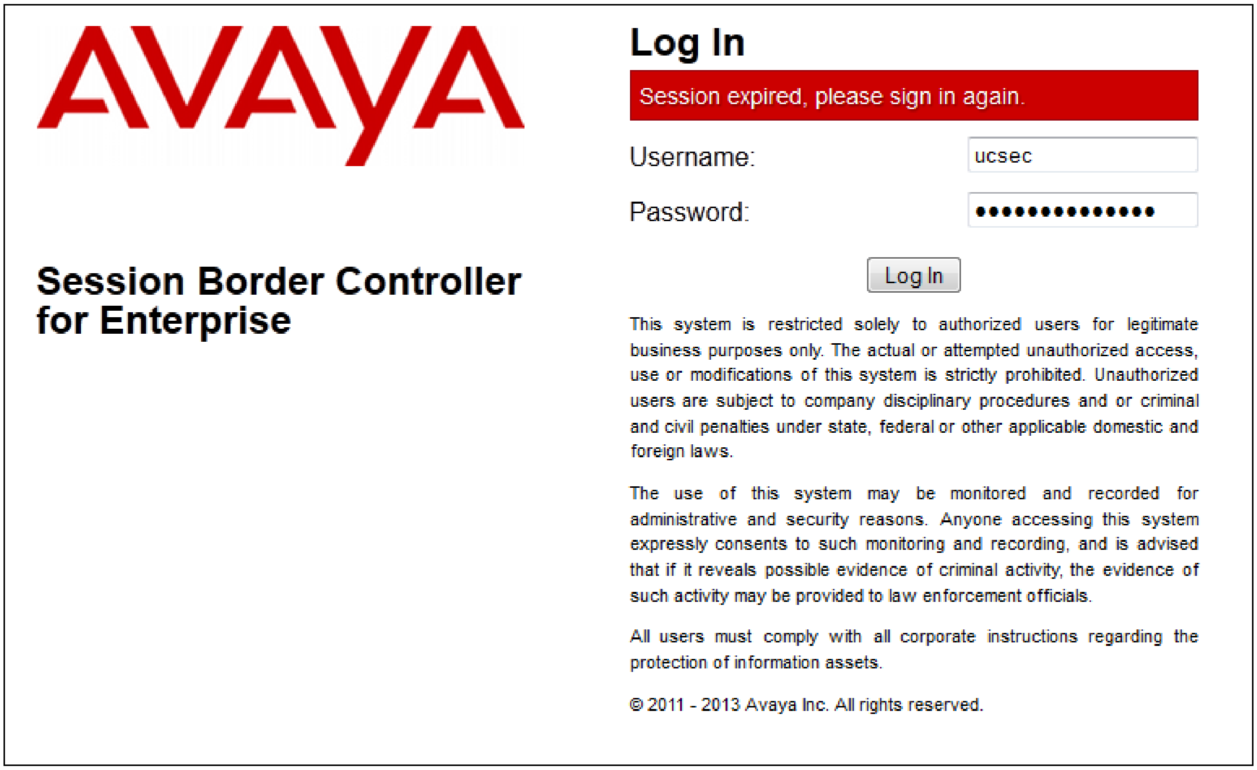
- Global Profiles:
    - URI Groups
    - Routing
    - Topology Hiding
    - Server Interworking
    - Server Configuration
- Domain Policies:
    - Application Rules
    - Media Rules
    - Signaling Rules
    - Endpoint Policy Group
    - Session Policy
- Device Specific Settings:

- Network Management
- Media Interface
- Signaling Interface
- End Point Flows → Server Flows
- Session Flows

6.1. Log into Avaya Session Border Controller for Enterprise

Use a web browser to access Avaya Session Border Controller for Enterprise (Avaya SBCE) web interface, enter https://<ip-addr>/sbc in the address field of the web browser, where <ip-addr> is the management LAN IP address of Avaya SBCE.

Enter the appropriate credentials then click **Log In**.



Session expired, please sign in again.

Username: ucsec

Password: ••••••••••••••

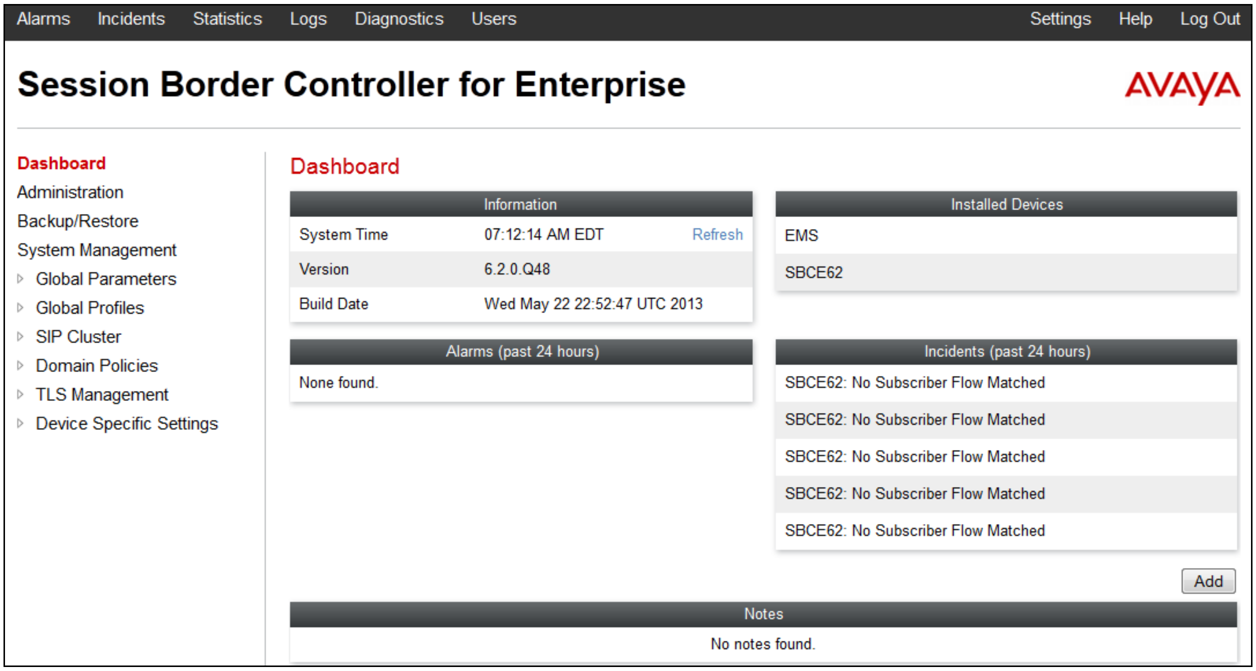
This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under 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.

© 2011 - 2013 Avaya Inc. All rights reserved.

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



Session Border Controller for Enterprise

Dashboard

Information		
System Time	07:12:14 AM EDT	Refresh
Version	6.2.0.Q48	
Build Date	Wed May 22 22:52:47 UTC 2013	

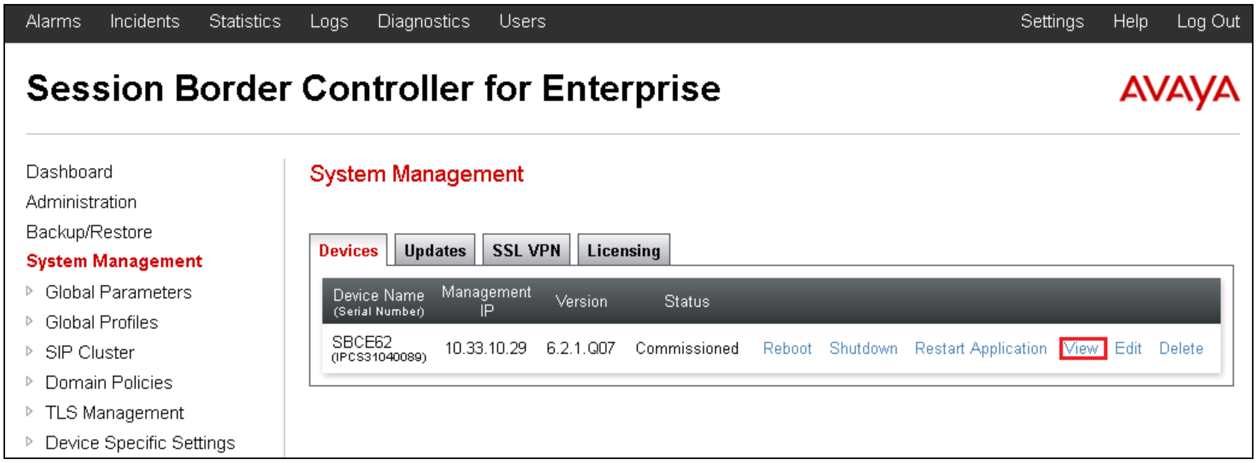
Installed Devices
EMS
SBCE62

Alarms (past 24 hours)
None found.

Incidents (past 24 hours)
SBCE62: No Subscriber Flow Matched
SBCE62: No Subscriber Flow Matched
SBCE62: No Subscriber Flow Matched
SBCE62: No Subscriber Flow Matched
SBCE62: No Subscriber Flow Matched

Notes
No notes found.

To view system information that has been configured during installation, navigate to **System Management** from the left menu pane. A list of installed devices is shown in the right pane. In the compliance test, a single device named **SBCE62** is added. To view the configuration of this device, click the **View** link as shown below.

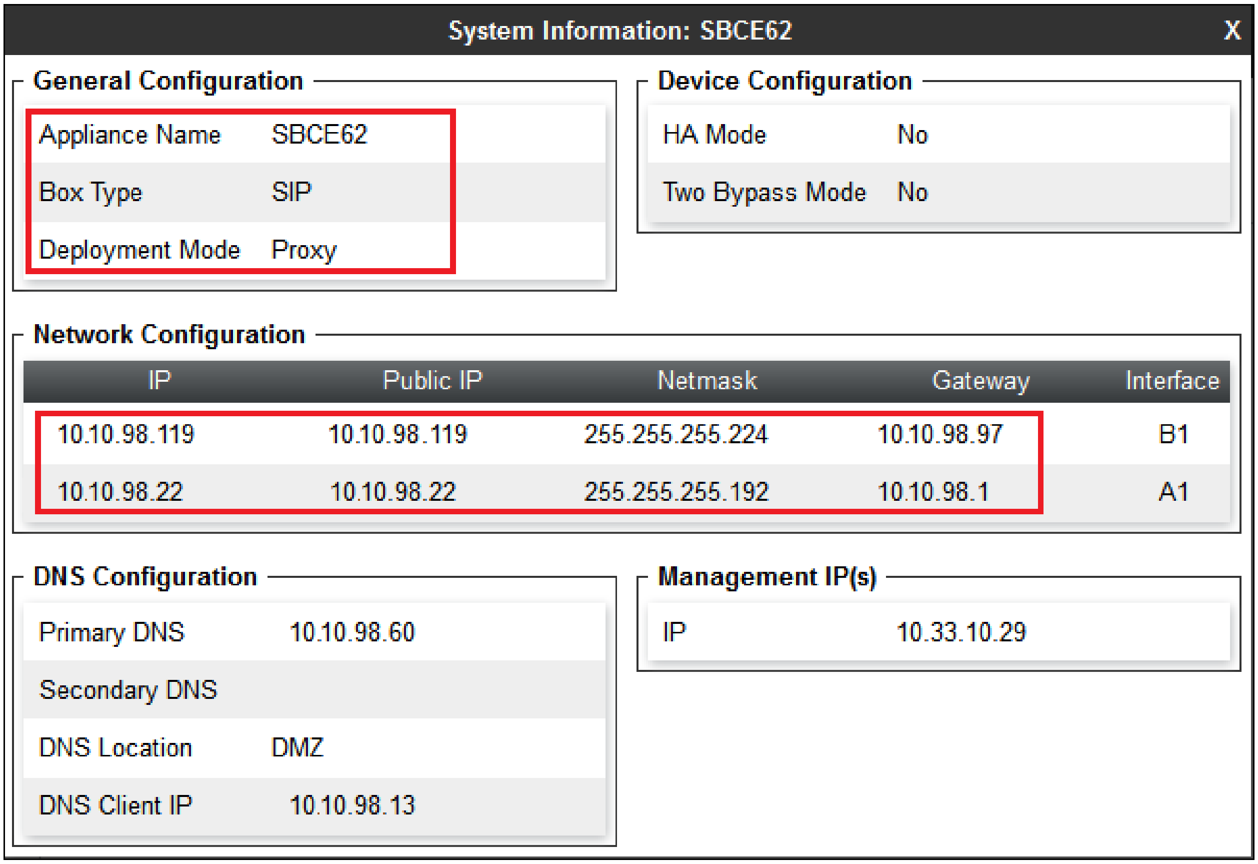


Session Border Controller for Enterprise

System Management

Device Name (Serial Number)	Management IP	Version	Status						
SBCE62 (IPCS31040089)	10.33.10.29	6.2.1.Q07	Commissioned	Reboot	Shutdown	Restart Application	View	Edit	Delete

The **System Information** screen shows **General Configuration**, **Device Configuration**, **Network Configuration, DNS Configuration** and **Management IP** information provided during installation and corresponds to **Figure 1**. The **Box Type** is set to **SIP** and the **Deployment Mode** is set to **Proxy**. Default values are used for all other fields.



General Configuration

Appliance Name	SBCE62
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

Network Configuration

IP	Public IP	Netmask	Gateway	Interface
10.10.98.119	10.10.98.119	255.255.255.224	10.10.98.97	B1
10.10.98.22	10.10.98.22	255.255.255.192	10.10.98.1	A1

DNS Configuration

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

Management IP(s)

IP	10.33.10.29

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 an URI Group, select **System Management → Global Profiles → URI Groups** and click on the **Add** button.

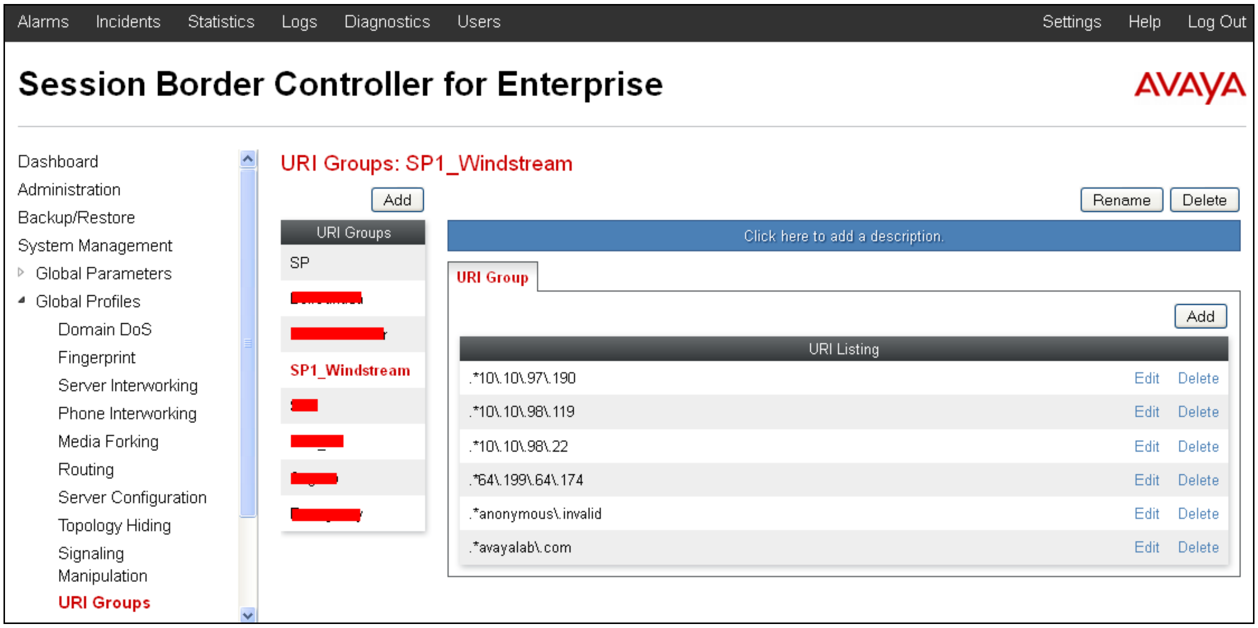
In the compliance testing, a URI Group named **SP1_Windstream** was added with the following URI type **Regular Expression**:

- "**.*10\.10\.98\.170**" – the signaling IP addresses of URI-Host in OPTIONS heartbeat originated by the SIP gateway.

- “**.*10\.10\.98\.119**” – the public IP address of Avaya SBCE.
- “**.*.10.\10.98\.22**” – the internal IP address of Avaya SBCE.
- “**.*64\.xxx\.xx\.174**” – the public proxy IP address of the service provider.
- “**.*anonymous\.invalid**” – the anonymous domain for the private call.
- “**.*avayalab\.com**” – the enterprise SIP domain.

This URI-Group is used to match the “From” and “To” headers in a SIP call dialog received from both the CS1000 and Windstream. If there is a match, the Avaya SBCE will apply the appropriate Routing profile (see Section **6.2.2**) and Server Flow (see **Section 6.4.4**) to route incoming and outgoing calls to the right destination.

The screenshot below illustrates the URI listing for URI Group **SP1_Windstream**.



Session Border Controller for Enterprise

URI Groups: SP1_Windstream

URI Groups
SP
[redacted]
[redacted]
SP1_Windstream
[redacted]
[redacted]
[redacted]
[redacted]

URI Listing		
.*10\.10\.97\.190	Edit	Delete
.*10\.10\.98\.119	Edit	Delete
.*10\.10\.98\.22	Edit	Delete
.*64\.199\.64\.174	Edit	Delete
.*anonymous\.invalid	Edit	Delete
.*avayalab\.com	Edit	Delete

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.

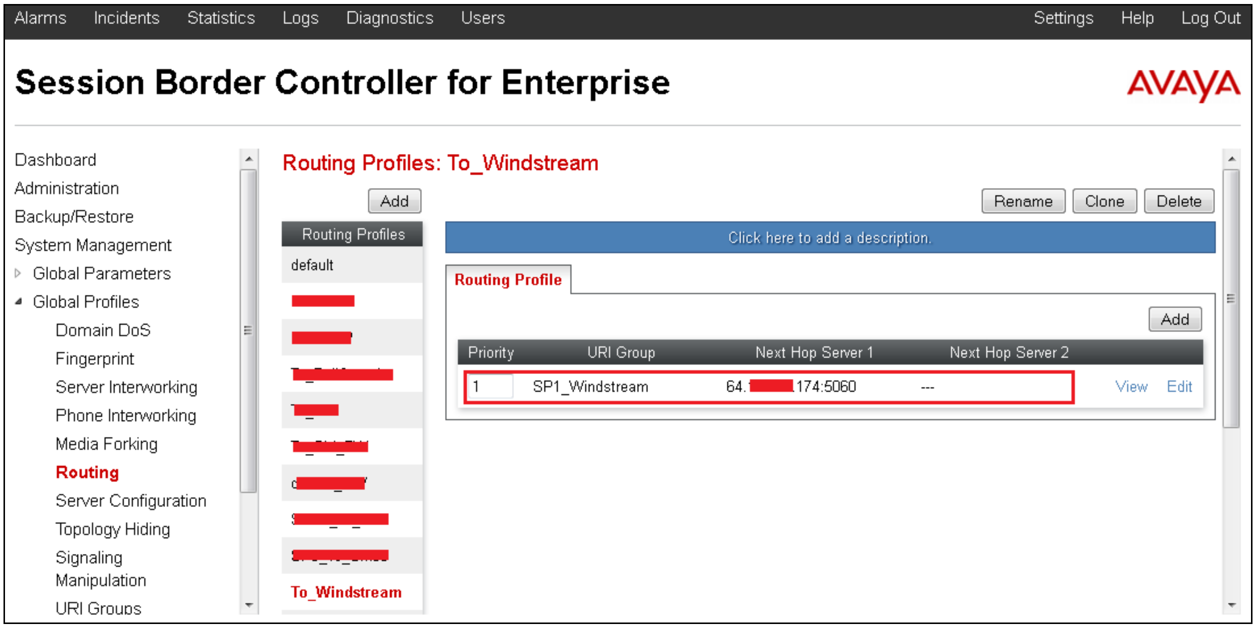
To create a Routing profile, select **System Management → Global Profiles → Routing** then click on the **Add** button.

In the compliance testing, a Routing profile **To_Windstream** was created to be used in conjunction with the Server Flow (see **Section 6.4.4**) defined for the CS1000. This entry is to route outgoing calls from the enterprise to Windstream.

In the opposite direction, a Routing profile **To_CAR276** was created to be used in conjunction with the Server Flow (see **Section 6.4.4**) defined for Windstream. This entry is to route incoming calls from Windstream to the enterprise.

6.2.2.1 Routing Profile for Windstream

The screenshot below illustrates the **System Management → Global Profiles → Routing**: **To_Windstream**. If there is a match between the SIP domain in the "To" header with the URI Group **SP1_Windstream** defined in **Section 6.2.1**, the call will be routed to the **Next Hop Server 1** which is the proxy IP address of Windstream Trunk Server on port **5060**.



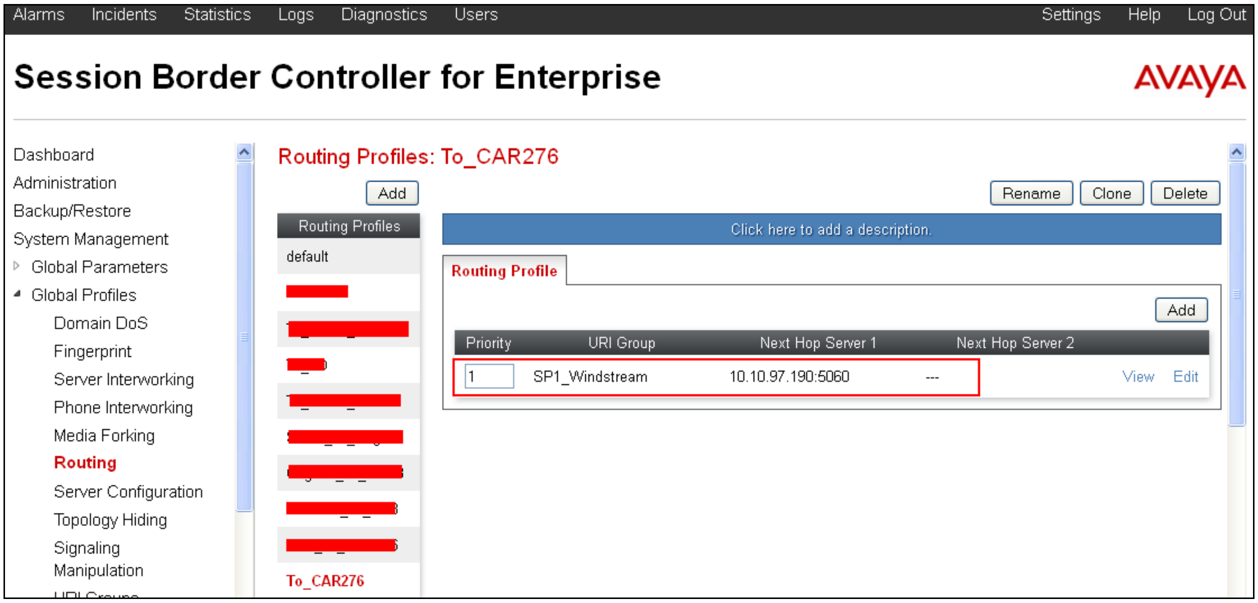
Routing Profiles: To_Windstream

Routing Profiles
default
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
To_Windstream

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	
1	SP1_Windstream	64.[redacted]174:5060	---	View Edit

6.2.2.2 Routing Profile for Avaya Communication Server 1000

The Routing Profile **To_CAR276** in the screenshot below was defined to route calls where the SIP domain in the "To" header matches the URI-Group **SP1_Windstream** defined in **Section 6.2.1**, to **Next Hop Server 1** which is the signaling IP address of CS1000 SIP gateway on port 5060.



Routing Profiles: To_CAR276

Routing Profiles
default
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
To_CAR276

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	
1	SP1_Windstream	10.10.97.190:5060	---	View Edit

6.2.3. Topology Hiding

Topology Hiding is a security feature of the Avaya SBCE 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 **System Management → Global Profiles → Topology Hiding** then click on the **Add**.

In the compliance testing, two Topology Hiding profiles were created: **Topo_Windstream** and **Topo_CAR276**.

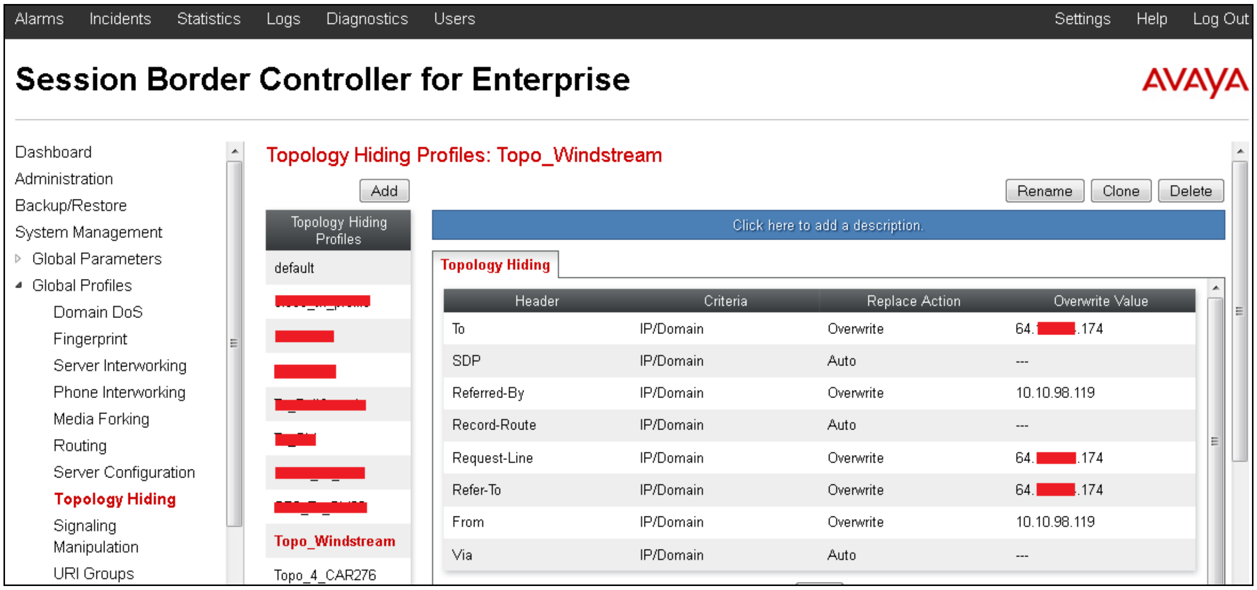
6.2.3.1 Topology Hiding Profile for Windstream

Topology Hiding profile **Topo_Windstream** was defined for outgoing calls to Windstream to:

- Mask URI-Host of the "Request-Line" and "To" headers with service provider public IP address **64.xxx.xx.174** to meet the requirements of Windstream.
- Change the "From" header added by the CS1000 with external IP address of Avaya SBCE known to Windstream.

This implementation is to secure the enterprise network topology and also to meet the SIP requirements from the service provider.

The screenshots below illustrate the Topology Hiding profile **Topo_Windstream**



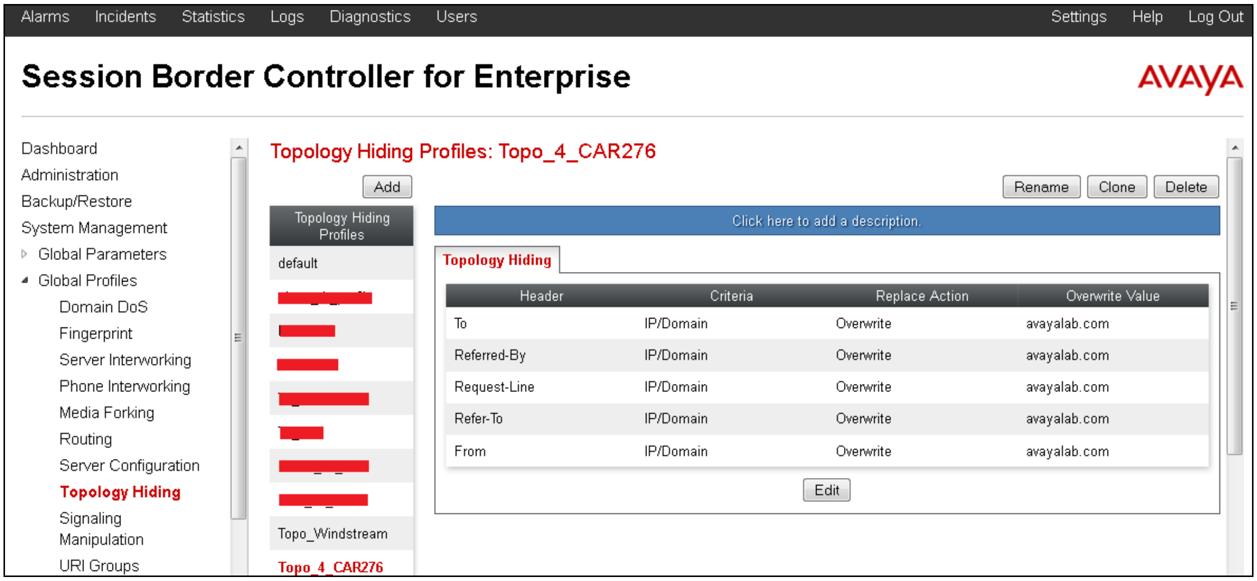
Header	Criteria	Replace Action	Overwrite Value
To	IP/Domain	Overwrite	64.[redacted].174
SDP	IP/Domain	Auto	---
Referred-By	IP/Domain	Overwrite	10.10.98.119
Record-Route	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	64.[redacted].174
Refer-To	IP/Domain	Overwrite	64.[redacted].174
From	IP/Domain	Overwrite	10.10.98.119
Via	IP/Domain	Auto	---

6.2.3.2 Topology Hiding Profile for the CS1000

Topology Hiding profile **Topo_COR76** was defined for incoming calls to the CS1000 to:

- Mask URI-Host of the “Request-Line”, “To”, “Refer-By”, “Refer-To” and “From” headers with the enterprise SIP domain **avayalab.com**.

The screenshots below illustrate the Topology Hiding profile **Topo_CAR276**.



Header	Criteria	Replace Action	Overwrite Value
To	IP/Domain	Overwrite	avayalab.com
Referred-By	IP/Domain	Overwrite	avayalab.com
Request-Line	IP/Domain	Overwrite	avayalab.com
Refer-To	IP/Domain	Overwrite	avayalab.com
From	IP/Domain	Overwrite	avayalab.com

Notes:

- The **Criteria** should be **IP/Domain** to allow the Avaya SBCE to mask both domain name and IP address presenting in the URI-Host.

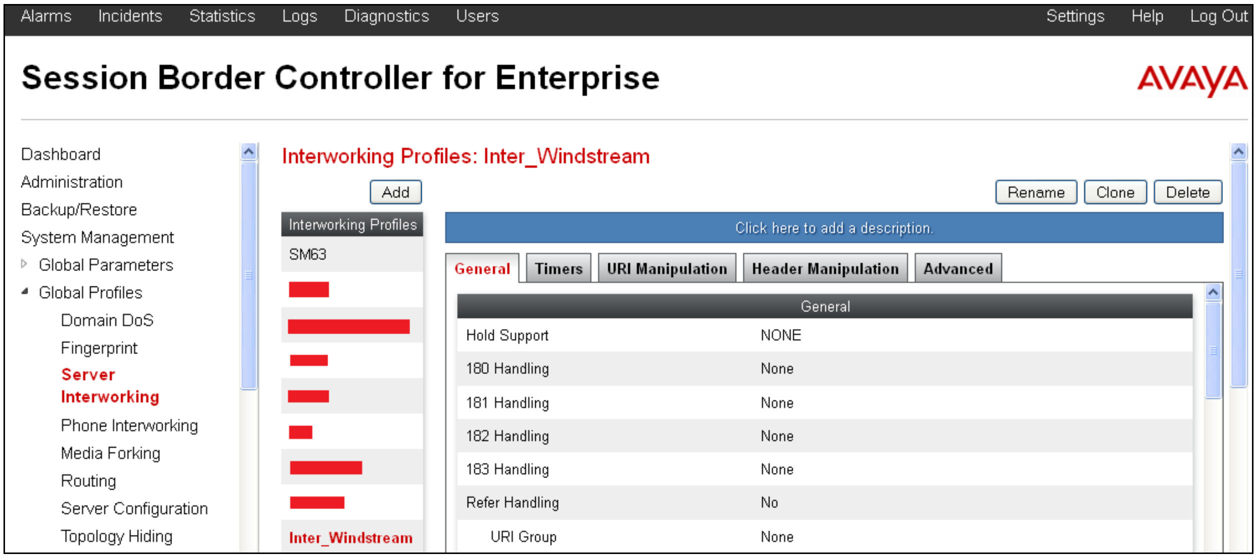
6.2.4. Server Interworking

Server Interworking profile features are configured differently for Call Server and Trunk Server. To create a Server Interworking profile, select **System Management → Global Profiles → Server Interworking** then click on the **Add** button.

In the compliance testing, two Server Interworking profiles **Inter_Windstream** and **Inter_CAR276** were created for Windstream (Trunk Server) and the CS1000 (Call Server).

6.2.4.1 Server Interworking Profile for Windstream

Server Interworking profile **Inter_Windstream** was defined to match the specification of Windstream. The **General** and **Advanced** tabs were configured with the following parameters while the other tabs **Timers, URI Manipulation** and **Header Manipulation** were kept as default.



Interworking Profiles: Inter_Windstream

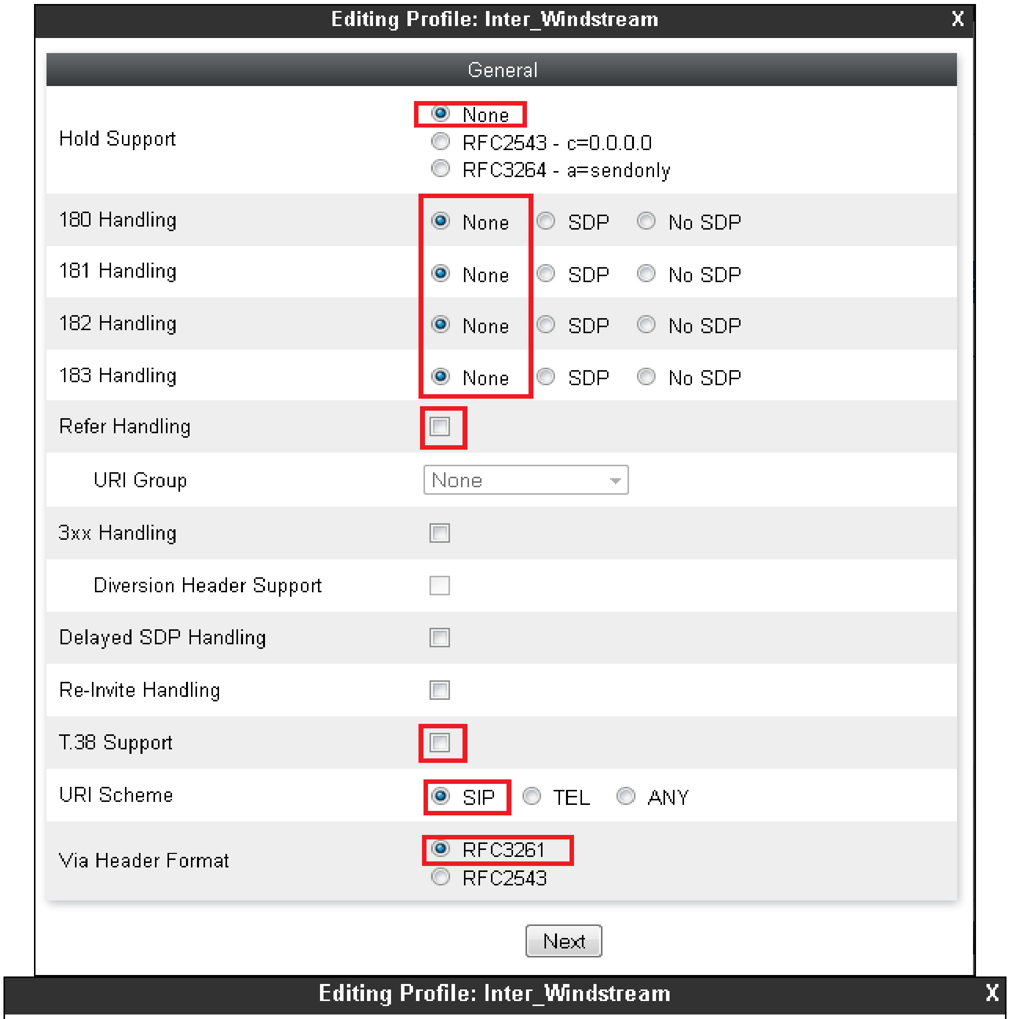
Interworking Profiles
SM63
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
Inter_Windstream

General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
URI Group	None

General settings:

- **Hold Support** = **None**. The Avaya SBCE will not handle Hold/ Resume signaling, it keeps the Hold/ Resume signaling unchanged to send to the destination server.
- **18X Handling** = **None**. The Avaya SBCE will not handle 18X, it keeps the incoming 18X response unchanged to send to the destination server.
- **Refer Handling** = **Unchecked**. The Avaya SBCE will not handle Refer, it keeps REFER unchanged to send to the destination server.
- **T.38 Support** = **Unchecked**. Windstream does not support the T.38 codec for fax over IP in the compliance testing.
- **UIR Scheme = SIP**.
- **Via Header Format = RFC3261**.
- **Privacy Enabled** = **Unchecked**. The Avaya SBCE will not mask the "From" header with **anonymous** to the destination server. It depends on the far end to enable/ disable the "Privacy" on individual call basis.
- **DTMF Support** = **None**. The Avaya SBCE will not modify the original DTMF transmission method sent by CS1000. It keeps the DTMF unchanged to send to the destination server.

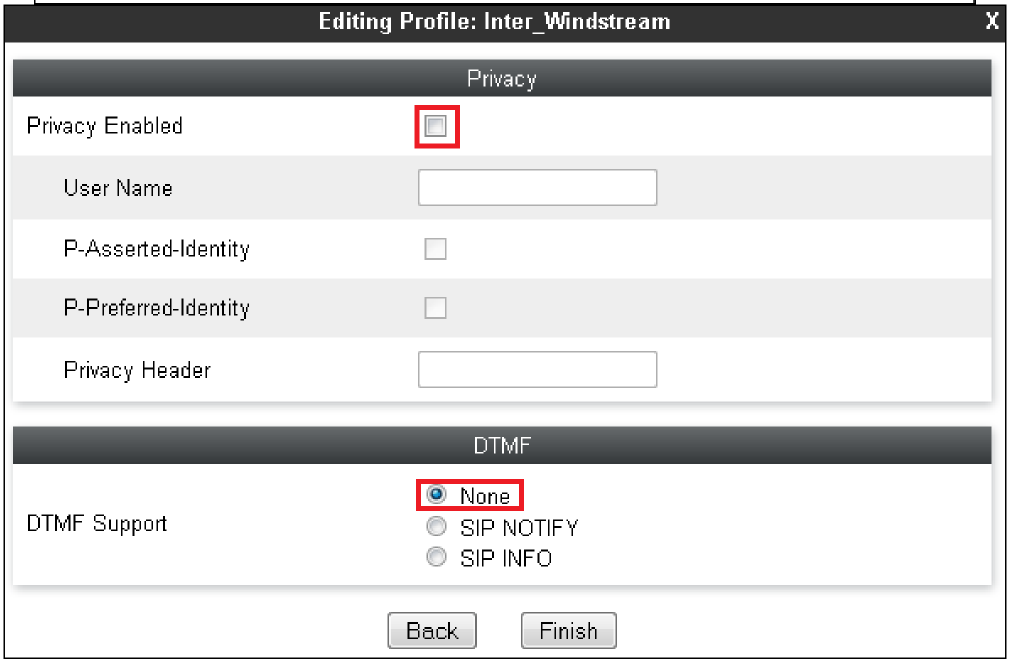
The screenshots below illustrate the Server Interworking profile **Inter_Windstream**.



Editing Profile: Inter_Windstream

General

Hold Support	● None ○ RFC2543 - c=0.0.0.0 ○ RFC3264 - a=sendonly
180 Handling	● None ○ SDP ○ No SDP
181 Handling	● None ○ SDP ○ No SDP
182 Handling	● None ○ SDP ○ No SDP
183 Handling	● None ○ SDP ○ No SDP
Refer Handling	□
URI Group	None
3xx Handling	□
Diversion Header Support	□
Delayed SDP Handling	□
Re-Invite Handling	□
T.38 Support	□
URI Scheme	● SIP ○ TEL ○ ANY
Via Header Format	● RFC3261 ○ RFC2543



Editing Profile: Inter_Windstream

Privacy

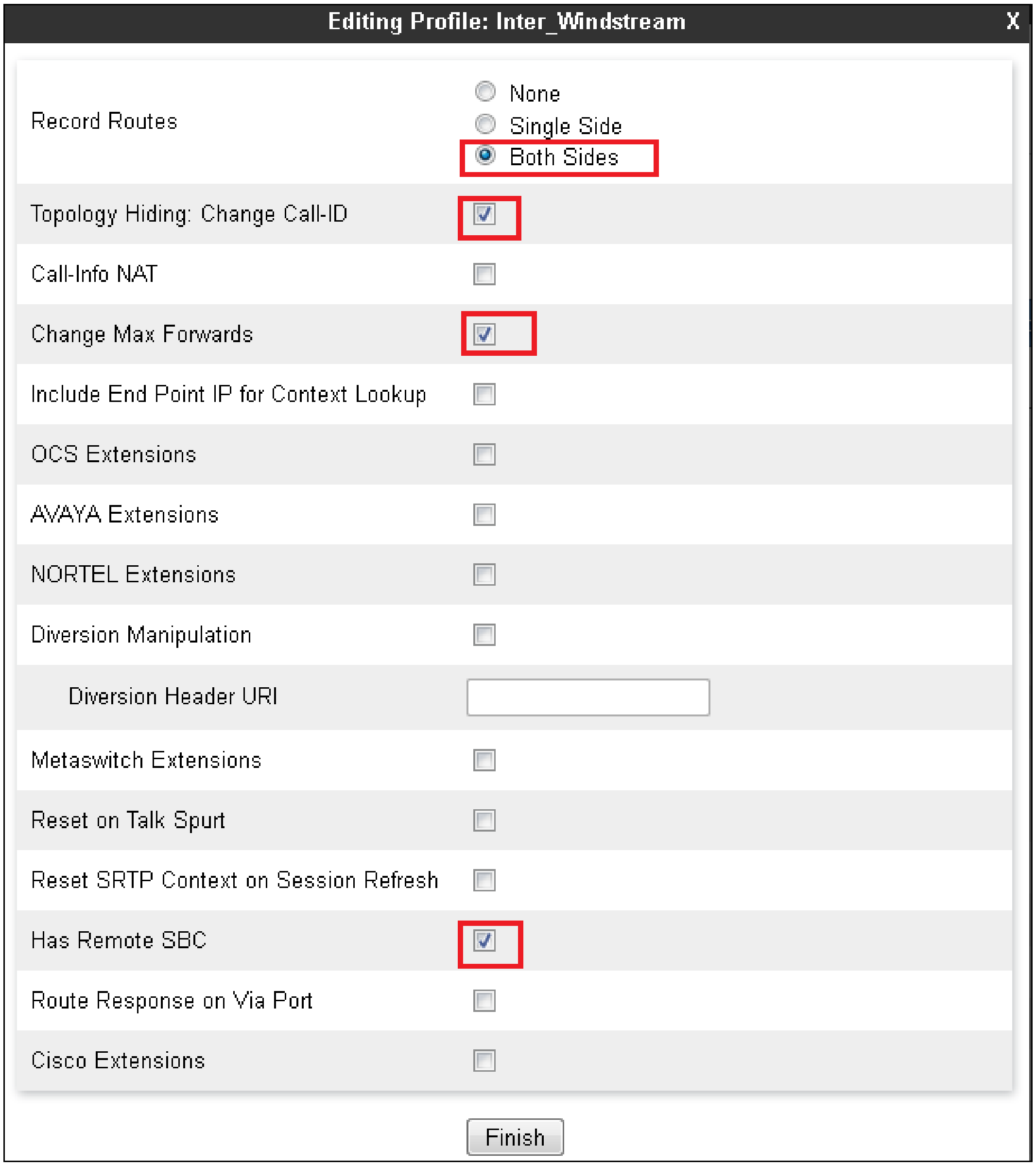
Privacy Enabled	□
User Name	
P-Asserted-Identity	□
P-Preferred-Identity	□
Privacy Header	

DTMF

DTMF Support	● None ○ SIP NOTIFY ○ SIP INFO

Advanced settings:

- **Record Routes** = **Both Sides**. The Avaya SBCE will send the "Record-Route" header to both the CS1000 and Windstream.
- **TopologyHiding**: **Change Call-ID** = **Checked**. The Avaya SBCE will mask the "Call-ID" header for the calls to the destination server.
- **Change MaxForwards** = **Checked**. The Avaya SBCE will reduce the counter of the "Max-Forwards" header by 1 for the calls to the destination server.
- **Has Remote SBC** = **Checked**. The Avaya SBCE will flexibly handle the changes to the SDP when the call is active.



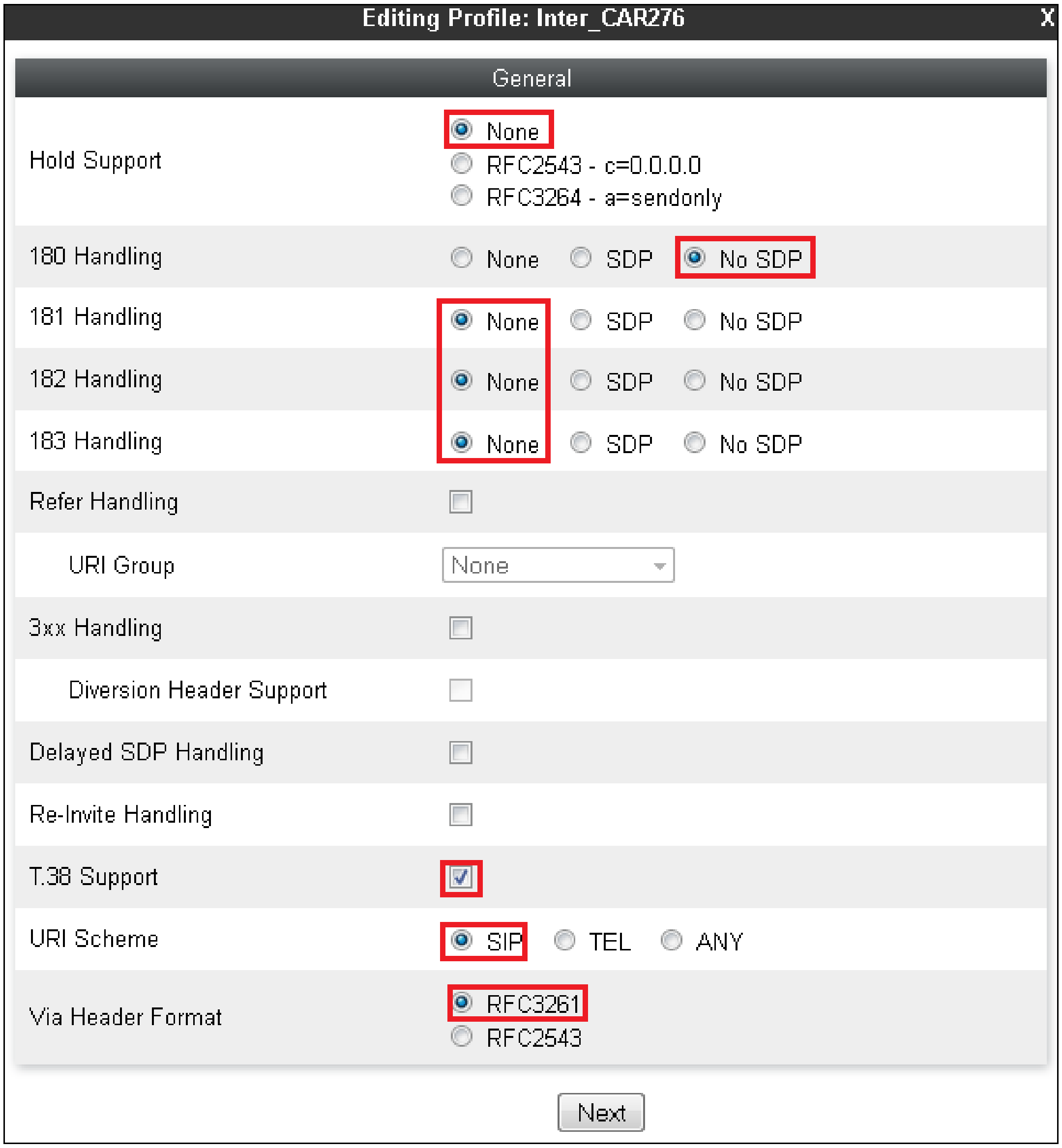
Editing Profile: Inter_Windstream

Record Routes	○ None ○ Single Side ● Both Sides
Topology Hiding: Change Call-ID	☑
Call-Info NAT	□
Change Max Forwards	☑
Include End Point IP for Context Lookup	□
OCS Extensions	□
AVAYA Extensions	□
NORTEL Extensions	□
Diversion Manipulation	□
Diversion Header URI	
Metaswitch Extensions	□
Reset on Talk Spurt	□
Reset SRTP Context on Session Refresh	□
Has Remote SBC	☑
Route Response on Via Port	□
Cisco Extensions	□

6.2.4.2 Server Interworking Profile for the CS1000

Server Interworking profile **Inter_CAR276** was similarly defined to match the specification of the CS1000. The “180 Handling” field must set to “No SDP” to fix the off-net blind transfer issue. See **Section 2.2**.

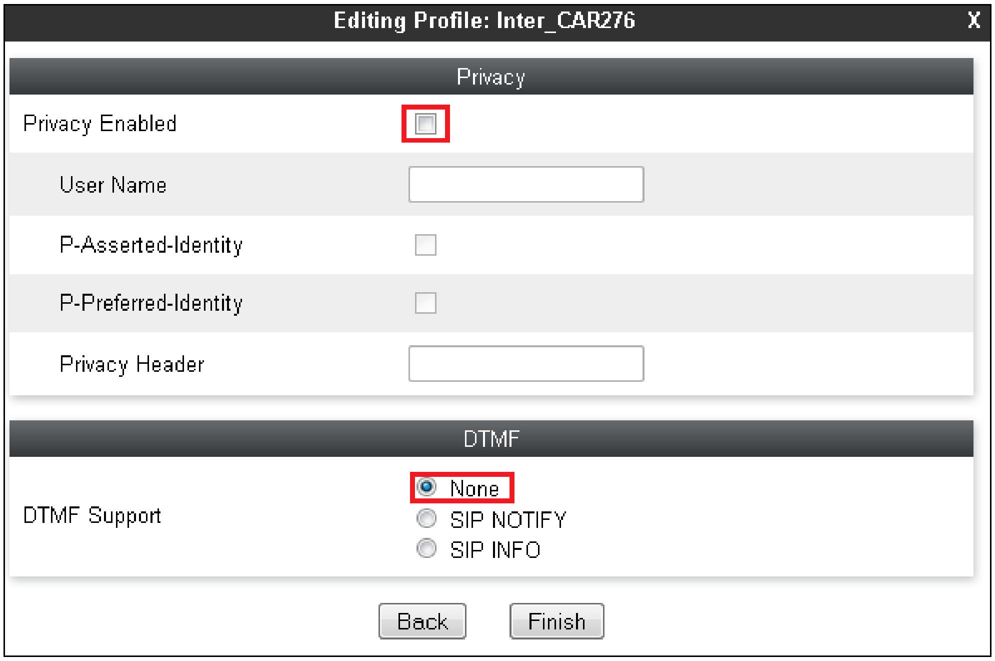
The screenshots below illustrate the Server Interworking profile **Inter_CAR276**.



Editing Profile: Inter_CAR276

General

Hold Support	● None ○ RFC2543 - c=0.0.0.0 ○ RFC3264 - a=sendonly
180 Handling	○ None ○ SDP ● No SDP
181 Handling	● None ○ SDP ○ No SDP
182 Handling	● None ○ SDP ○ No SDP
183 Handling	● None ○ SDP ○ No SDP
Refer Handling	□
URI Group	None
3xx Handling	□
Diversion Header Support	□
Delayed SDP Handling	□
Re-Invite Handling	□
T.38 Support	☑
URI Scheme	● SIP ○ TEL ○ ANY
Via Header Format	● RFC3261 ○ RFC2543



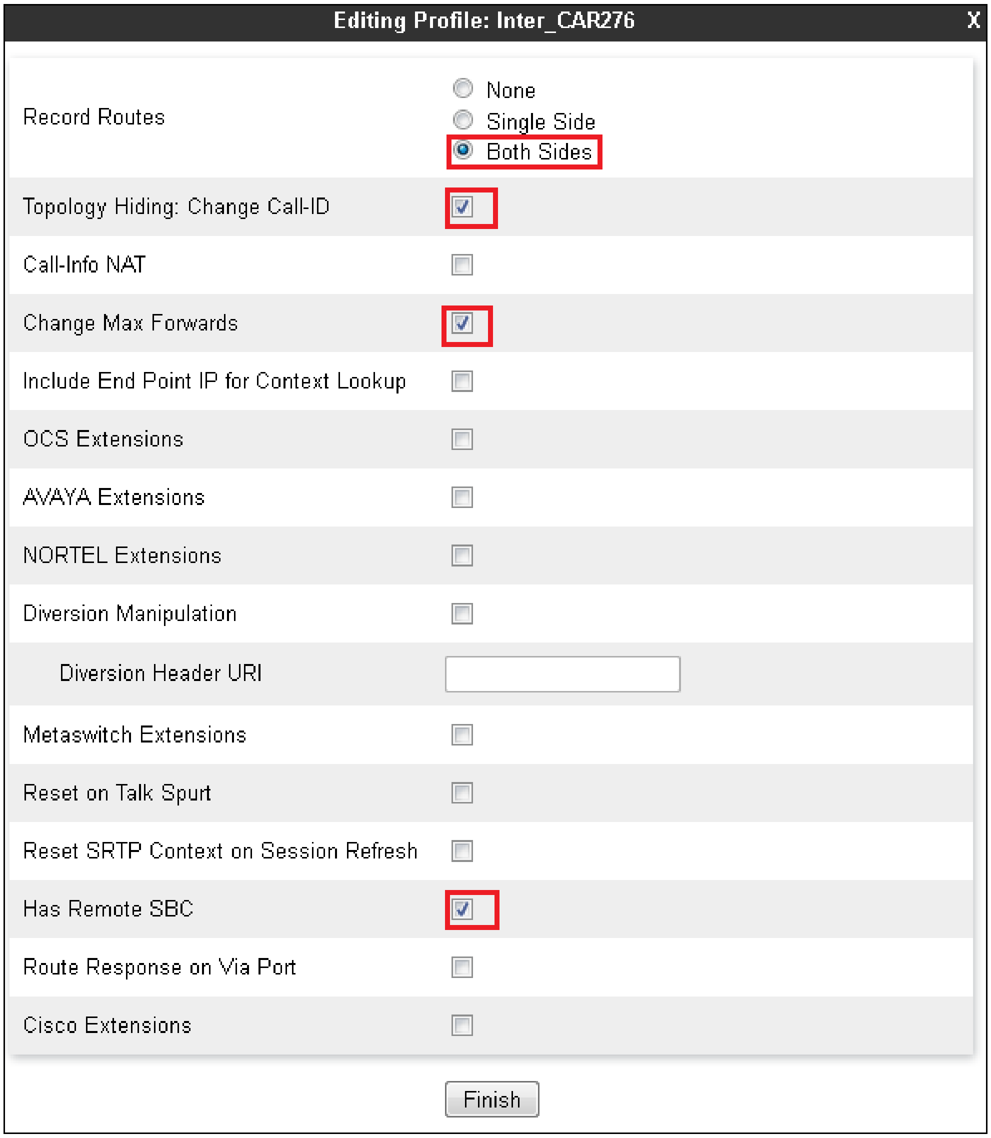
Editing Profile: Inter_CAR276

Privacy

Privacy Enabled	□
User Name	
P-Asserted-Identity	□
P-Preferred-Identity	□
Privacy Header	

DTMF

DTMF Support	● None ○ SIP NOTIFY ○ SIP INFO



Editing Profile: Inter_CAR276

Record Routes	○ None ○ Single Side ● Both Sides
Topology Hiding: Change Call-ID	☑
Call-Info NAT	□
Change Max Forwards	☑
Include End Point IP for Context Lookup	□
OCS Extensions	□
AVAYA Extensions	□
NORTEL Extensions	□
Diversion Manipulation	□
Diversion Header URI	
Metaswitch Extensions	□
Reset on Talk Spurt	□
Reset SRTP Context on Session Refresh	□
Has Remote SBC	☑
Route Response on Via Port	□
Cisco Extensions	□

6.2.5. Signaling Manipulation

The Signaling Manipulation feature allows the ability to add, change and delete any of the headers in a SIP message. This feature provides the ability to configure a manipulation in a highly flexible manner using a proprietary scripting language called SigMa.

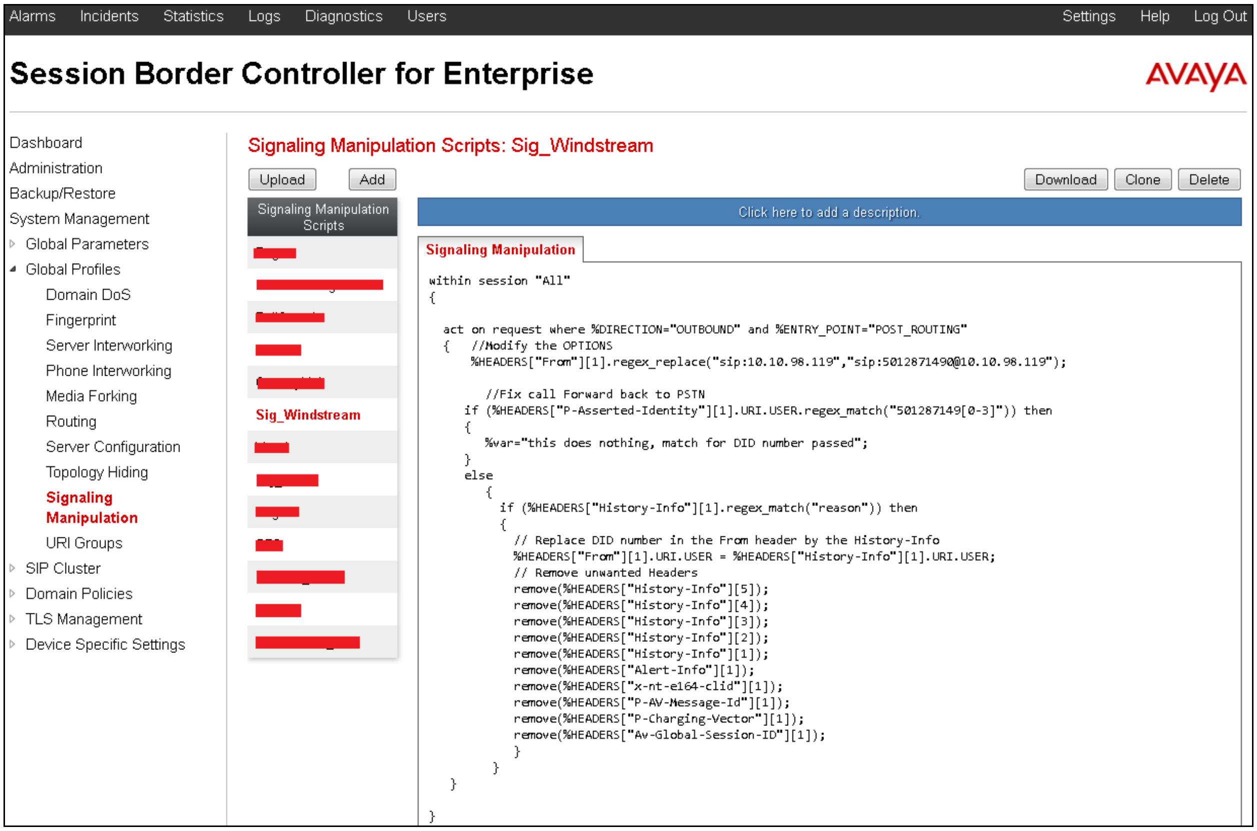
The SigMa scripting language is designed to express any of the SIP header manipulations done by the Avaya SBCE. Using this language, a script can be written and tied to a given Server Configuration (see **Section 0**) through the Avaya SBCE web interface. The Avaya SBCE appliance then interprets this script at the given entry point or "hook point".

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

6.2.5.1 Signaling Manipulation for Windstream

To create a Signaling Manipulation script, select **System Management → Global Profiles → Signaling Manipulation** then click on the **Add** button.

In the compliance testing, a SigMa script named **Sig_Windstream** was created for Server Configuration for Windstream and described in detail below.



```
within session "All"
{

  act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {   //Modify the OPTIONS
      %HEADERS["From"][1].regex_replace("sip:10.10.98.119","sip:5012871490@10.10.98.119");

        //Fix call Forward back to PSTN
     if (%HEADERS["P-Asserted-Identity"][1].URI.USER.regex_match("501287149[0-3]")) then
     {
        %var="this does nothing, match for DID number passed";
     }
     else
        {
          if (%HEADERS["History-Info"][1].regex_match("reason")) then
          {
            // Replace DID number in the From header by the History-Info
            %HEADERS["From"][1].URI.USER = %HEADERS["History-Info"][1].URI.USER;
            // Remove unwanted Headers
            remove(%HEADERS["History-Info"][5]);
            remove(%HEADERS["History-Info"][4]);
            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-Charging-Vector"][1]);
            remove(%HEADERS["Av-Global-Session-ID"][1]);
            }
         }
   }

}
```

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 outbound calls to Windstream. The manipulation will be done on the header of the OPTION message to change from sip:10.10.98.119 to sip:501xxx1490@10.10.98.119 which has DID 501xxx1490 known by Windstream.

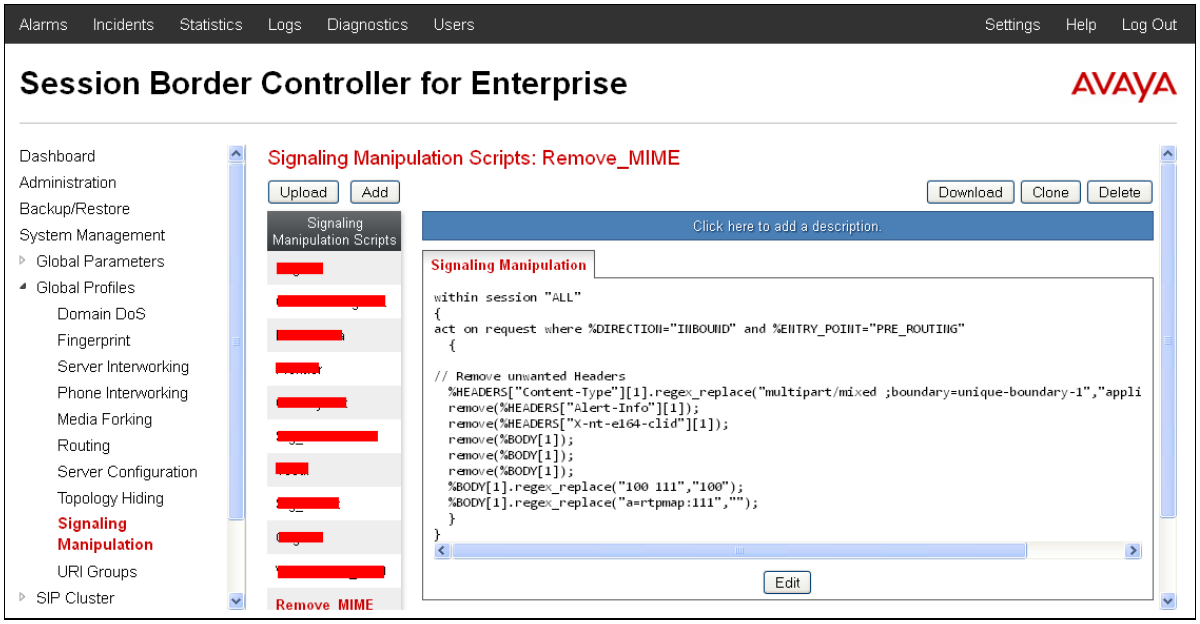
```
act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
{
 //Modify the OPTIONS
%HEADERS["From"][1].regex_replace("sip:10.10.98.119","sip:501xxx1490@10.10.98.119");
```

The script below is to fix the call forward: first call originated from PSTN and the second call forward back from the enterprise to PSTN, and to remove unwanted headers in the call forward for the way from the CS1000 to Windstream.

```
//Fix call Forward back to PSTN
     if (%HEADERS["P-Asserted-Identity"][1].URI.USER.regex_match("501287149[0-3]"))
then
     {
        %var="this does nothing, match for DID number passed";
     }
     else
        {
          if (%HEADERS["History-Info"][1].regex_match("reason")) then
          {
            // Replace DID number in the From header by the History-Info
            %HEADERS["From"][1].URI.USER = %HEADERS["History-Info"][1].URI.USER;
            // Remove unwanted Headers
            remove(%HEADERS["History-Info"][5]);
            remove(%HEADERS["History-Info"][4]);
            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-Charging-Vector"][1]);
            remove(%HEADERS["Av-Global-Session-ID"][1]);
            }
```

6.2.5.2 Signaling Manipulation for Avaya CS1000

In the compliance testing, a SigMa script named **Remove_MIME** was created for the Server Configuration for Avaya CS1000 and described in detail below.



```
within session "ALL"
{
act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
  {

// Remove unwanted Headers
  %HEADERS["Content-Type"][1].regex_replace("multipart/mixed ;boundary=unique-boundary-1","appli
  remove(%HEADERS["Alert-Info"][1]);
  remove(%HEADERS["X-nt-e164-clid"][1]);
  remove(%BODY[1]);
  remove(%BODY[1]);
  remove(%BODY[1]);
  %BODY[1].regex_replace("100 111","100");
  %BODY[1].regex_replace("a=rtpmap:111","");
  }
}
```

The statement **“act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"”** is to specify the script will take effect on all type of SIP messages for inbound calls from Avaya CS1000 to Avaya SBCE. The manipulation will be done on the Content-Type header.

```
within session "ALL"
{
act on request where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
  {

// Remove unwanted Headers
  %HEADERS["Content-Type"][1].regex_replace("multipart/mixed
;boundary=unique-boundary-1","application/sdp");
  remove(%HEADERS["Alert-Info"][1]);
  remove(%HEADERS["X-nt-e164-clid"][1]);
  remove(%BODY[1]);
  remove(%BODY[1]);
  remove(%BODY[1]);
  %BODY[1].regex_replace("100 111","100");
  %BODY[1].regex_replace("a=rtpmap:111","");
  }
}
```

6.2.6. Server Configuration

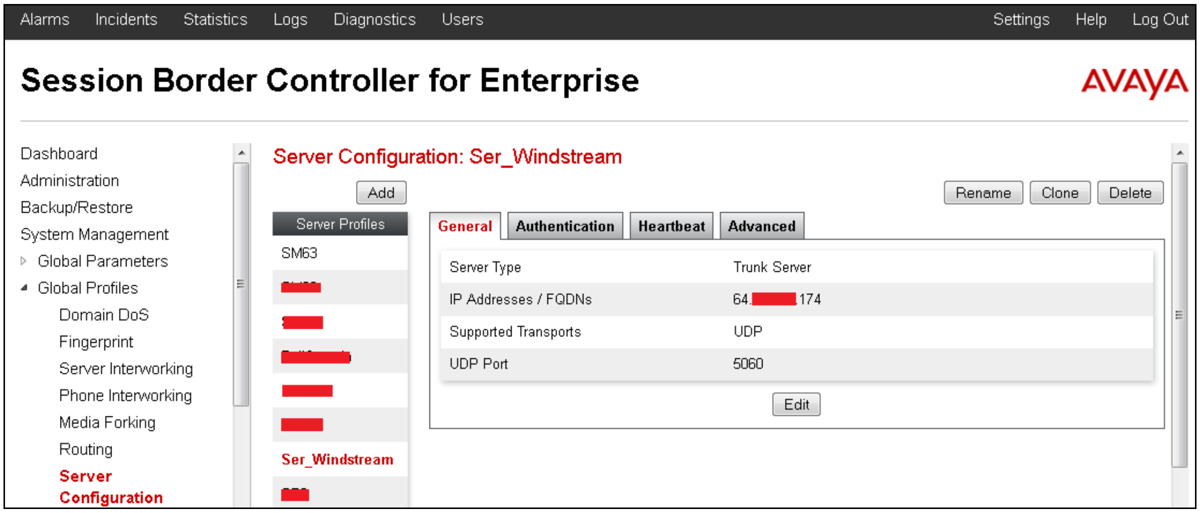
The Server Configuration screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. These tabs are used to configure and manage various SIP Call Server specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics and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

To create a Server Configuration entry, select **System Management → Global Profiles →Server Configuration** then click on the **Add** button.

In the compliance testing, two separate Server Configurations were created, server entry **Ser_Windstream** for Windstream and server entry **CAR276** for Avaya CS1000.

6.2.6.1 Server Configuration for Windstream

The Server Configuration **Ser_Windstream** was added for Windstream, it is discussed in detail below. The **General** and **Advanced** tabs were provisioned. The **Heartbeat** tab is kept as disabled (the default value) to allow Avaya SBCE to forward OPTIONS message from Avaya CS1000 to Windstream. The screen below shows the server configuration for Windstream.

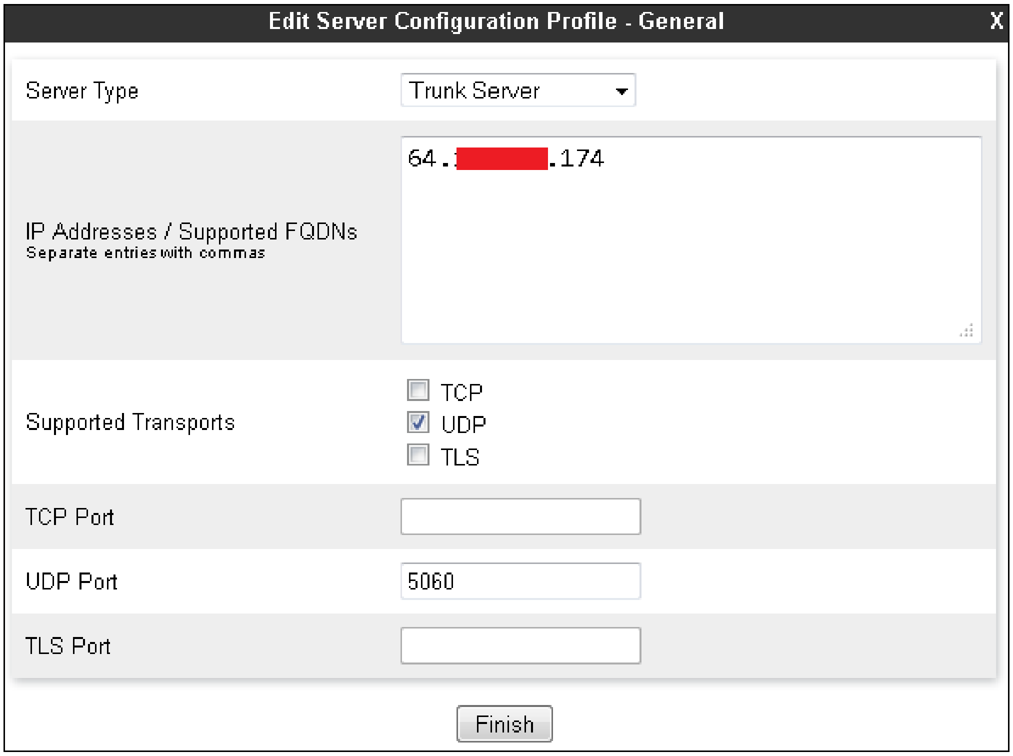


Server Configuration: Ser_Windstream

Server Profiles: SM63, [redacted], [redacted], [redacted], [redacted], [redacted], Ser_Windstream, [redacted]

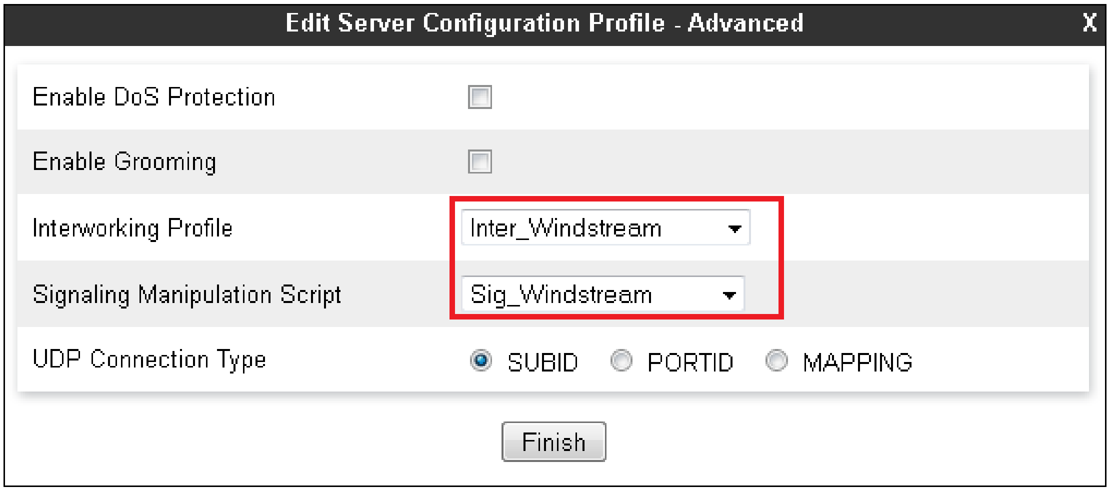
Server Type	Trunk Server
IP Addresses / FQDNs	64.[redacted].174
Supported Transports	UDP
UDP Port	5060

In the **General** tab, specify Server Type for Windstream as a **Trunk Server**. The IP connectivity has also been defined as shown in the screenshot below. In this compliance testing, Windstream supported transport protocol **UDP** and listens on port **5060**.



Server Type	Trunk Server
IP Addresses / Supported FQDNs Separate entries with commas	64.[redacted].174
Supported Transports	□ TCP ☑ UDP □ TLS
TCP Port	
UDP Port	5060
TLS Port	

Under the **Advanced** tab, for **Interworking Profile** drop down list, select **Inter_Windstream** as defined in **Section 6.2.4.1** and for **Signaling Manipulation Script** drop down list, select **Sig_Windstream** as defined in **Section 6.2.5**. These configurations are applied to the specific SIP profile and SigMa rules for the traffic from and to Windstream. The other settings are kept as default. Click **Finish** button to save and close the window.

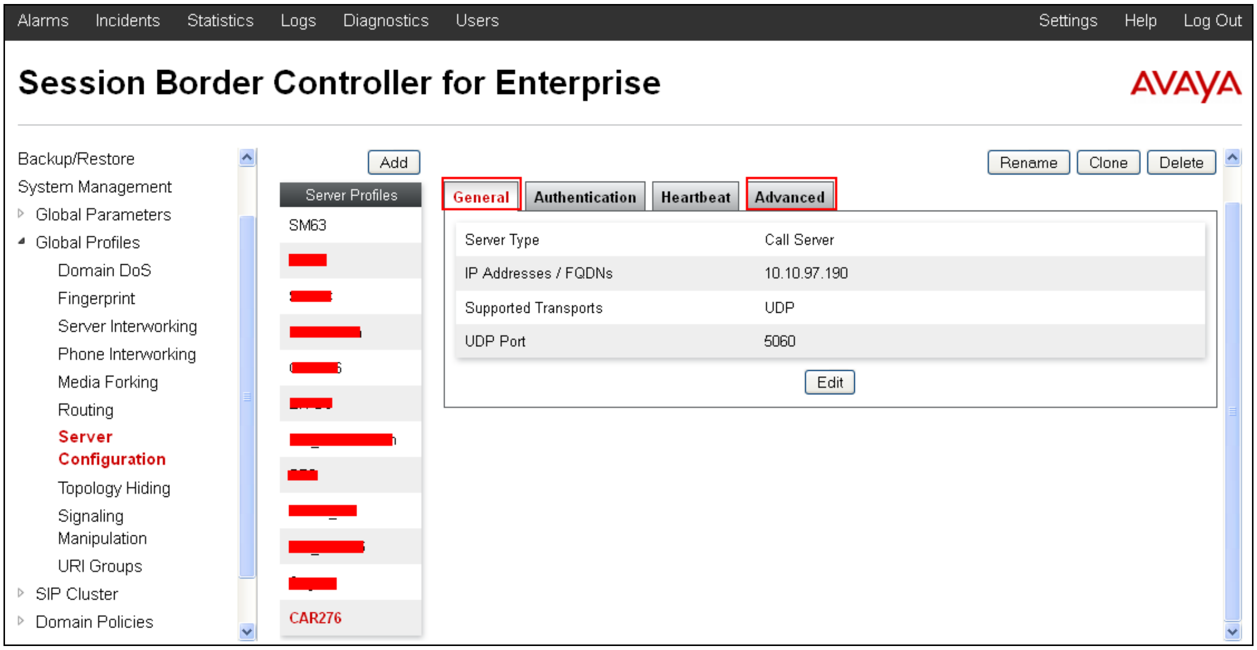


Edit Server Configuration Profile - Advanced

Enable DoS Protection	□
Enable Grooming	□
Interworking Profile	Inter_Windstream
Signaling Manipulation Script	Sig_Windstream
UDP Connection Type	● SUBID ○ PORTID ○ MAPPING

6.2.6.2 Server Configuration for Avaya CS1000

The Server Configuration **CAR276** was added for the CS1000, it is discussed in detail below. Only the **General** and **Advanced** tabs required provisioning. The **Heartbeat** tab is kept as disabled (the default value) to allow the Avaya SBCE to forward the OPTIONS heartbeat from Windstream to Avaya CS1000 to query for the status of the SIP Trunk.

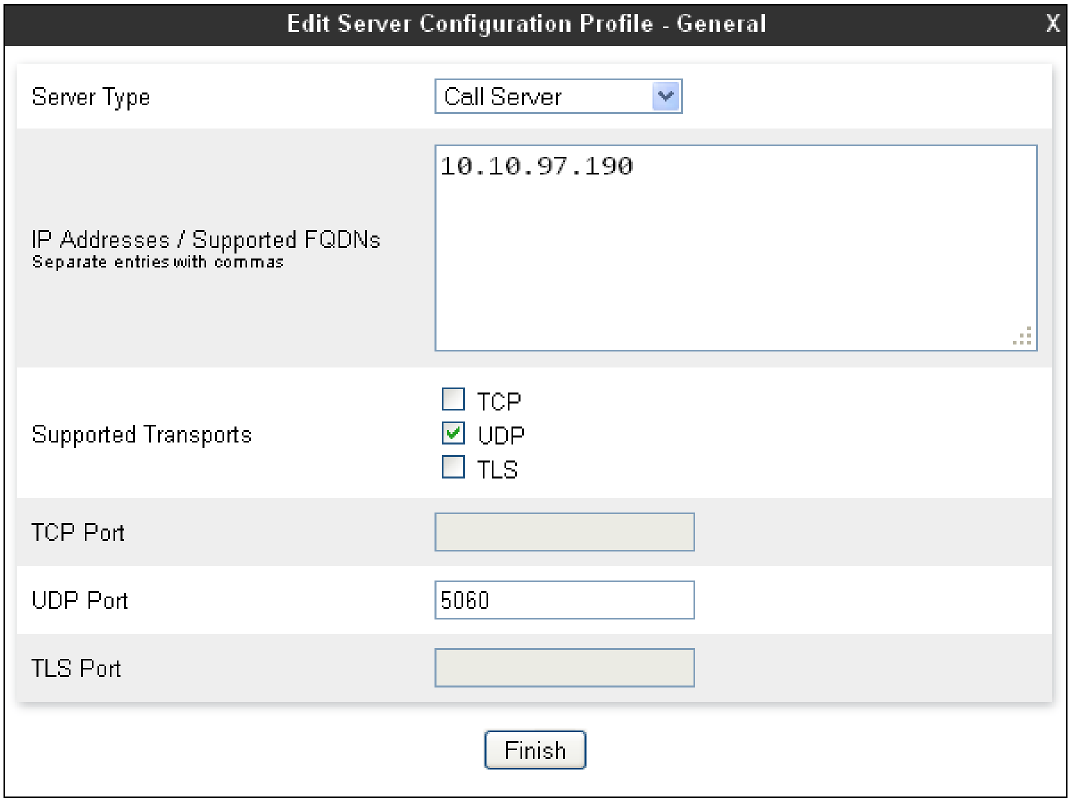


Session Border Controller for Enterprise

Server Profiles: SM63, [redacted], [redacted], [redacted], [redacted], [redacted], [redacted], [redacted], [redacted], [redacted], [redacted], CAR276

Server Type	Call Server
IP Addresses / FQDNs	10.10.97.190
Supported Transports	UDP
UDP Port	5060

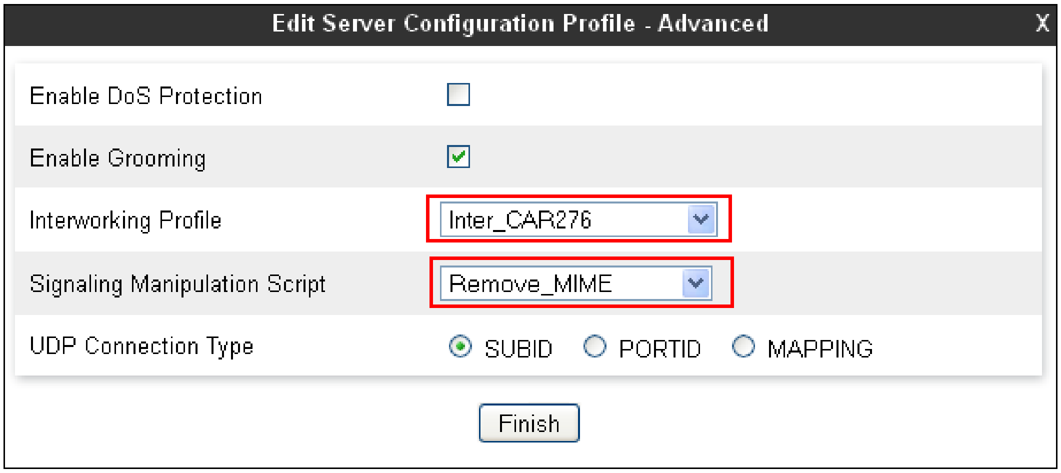
In the **General** tab, specify Server Type as **Call Server**. The IP connectivity has also been defined as shown in the screenshot below. In this compliance testing, the CS1000 was configured with transport protocol **UDP** and listens on port **5060**. Click **Finish** button to save and close the window.



Edit Server Configuration Profile - General

Server Type	Call Server
IP Addresses / Supported FQDNs Separate entries with commas	10.10.97.190
Supported Transports	□ TCP ☑ UDP □ TLS
TCP Port	
UDP Port	5060
TLS Port	

Under the **Advanced** tab, for **Interworking Profile** drop down list, select **Intel_CAR276** as defined in **Section 6.2.4.2** and for **Signaling Manipulation Script** drop down list select **Remove_MIME** as defined in **Section 6.2.5.2**. The other settings are kept as default. Click **Finish** button to save and close the window.



Edit Server Configuration Profile - Advanced

Enable DoS Protection	□
Enable Grooming	☑
Interworking Profile	Inter_CAR276
Signaling Manipulation Script	Remove_MIME
UDP Connection Type	● SUBID ○ PORTID ○ MAPPING

6.3. Domain Policies

Domain Policies configure various rule sets (policies) to control unified communications based upon the 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 Avaya SBCE to aggregate, monitor, control and normalize call flow. There are default policies available for use, or a custom domain policy can be created.

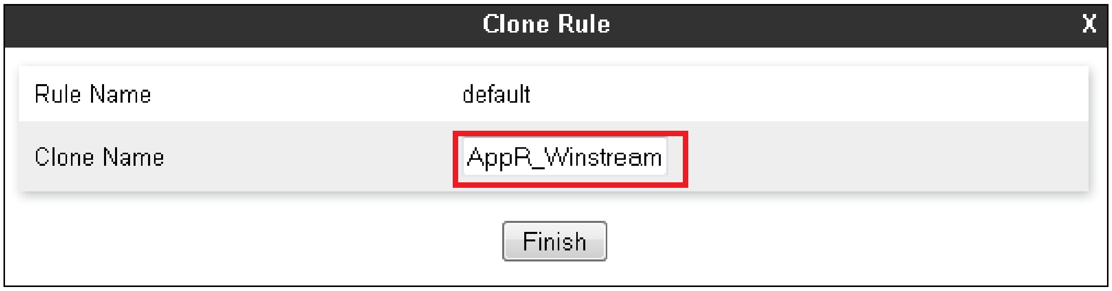
6.3.1. Application Rules

Application Rules define which types of SIP-based Unified Communications (UC) applications the Avaya SBCE 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.

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

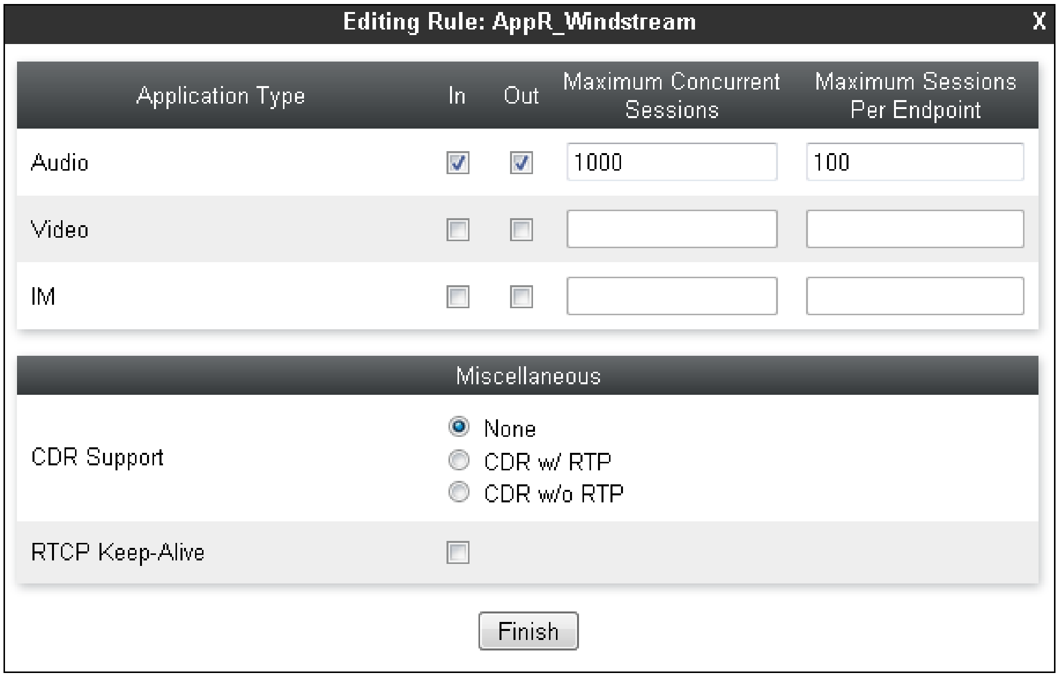
To clone an Application Rule, navigate to **Domain Policies → Application Rules**, select the default rule then click on the **Clone Rule** button (not shown).

Enter a descriptive name, e.g., **AppR_Windstream** for the new rule then click on the **Finish** button.



Rule Name	default
Clone Name	AppR_Winstream

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 to process. The following screen shows the modified Application Rule with the **Maximum Concurrent Sessions** and **Maximum Session Per Endpoint** set to **1000** and **100**. In the compliance testing, the CS1000 was programmed to control the concurrent sessions by setting the number of Virtual Trunks (see **Section 5.5.7**) to the allotted number. Therefore, the values in the Application Rule **AppR_Windstream** are set high enough to be considered non-blocking.



Editing Rule: AppR_Windstream

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	☑	☑	1000	100
Video	□	□		
IM	□	□		

Miscellaneous

CDR Support	● None ○ CDR w/ RTP ○ CDR w/o RTP
RTCP Keep-Alive	□

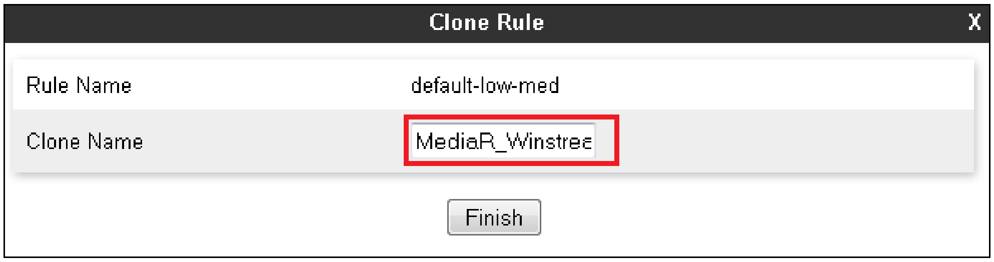
6.3.2. Media Rules

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 packet matching the criteria will be handled by the Avaya SBCE.

A custom Media Rule was created to set the **Quality of Service** and **Media Anomaly Detection**. The sample configuration showed Media Rule **MediaR_Windstream** which was used for both the enterprise and Windstream networks.

To create a **Media Rule**, navigate to **Domain Policies → Media Rules**, select the **default-low-med** rule then click on the **Clone** button (not shown).

Enter a descriptive name, e.g., **MediaR_Windstream** for the new rule then click **Finish** button.

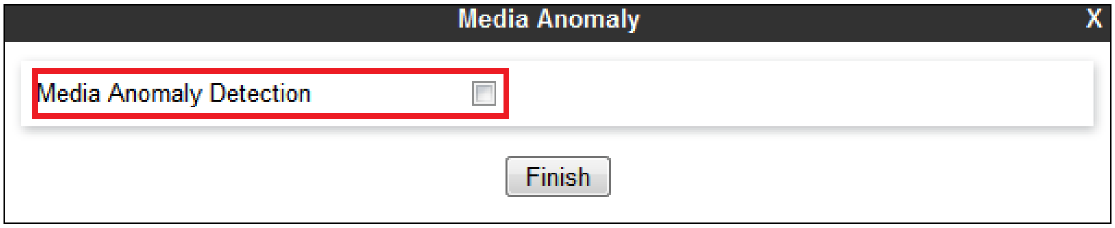


Clone Rule

Rule Name	default-low-med
Clone Name	MediaR_Winstree

When the RTP changes while the call is in progress, the Avaya SBCE interprets this as an anomaly and an alert will be created in the Incidents Log. Disabling **Media Anomaly Detection** could prevent the **RTP Injection Attack** alerts from being created in the log when the audio attributes change.

To modify Media Anomaly, select the **Media Anomaly** tab and click on the **Edit** button (not shown). Then uncheck **Media Anomaly Detection** and click on the **Finish** button.

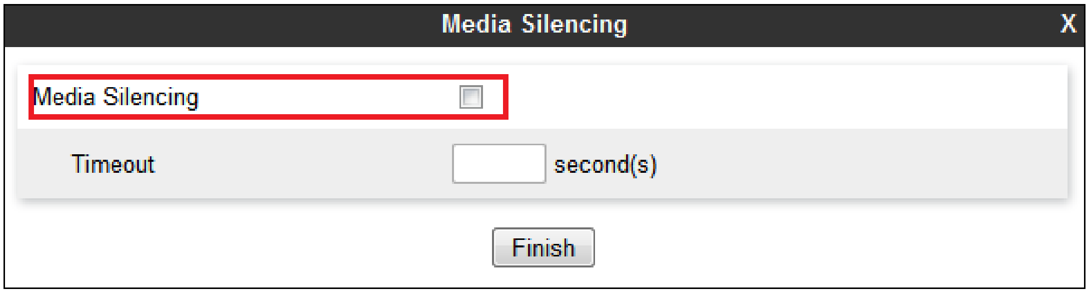


Media Anomaly

Media Anomaly Detection ☐

On the Avaya SBCE, the Media Silencing feature detects the silence when the call is in progress. If the silence is detected and exceeds the allowed duration, the Avaya SBCE generates an alert in the **Incidents Log**. In the compliance testing, the Media Silencing detection was disabled to prevent the call from unexpectedly disconnecting due to a RTP packet lost on the public Internet.

To modify Media Silencing, select the **Media Silencing** tab and click on the **Edit** button (not shown). Then uncheck **Media Silencing** and click on the **Finish** button.

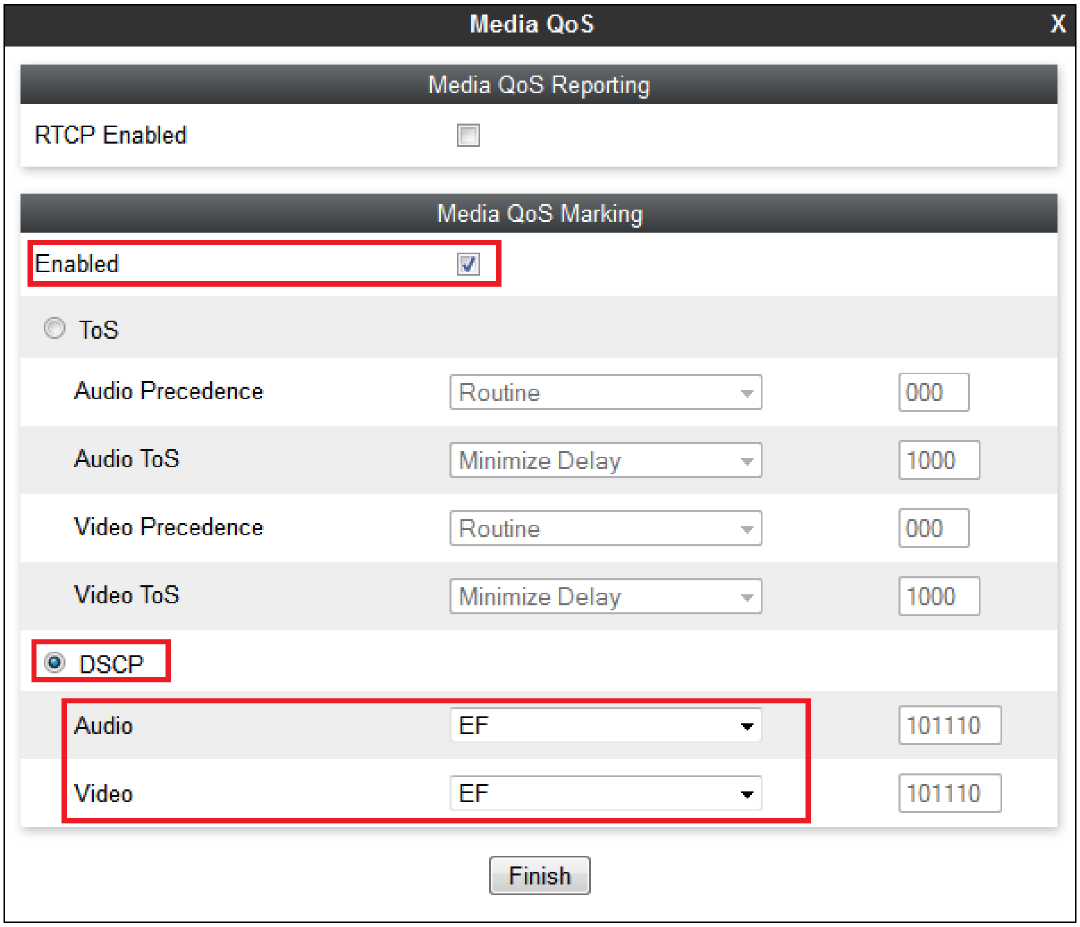


Media Silencing

Media Silencing ☐

Timeout ____ second(s)

Under **Media QoS** tab, click on the **Edit** button (not shown) to configure the Quality of Service (QoS). The Avaya SBCE can be configured to mark the Differentiated Services Code Point (DSCP) in the IP packet header with specific values to support Quality of Services policies for the media. The **Audio** and **Video** are set to **EF** as recommended by the service provider. The following screen shows the QoS values used for the compliance testing.



Media QoS

Media QoS Reporting

RTCP Enabled	□	

Media QoS Marking

Enabled	☑	
○ ToS		
Audio Precedence	Routine	000
Audio ToS	Minimize Delay	1000
Video Precedence	Routine	000
Video ToS	Minimize Delay	1000
● DSCP		
Audio	EF	101110
Video	EF	101110

6.3.3. Signaling Rules

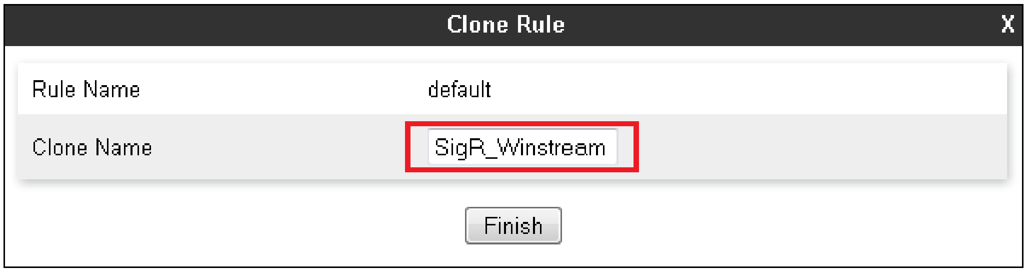
Signaling Rules define actions to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. When SIP signaling packets are received by the Avaya SBCE, they are parsed and "pattern-matched" against the particular signaling criteria defined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

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

In the compliance testing, two **Signaling Rules** were created for Windstream and the CS1000.

6.3.3.1 Signaling Rule for Windstream

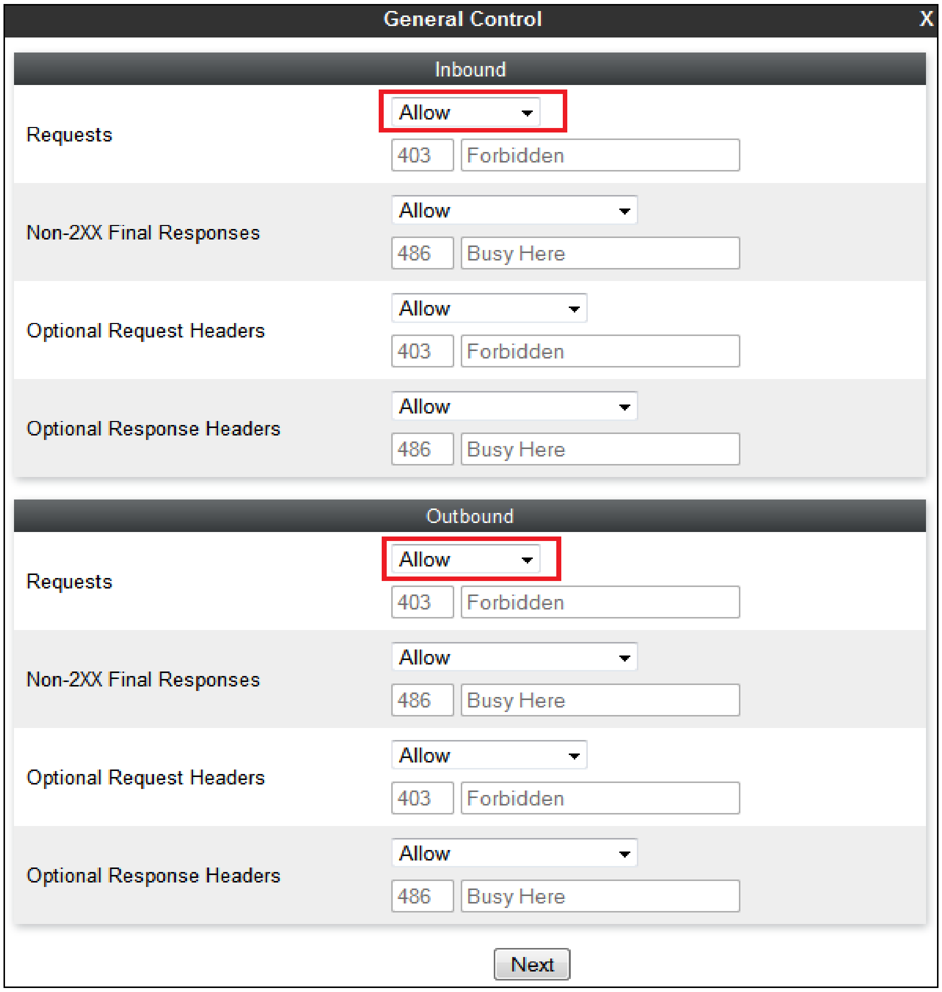
Clone a Signaling Rule with a descriptive name, e.g., **SigR_Windstream** and click on the **Finish** button.



Clone Rule

Rule Name	default
Clone Name	SigR_Winstream

The **SigR_Windstream** was configured to allow the Avaya SBCE to accept inbound and outbound call requests from Windstream. Cloning the Signaling Rule default, the **SigR_Windstream** will allow all requests by default as shown in the following screenshot.



General Control

Inbound

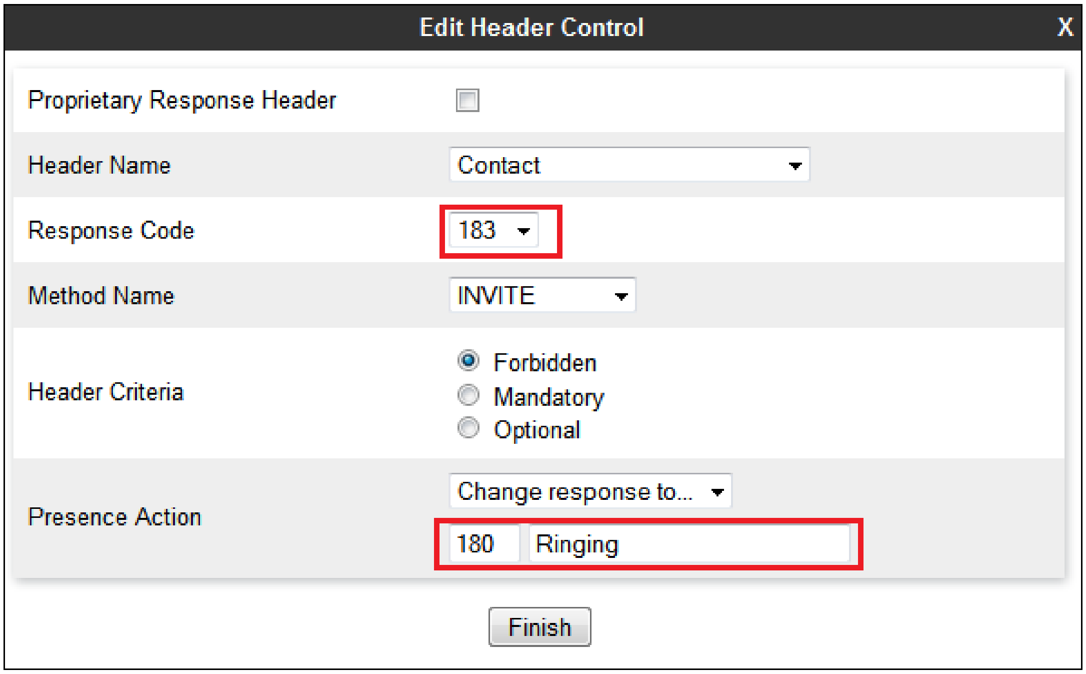
Requests	Allow	403	Forbidden
Non-2XX Final Responses	Allow	486	Busy Here
Optional Request Headers	Allow	403	Forbidden
Optional Response Headers	Allow	486	Busy Here

Outbound

Requests	Allow	403	Forbidden
Non-2XX Final Responses	Allow	486	Busy Here
Optional Request Headers	Allow	403	Forbidden
Optional Response Headers	Allow	486	Busy Here

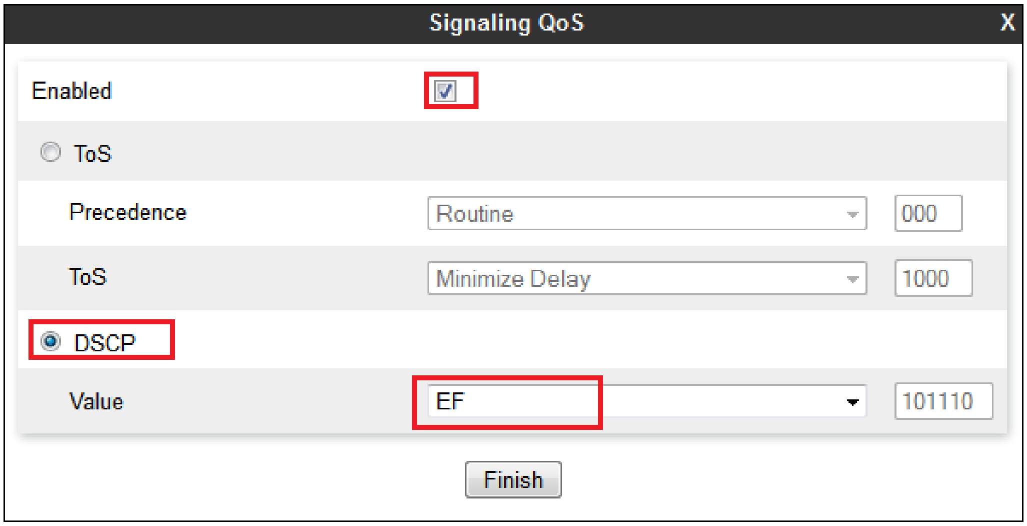
On the **Response Headers** tab, click on **Add In Header Control** button to add a header control. This header will modify "183 SDP Session Progress" message responded from Windstream to

“180 SDP Ringing”. This header control combines with Server Interworking in section **6.2.4.2** to fix the ring back tone issue for the call blind transfer. See **Section 2.2**.



Proprietary Response Header	□
Header Name	Contact
Response Code	183
Method Name	INVITE
Header Criteria	● Forbidden ○ Mandatory ○ Optional
Presence Action	Change response to... 180 Ringing

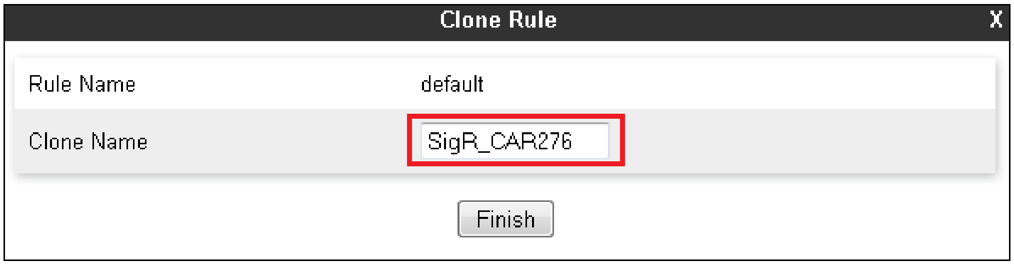
On the **Signaling QoS** tab, select the proper Quality of Service (QoS). The Avaya SBCE can be configured to mark the Differentiated Services Code Point (DSCP) in the IP packet header with specific values to support Quality of Services policies for signaling. The following screen shows the QoS value used for the compliance testing.



Enabled	☑	
○ ToS		
Precedence	Routine	000
ToS	Minimize Delay	1000
● DSCP		
Value	EF	101110

6.3.3.2 Signaling Rule for the CS1000

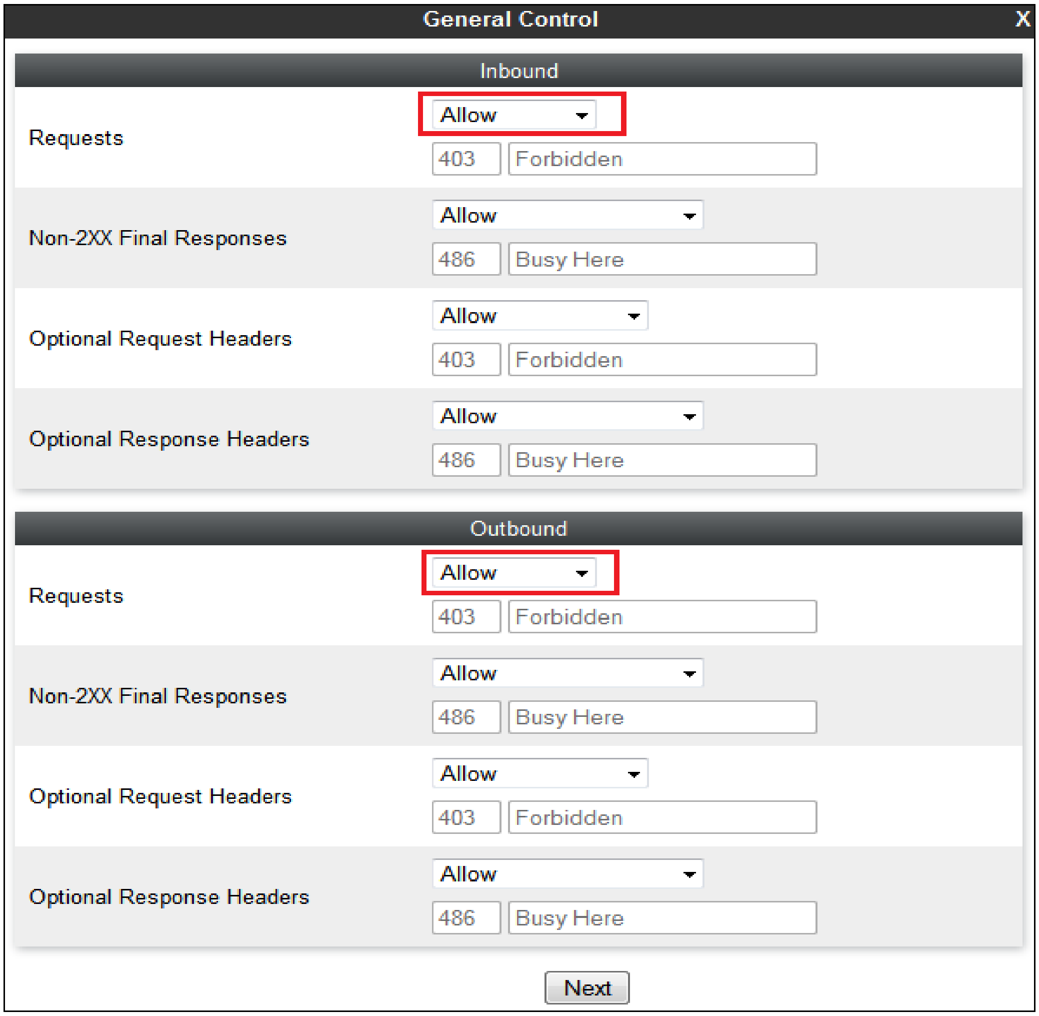
Clone a Signaling Rule with a descriptive name e.g., **SigR_CAR276** for the CS1000 and click on the **Finish** button.



Clone Rule

Rule Name	default
Clone Name	SigR_CAR276

This **SigR_CAR276** is configured to allow the Avaya SBCE to accept inbound and outbound call requests from the CS1000. Cloning the **S**ignaling Rule **default**, the **SigR_CAR276** will allow all requests **by default** as shown in the following screenshot.



General Control

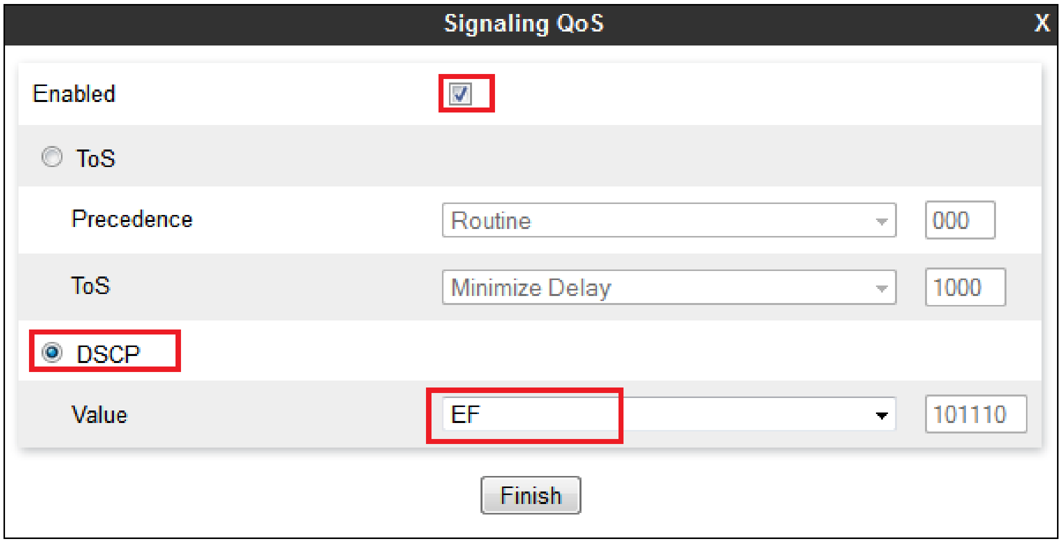
Inbound

Requests	Allow	403	Forbidden
Non-2XX Final Responses	Allow	486	Busy Here
Optional Request Headers	Allow	403	Forbidden
Optional Response Headers	Allow	486	Busy Here

Outbound

Requests	Allow	403	Forbidden
Non-2XX Final Responses	Allow	486	Busy Here
Optional Request Headers	Allow	403	Forbidden
Optional Response Headers	Allow	486	Busy Here

On the **Signaling QoS** tab, select the proper Quality of Service (QoS). The Avaya SBCE can be configured to mark the Differentiated Services Code Point (DSCP) in the IP packet header with specific values to support Quality of Services policies for signaling. The following screen shows the QoS value used for the compliance testing.



Signaling QoS

Enabled	☑	
○ ToS		
Precedence	Routine	000
ToS	Minimize Delay	1000
● DSCP		
Value	EF	101110

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**.**

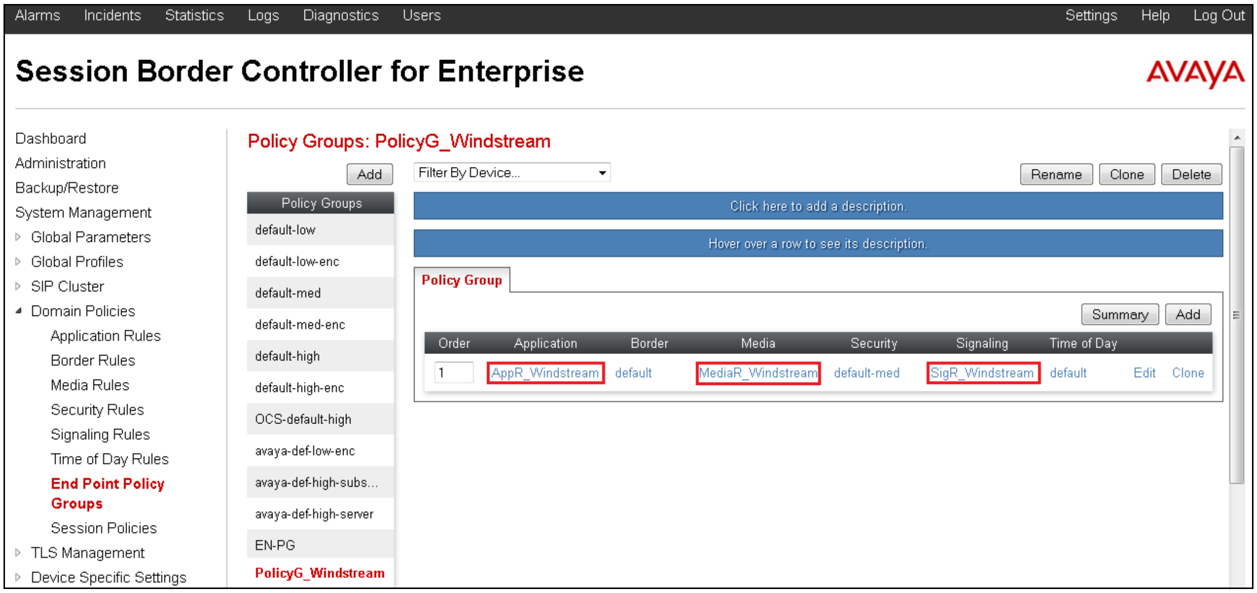
Two Endpoint Policy Groups were separately created for Windstream and the CS1000.

To create a policy group, navigate to **System Management → Domain Policies → Endpoint Policy Groups** and click on the **Add** button (not shown).

6.3.4.1 Endpoint Policy Group for Windstream

The following screen shows **PolicyG_Windstream** created for Windstream.

- Set Application Rule to **AppR_Windstream** which was created in **Section 6.3.1**.
- Set Media Rule to **MediaR_Windstream** which was created in and **Section 6.3.2**.
- Set Signaling Rule to **SigR_Windstream** which was created in **Section 6.3.3.1**.
- Set **Border** and **Time of Day** rules to **default**.
- Set **Security** rule to **default-med**.



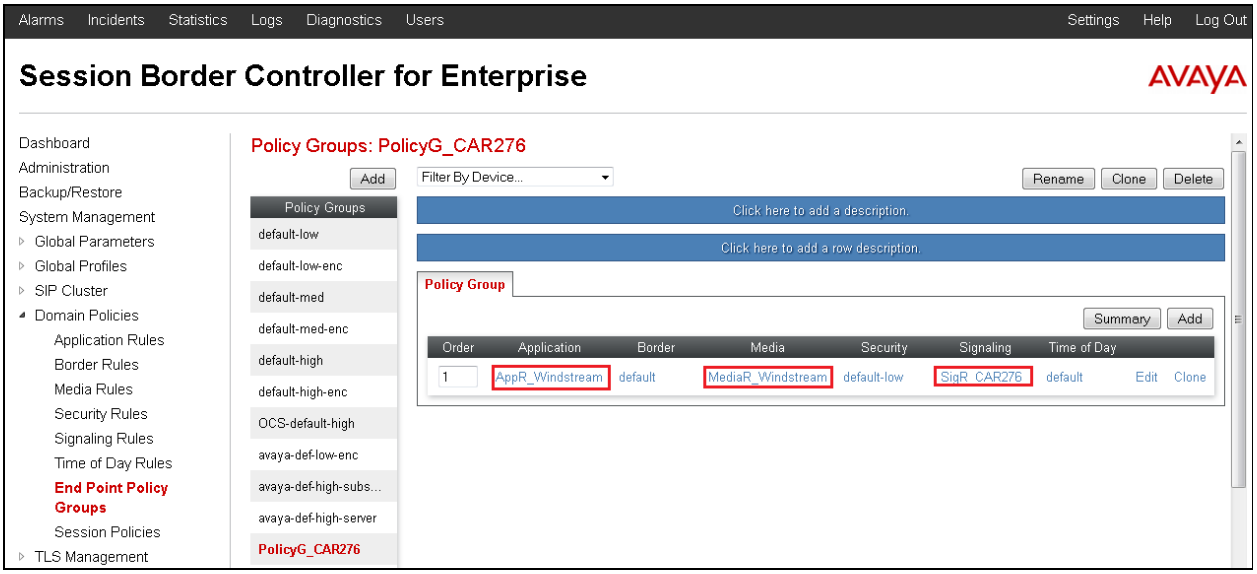
Policy Groups: PolicyG_Windstream

Order	Application	Border	Media	Security	Signaling	Time of Day		
1	AppR_Windstream	default	MediaR_Windstream	default-med	SigR_Windstream	default	Edit	Clone

6.3.4.2 Endpoint Policy Group for the CS1000

The following screen shows policy group **PolicyG_CAR276** created for the CS1000.

- Set Application Rule to **AppR_Windstream** which was created in **Section 6.3.1**.
- Set Media Rule to **MediaR_Windstream** which was created in and **Section 6.3.2**.
- Set Signaling Rule **SigR_CAR276** which was created in **Section 6.3.3.2**.
- Set the **Border** and **Time of Day** rules to **default**.
- Set the **Security** rule to **default-low**.



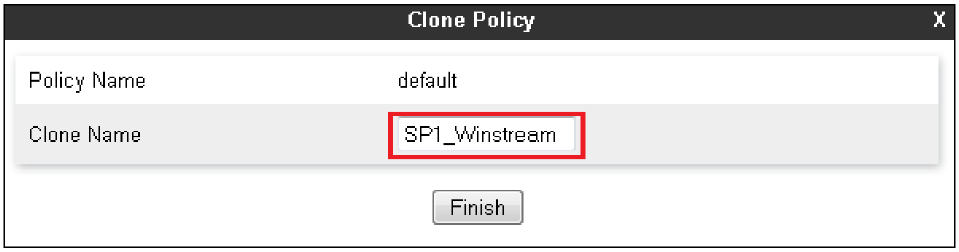
Policy Groups: PolicyG_CAR276

Order	Application	Border	Media	Security	Signaling	Time of Day		
1	AppR_Windstream	default	MediaR_Windstream	default-low	SigR_CAR276	default	Edit	Clone

6.3.5. Session Policy

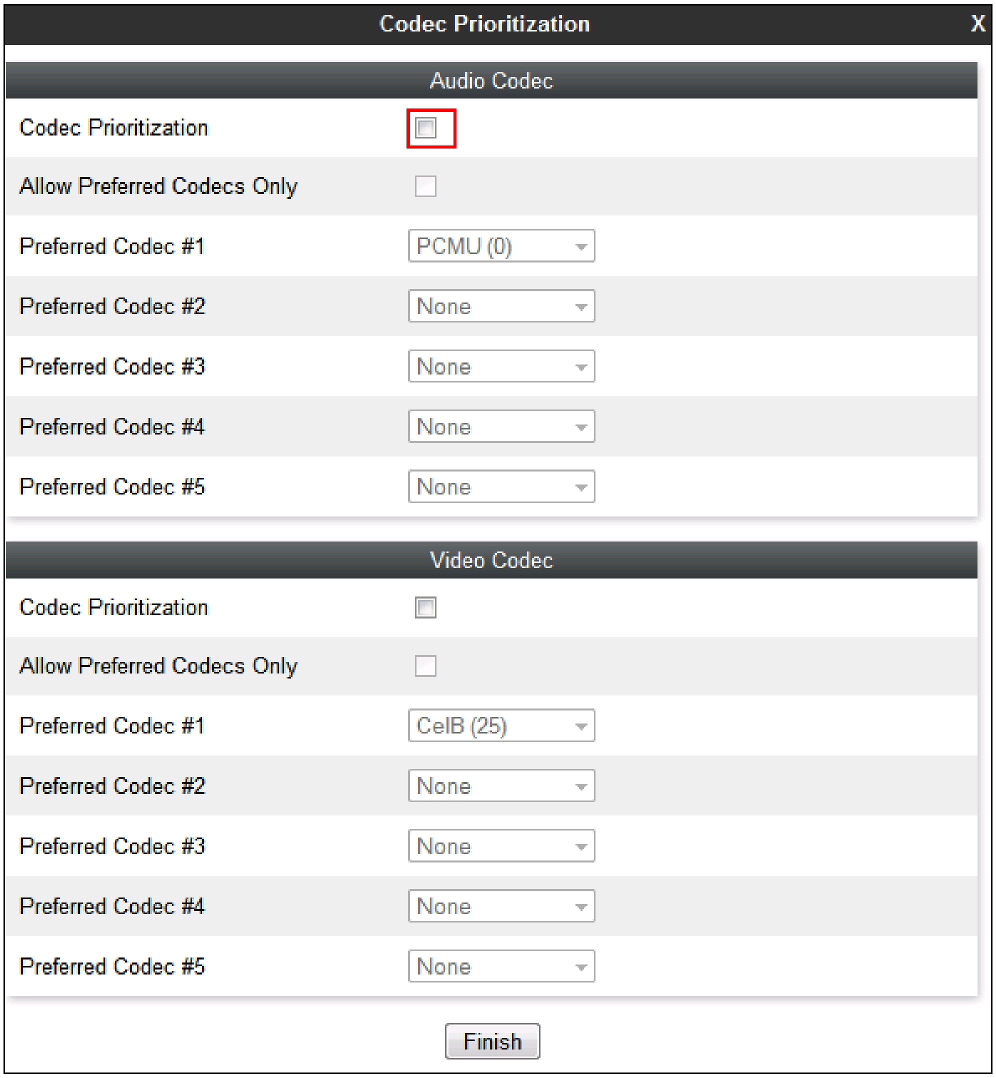
Session Policy is applied based on the source and destination of a media session (i.e., which codec is to be applied to the media session between its source and destination). The source and destination are defined in URI Group in **Section 6.2.1**.

In the compliance testing, the Session Policy **Windstream** was created to match the codec configuration on Windstream. The policy also allows the Avaya SBCE to anchor media in off-net call forward and call transfer scenarios. To clone a common Session Policy which applies to both Windstream and the CS1000, navigate to **Domain Policies → Session Policies**, select the **default** rule then click on the **Clone** button (not shown). Enter a descriptive name, e.g., **SP1_Windstream** for the new policy and click on the **Finish** button.



Policy Name	default
Clone Name	SP1_Winstream

Windstream supports voice codec G.711MU and G.729. To define **Codec Prioritization** for Audio Codec, select the profile **Windstream** created above, click on the **Edit** button (not shown) and leave the **Codec Prioritization** option unchecked, with this configuration Avaya SBCE will pass all codecs that are supported and sent by CS1000 to Windstream and vice versa.



Codec Prioritization

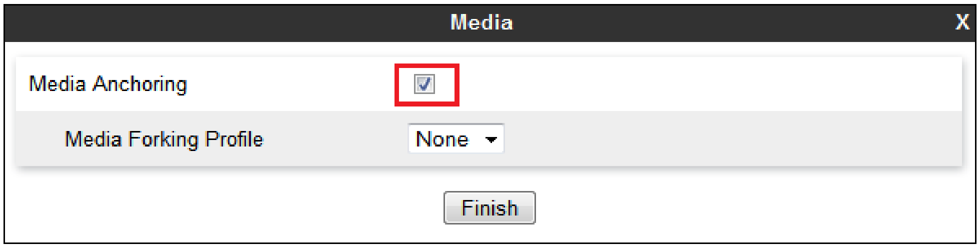
Audio Codec

Codec Prioritization	□
Allow Preferred Codecs Only	□
Preferred Codec #1	PCMU (0)
Preferred Codec #2	None
Preferred Codec #3	None
Preferred Codec #4	None
Preferred Codec #5	None

Video Codec

Codec Prioritization	□
Allow Preferred Codecs Only	□
Preferred Codec #1	CelB (25)
Preferred Codec #2	None
Preferred Codec #3	None
Preferred Codec #4	None
Preferred Codec #5	None

Under **Media** tab of the Session Policy **SP1_Windstream** created above, click on the **Edit** button (not shown) then check on **Media Anchoring** to allow the Avaya SBCE to anchor media in off-net call forward and call transfer scenarios.



Media

Media Anchoring	☑
Media Forking Profile	None

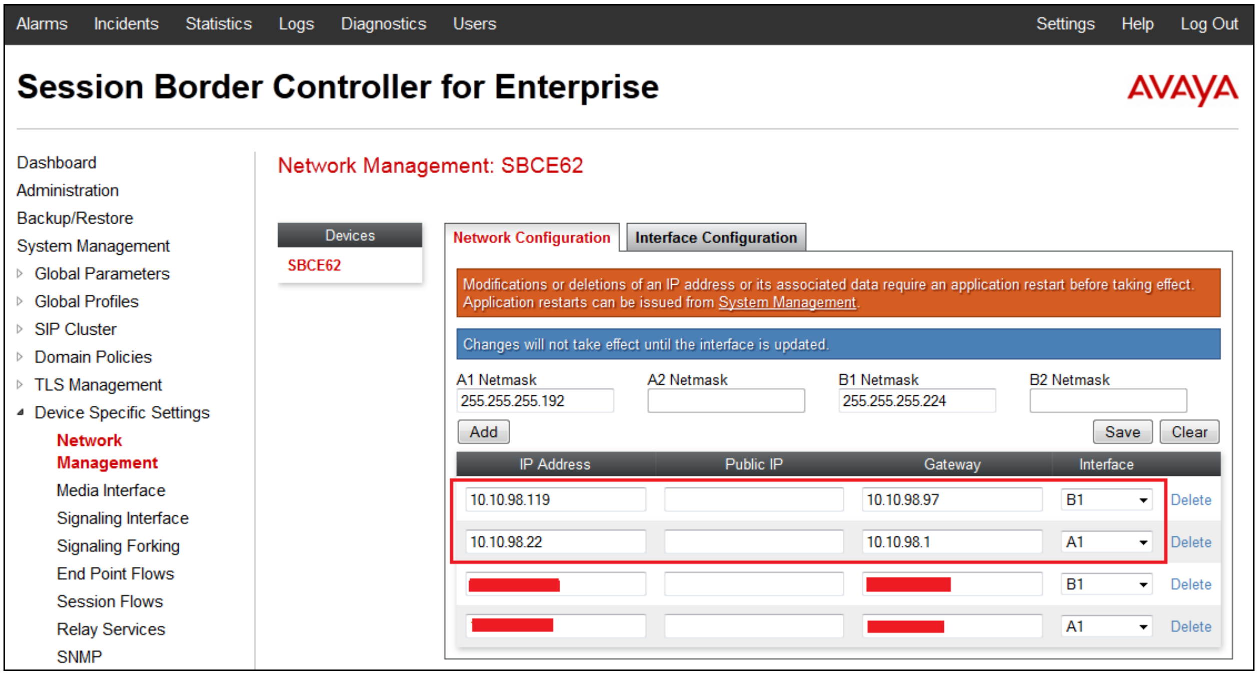
6.4. Device Specific Settings

Device Specific Settings 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

The Network Management page is where the network interface settings are configured and enabled. During the installation process of the Avaya SBCE, certain network-specific information is defined such as device IP addresses, public IP addresses, subnet mask, gateway, etc. to interface the device to the network. This information populates the various Network Management tabs, which can be edited as needed to optimize device performance and network efficiency.

Navigate to **System Management → Device Specific Settings → Network Management**, Under the **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** appropriate to the parameters shown in **Figure 1**.



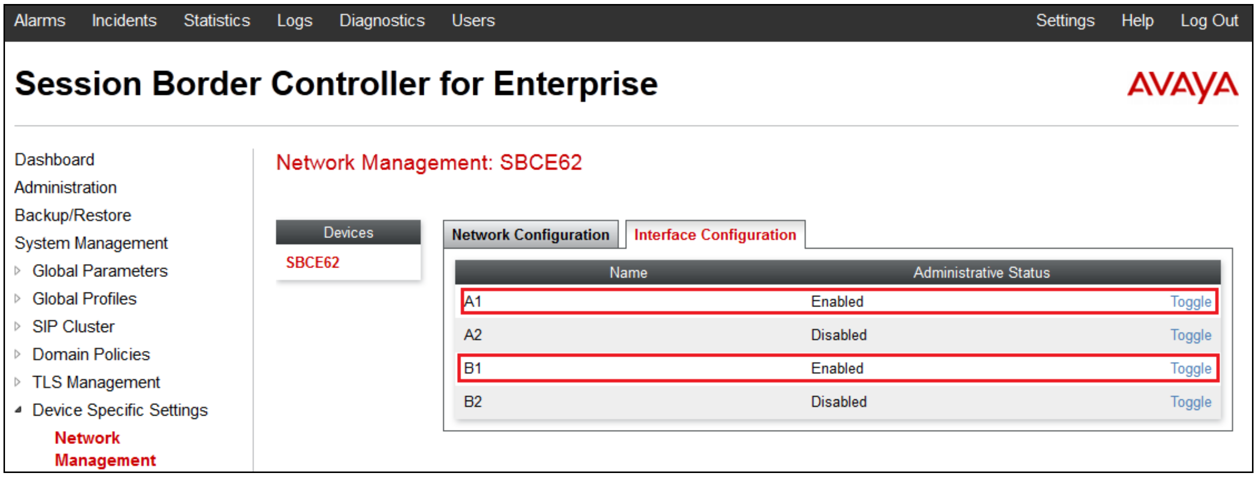
Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management.

Changes will not take effect until the interface is updated.

A1 Netmask	A2 Netmask	B1 Netmask	B2 Netmask
255.255.255.192		255.255.255.224	

IP Address	Public IP	Gateway	Interface	
10.10.98.119		10.10.98.97	B1	Delete
10.10.98.22		10.10.98.1	A1	Delete
[redacted]		[redacted]	B1	Delete
[redacted]		[redacted]	A1	Delete

On the **Interface Configuration** tab, enable the interfaces connecting to the inside and outside networks. To enable an interface click it's **Toggle State** button. The following screen shows interface **A1** and **B1** were **Enabled**.



Network Management: SBCE62

Name	Administrative Status	
A1	Enabled	Toggle
A2	Disabled	Toggle
B1	Enabled	Toggle
B2	Disabled	Toggle

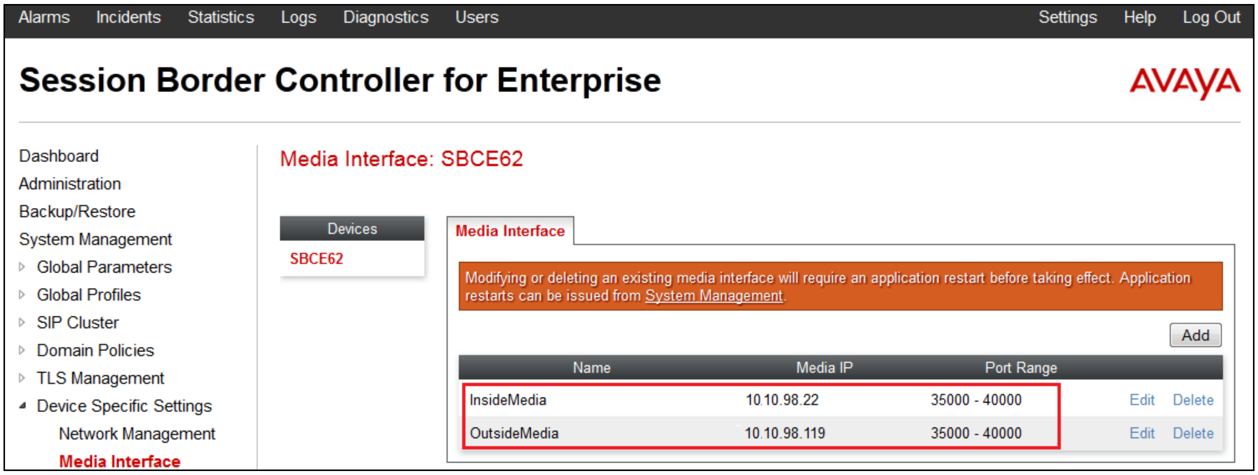
6.4.2. Media Interface

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

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

Two separate Media Interfaces are needed for both the inside and outside interfaces. The following screen shows the Media Interfaces **InsideMedia** and **OutsideMedia** were created for the compliance testing.

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



Media Interface: SBCE62

Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.

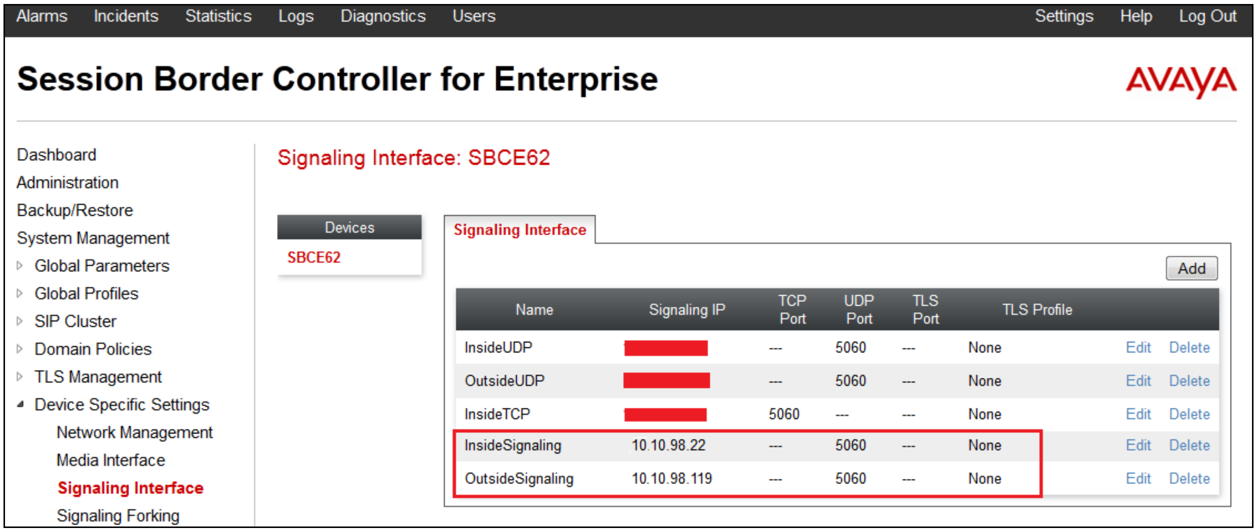
Name	Media IP	Port Range		
InsideMedia	10.10.98.22	35000 - 40000	Edit	Delete
OutsideMedia	10.10.98.119	35000 - 40000	Edit	Delete

6.4.3. Signaling Interface

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

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

Two separate Signaling Interfaces are needed for both inside and outside interfaces. The following screen shows the Signaling Interfaces **InsideSignaling** and **OutsideSignaling** were created in the compliance testing with **UDP/5060** for both inside and outside interfaces.



Signaling Interface: SBCE62

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile		
InsideUDP	[redacted]	---	5060	---	None	Edit	Delete
OutsideUDP	[redacted]	---	5060	---	None	Edit	Delete
InsideTCP	[redacted]	5060	---	---	None	Edit	Delete
InsideSignaling	10.10.98.22	---	5060	---	None	Edit	Delete
OutsideSignaling	10.10.98.119	---	5060	---	None	Edit	Delete

6.4.4. End Point Flows - Server Flow

When a packet is received by Avaya SBCE, 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.

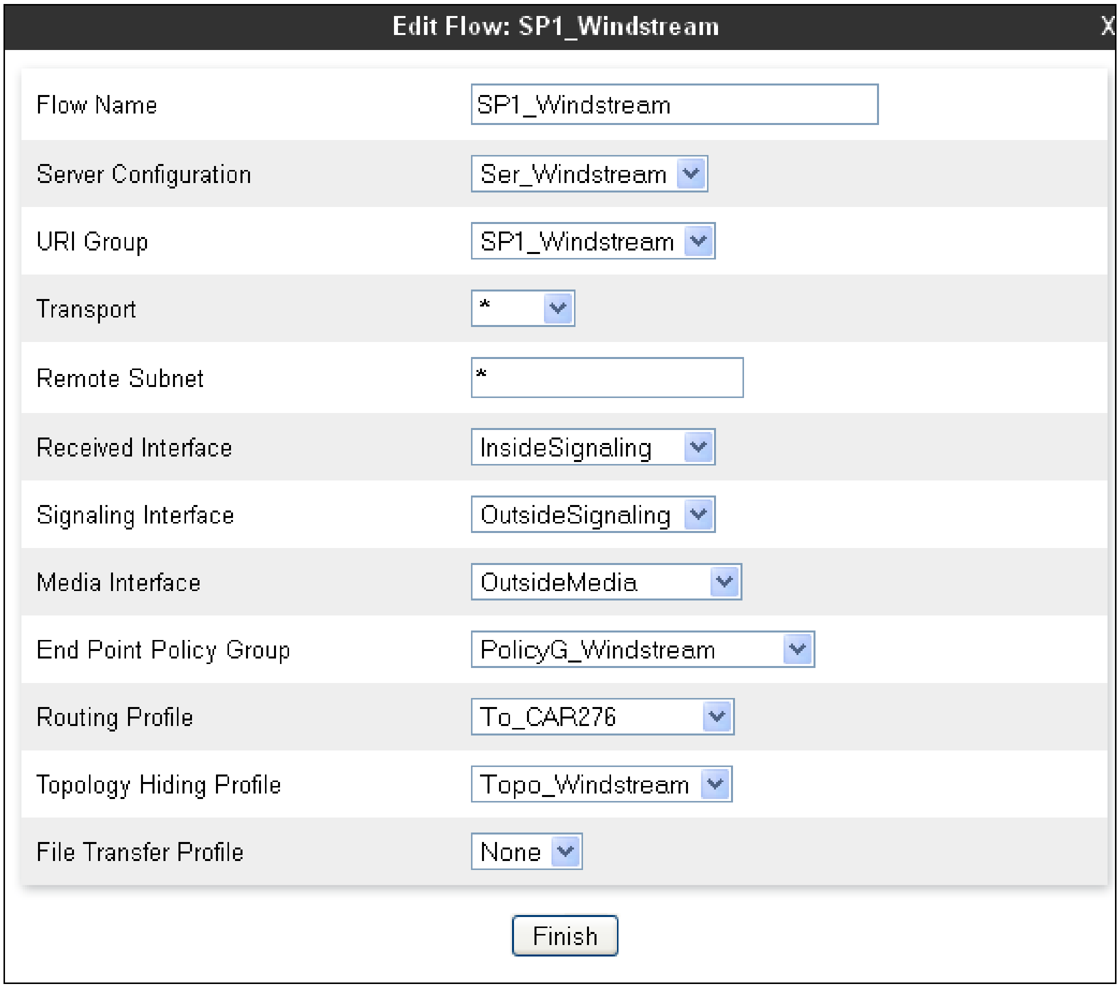
In the compliance testing, two separate Server Flows were created for Windstream and the CS1000.

To create a Server Flow, navigate to **System Management → Device Specific Settings → End Point Flows**, select the **Server Flows** tab and click on the **Add** button (not shown). In the new window that appears, enter the following values while the other fields are kept as default.

- **Flow Name**: Enter a descriptive name.
- **Server Configuration**: Select the Server Configuration **Ser_Windstream** created in **Section 0** which the Server Flow associates to.
- **URI Group**: Select the URI Group **SP1_Windstream** created in **Section 6.2.1**.

- **Received Interface**: Select the Signaling Interface created in **Section 6.4.3** which the Server Configuration is designed to receive SIP signaling from.
- **Signaling Interface**: Select the Signaling Interface created in **Section 6.4.3** which the Server Configuration is designed to send the SIP signaling to.
- **Media Interface**: Select the Media Interface created in **Section 6.4.2** which the Server Configuration is designed to send the RTP to.
- **End Point Policy Group**: Select the End Point Policy Group created in **Section 6.3.4**.
- **Routing Profile**: Select the Routing Profile created in **Section 6.2.2** which the Server Configuration is designed to route the calls to.
- **Topology Hiding Profile**: Select the Topology Hiding profile created in **Section 6.2.3** to apply toward the Server Configuration.
- Use default values for all remaining fields. Click **Finish** to save and exit.

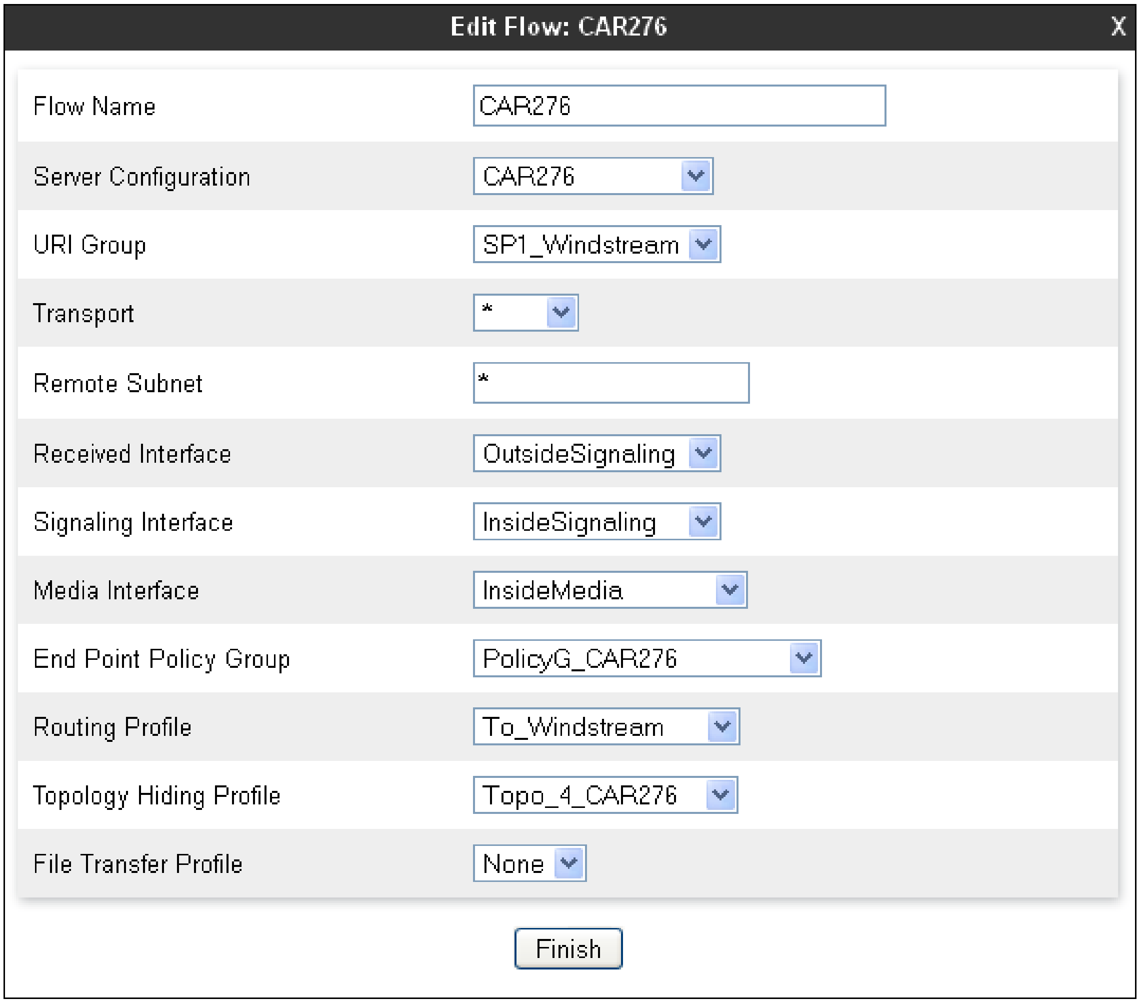
The following screen shows the Server Flow named **SP1_Windstream** for Windstream.



Edit Flow: SP1_Windstream

Flow Name	SP1_Windstream
Server Configuration	Ser_Windstream
URI Group	SP1_Windstream
Transport	*
Remote Subnet	*
Received Interface	InsideSignaling
Signaling Interface	OutsideSignaling
Media Interface	OutsideMedia
End Point Policy Group	PolicyG_Windstream
Routing Profile	To_CAR276
Topology Hiding Profile	Topo_Windstream
File Transfer Profile	None

The following screen shows the Server Flow named **CAR276** for the CS1000.



Edit Flow: CAR276

Flow Name	CAR276
Server Configuration	CAR276
URI Group	SP1_Windstream
Transport	*
Remote Subnet	*
Received Interface	OutsideSignaling
Signaling Interface	InsideSignaling
Media Interface	InsideMedia
End Point Policy Group	PolicyG_CAR276
Routing Profile	To_Windstream
Topology Hiding Profile	Topo_4_CAR276
File Transfer Profile	None

6.4.5. Session Flows

Session Flows allow the 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 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.

A common Session Flow **SP1** was created for both Windstream and the CS1000.

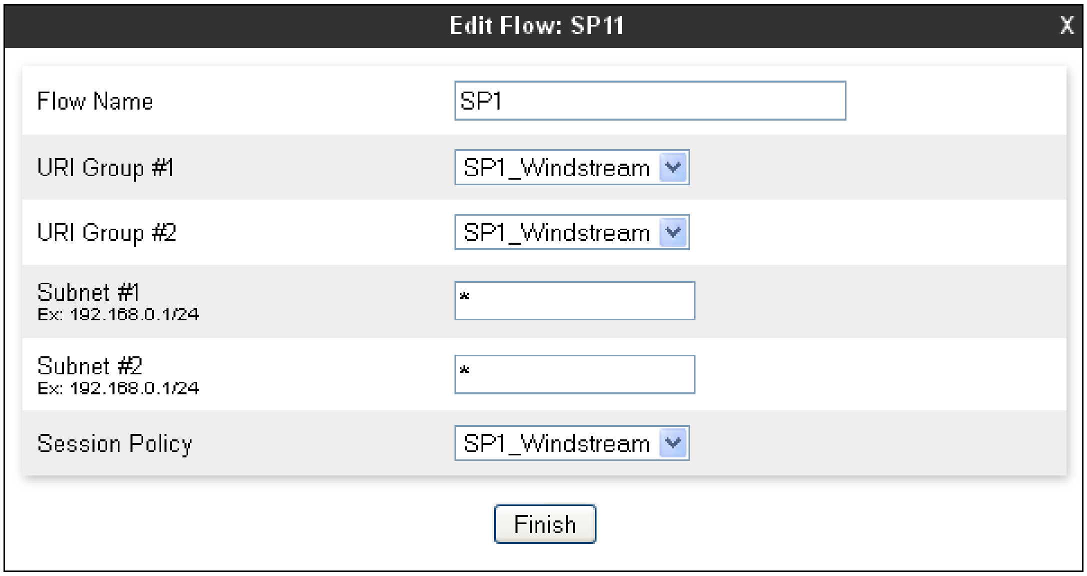
To create a session flow, navigate to **System Management → Device Specific Settings → Session Flows** then click on the **Add Flow** button (not shown). In the new window that appears, enter the following values while the remaining fields are kept as default.

- **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 on the **Finish** button.

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 **SP1**.



Edit Flow: SP11

Flow Name	SP1
URI Group #1	SP1_Windstream
URI Group #2	SP1_Windstream
Subnet #1 Ex: 192.168.0.1/24	*
Subnet #2 Ex: 192.168.0.1/24	*
Session Policy	SP1_Windstream

7. Configure Windstream SIP Trunking Service

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 the enterprise. Windstream will provide the customer with the necessary information to configure the SIP Trunk connection from the enterprise to Windstream.

The information provided by Windstream includes:

- IP address of the Windstream SIP proxy.
- Service provider public SIP domains.
- Supported codecs.
- DID numbers.
- IP addresses and port numbers used for signaling or media through any security devices.
- A customer specific SIP signaling reference.

8. Verification

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 commands that can be used to troubleshoot the solution.

8.1. Verification Steps

The following activities are made to each test scenario.

- Calls are checked for the correct call progress tones and cadences.
- During the ringing state, the ring back tone and destination ringing are checked.
- Calls are checked in both hands-free and handset mode due to internal Avaya requirement.
- Calls are checked for speech path in both directions using spoken words to ensure clarity of speech.
- The display(s) of the sets/clients involved are checked for consistent and expected calling party name and number and redirection information both prior to answer and after call establishment.
- The speech path and messaging system are observed for timely and quality End to End tone audio path generation and application responses.
- The call server maintenance terminal window is used for the monitoring of BUG(s), ERR and AUD messages.
- Speech path and display checked before and after calls are put on/off hold from each end.
- Applicable files are screened on an hourly basis during the testing for messages that may indicate technical issues. This refers to Avaya PBX files.
- Calls are checked to ensure that all resources such as Virtual trunks, TDM trunks, Sets and VGWs are released when a call scenario ends.

8.2. Protocol Traces

The following SIP message headers are inspected using sniffer traces:

- Request-URI: Verify the request number and SIP domain.
- From: Verify the display name and display number.
- To: Verify the display name and display number.
- P-Asserted-Identity: Verify the display name and display number.
- Privacy: Verify privacy masking with “user, id”.
- Diversion: Verify DID number.
- Authorization: Verify Digest Authentication implementation.

The following attributes in SIP message body are inspected using sniffer traces:

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

a) SIP/INVITE from CS1000 captured at Avaya SBCE OUTSIDE interface.

```
INVITE sip:6139675258@64.xxx.xx.174;user=phone SIP/2.0
From: "OfficeE 1490" sip:501xxx1490@10.10.98.119;user=phone
;tag=34d3d50-aa610a87-13c4-55013-54cba-321577fb-54cba
To: <sip:6139675258@64.xxx.xx.174;user=phone>
CSeq: 1 INVITE
Call-ID: fa9d8b43e2953717f450c54e0f127b40
Contact: <sip:5012871490@135.10.98.119:5060;transport=udp;user=phone;
gsid=f60d0850-9e48-11e3-87c0-e41f13b32ca8>
Record-Route: <sip:10.10.98.119:5060;ipcs-line=340148;lr;transport=udp>
Allow: INVITE, ACK, BYE, REGISTER, REFER, NOTIFY, CANCEL, PRACK, OPTIONS, INFO,
SUBSCRIBE, UPDATE
Supported: 100rel, x-nortel-sipvc, replaces
User-Agent: Nortel CS1000 SIP GW release_7.0 version_ssLinux-7.65.16 AVAYA-SM-6.3.4.0.634014
Max-Forwards: 30
Via: SIP/2.0/UDP 10.10.98.119:5060;branch=z9hG4bK-s1632-000536499325-1--s1632-
Alert-Info: <cid:external@avayalab.com>
Privacy: none
P-Asserted-Identity: "OfficeE 1490" <sip:501xxx1490@10.10.98.119;user=phone>
History-Info: <sip:6139675258@64.xxx.xx.174;user=phone>;index=1
History-Info:<sip:6139675258@avayalab.com;user=phone>;index=1.1
Remote-Address: 10.33.5.6:5201:1:2
Content-Type: application/sdp
P-AV-Message-Id: 1_1
x-nt-e164-clid: +5012871490@avayalab.com;user=phone
P-Charging-Vector: icid-value="f60d0850-9e48-11e3-87c0-e41f13b32ca8"
Av-Global-Session-ID: f60d0850-9e48-11e3-87c0-e41f13b32ca8
P-Location: SM;origlocname="Belleville";origsiglocname="Belleville";origmedialocname="Belleville";
termlocname="Belleville";termsiglocname="Belleville";smaccounting="true"
Content-Length: 264
v=0
o=- 257 1 IN IP4 10.10.98.119
s=-
c=IN IP4 10.10.98.119
t=0 0
m=audio 35464 RTP/AVP 0 8 18 101 111
c=IN IP4 10.10.98.119
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=rtpmap:111 X-nt-inforeq/8000
a=ptime:20
a=sendrecv
```

b) SIP/183 SDP responded from Windstream

```
SIP/2.0 183 Session Progress
Via: SIP/2.0/UDP 10.10.98.119:5060;branch=z9hG4bK-s1632-000536499325-1--s1632-
Record-Route: <sip:10.10.98.119:5060;ipcs-line=340148;lr;transport=udp>
From: "OfficeE 866972" <sip:501xxx1490@10.10.98.119;user=phone>;tag=34d3d50-aa610a87-
13c4-55013-54cba-321577fb-54cba
To:
<sip:6139675258@64.xxx.xx.174;user=phone>;tag=fe6eU1vW9o3YmqAsCF9CEFCB62614da6
Call-ID: fa9d8b43e2953717f450c54e0f127b40
CSeq: 1 INVITE
Contact: <sip:6139675258@64.xxx.xx.174:5060>
Content-Type: application/sdp
Content-Length:   177
v=0
o=- 1782959037 1782959037 IN IP4 64.xxx.xx.174
s=-
c=IN IP4 64.xxx.xx.174
t=0 0
m=audio 16604 RTP/AVP 0 101
a=rtpmap:101 telephone-event/8000
a=ptime:20
a=sendrecv
```

c) SIP/200 SDP responded from Windstream

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.10.98.119:5060;branch=z9hG4bK-s1632-000536499325-1--s1632-
Record-Route: <sip:10.10.98.119:5060;ipcs-line=340148;lr;transport=udp>
From: "OfficeE 1490" <sip:5012871490@10.10.98.119;user=phone>;tag=34d3d50-aa610a87-
13c4-55013-54cba-321577fb-54cba
To:
<sip:6139675258@64.xxx.xx.174;user=phone>;tag=fe6eU1vW9o3YmqAsCF9CEFCB62614da6
Call-ID: fa9d8b43e2953717f450c54e0f127b40
CSeq: 1 INVITE
Contact: <sip:6139675258@64.xxx.xx.174:5060>
Content-Type: application/sdp
Content-Length:   177
v=0
o=- 1782959037 1782959037 IN IP4 64.xxx.xx.174
s=-
c=IN IP4 64.xxx.xx.174
t=0 0
m=audio 16604 RTP/AVP 0 101
a=rtpmap:101 telephone-event/8000
a=ptime:20
a=sendrecv
```

9. Conclusion

These Application Notes describe the configuration necessary to connect the Avaya Communication Server 1000 Release 7.6 and the Avaya Session Border Controller for Enterprise Release 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 enterprises.

All of the test cases have been executed. Despite the number of observations and limitations 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 the Avaya Communication Server 1000 Release 7.6 and the Avaya Session Border Controller for Enterprise Release 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] *Network Routing Service Fundamentals, Avaya Communication Server 1000,* Release 7.6, Document Number NN43001-130, Revision 03.02, Jun 2013.

[2] *IP Peer Networking Installation and Commissioning, Avaya Communication Server 1000,* Release 7.6, Document Number NN43001-313, Revision: 05.02, Jun 2013.

[3] *Communication Server 1000E Overview, Avaya Communication Server 1000,* Release 7.6, Document Number NN43041-110, Revision: 05.02, Jun 2013.

[4] *Communication Server 1000 Unified Communications Management Common Services Fundamentals, Avaya Communication Server 1000,* Release 7.6, Document Number NN43001-116, Revision 05.08, Jun 2013.

[5] *Communication Server 1000 Dialing Plans Reference, Avaya Communication Server 1000,* Release 7.5, Document Number NN43001-283, Revision 05.02, November 2010.

[6] *Product Compatibility Reference, Avaya Communication Server 1000,* Release 7.6, Document Number NN43001-256, Revision 05.02, Jun 2013.

[7] *Installing and Configuring Avaya Aura® System Platform*, Release 6.3.1, Oct 2013.

[8] *Administering Avaya Aura® System Platform*, Release 6.3.1, Oct 2013.

[9] *Installing and Upgrading Avaya Aura® System Manager*, Release 6.3, Oct 2013.

[10] *Maintaining and Troubleshooting Avaya Aura® Session Manager*, Release 6.3, Oct 2013, Document Number 03-603473.

[11] *Administering Avaya Aura® Session Manager*, Release 6.3, Oct 2013, Document Number 03-603324.

[12] *Administering Avaya Session Border Controller for Enterprise,* Release 6.2, Issue 2, Jan 2013.

[13] *RFC3261 SIP: Session Initiation Protocol,* http://www.ietf.org/.

[14] *RFC3262, Reliability of Provisional Responses in the Session Initiation Protocol (SIP)* http://www.ietf.org/.

[15] *RFC2833 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.

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.