



Avaya Solution & Interoperability Test Lab

Application Notes for Gamma SIP Trunking Service with Avaya Communication Server 1000E Release 7.6, Avaya Aura® Session Manager Release 6.3 and Avaya Session Border Controller for Enterprise Release 6.2 – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Gamma SIP Trunking Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Communication Server 1000E Release 7.6, Avaya Aura® Session Manager Release 6.3, Avaya Session Border Controller for Enterprise Release 6.2 and various Avaya endpoints. This documented solution does not extend to configurations without Avaya Aura® Session Manager or Avaya Session Border Controller for Enterprise.

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

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

Table of Contents

1. Introduction.....	4
2. General Test Approach and Test Results.....	4
2.1. Interoperability Compliance Testing	4
2.2. Test Results.....	5
2.3. Support.....	6
3. Reference Configuration	7
4. Equipment and Software Validated	8
5. Configure Avaya Communication Server 1000E	9
5.1. Log into the CS1000.....	9
5.1.1. Log into Unified Communications Management (UCM) and Element Manager (EM)...	9
5.1.2. Log into Call Server Command Line Interface (CLI)	10
5.2. Administer Node IP Telephony	11
5.2.1. Obtain Node IP Address	11
5.2.2. Administer Quality of Service (QoS)	12
5.2.3. Synchronize the new configuration	12
5.3. Administer Voice Codec.....	13
5.3.1. Enable Voice Codec, Node IP Telephony	13
5.3.2. Administer Voice Codec on Media Gateways.....	14
5.4. Administer Zones and Bandwidth	15
5.4.1. Create Zone for VGW and IP phones	15
5.4.2. Create Zone for virtual SIP Trunk	16
5.5. Administer SIP Trunk Gateway.....	16
5.5.1. Integrated Services Digital Network (ISDN).....	16
5.5.2. Administer SIP Trunk Gateway to the Avaya SBCE	17
5.5.3. Administer Virtual D-Channel.....	18
5.5.4. Administer Virtual Super-Loop	20
5.5.5. Enable Music for Customer Data Block	20
5.5.6. Administer Virtual SIP Route	21
5.5.7. Administer Virtual SIP Trunks	24
5.5.8. Administer Calling Line Identification Entry	25
5.5.9. Enable External Trunk to Trunk Transferring	26
5.6. Administer Dialing Plans.....	27
5.6.1. Define ESN Access Codes and Parameters (ESN)	27
5.6.2. Associate Numbering Plan Area Code (NPA) and Special Number (SPN) calls to ESN Access Code 1	28
5.6.3. Administer Digit Manipulation Block (DMI).....	28
5.6.4. Administer Route List Block (RLB).....	30
5.6.5. Administer Incoming Digit Translation (IDC)	31
5.6.6. Administer Outbound Call - Special Number.....	31
6. Configure Avaya Aura® Session Manager	33
6.1. Avaya Aura® System Manager Login and Navigation	33
6.2. Specify SIP Domain.....	34
6.3. Add Location	35
6.4. Add Adaptations	36

6.5. Add SIP Entities.....	37
6.6. Add Entity Links.....	39
6.7. Add Routing Policies	40
6.8. Add Dial Patterns.....	42
6.9. Add Avaya Aura ® Session Manager.....	44
7. Configure Avaya Session Border Controller for Enterprise	46
7.1. Log into Avaya Session Border Controller for Enterprise.....	47
7.2. Global Profiles	49
7.2.1. Uniform Resource Identifier (URI) Groups.....	49
7.2.2. Routing Profiles	50
7.2.3. Topology Hiding.....	52
7.2.4. Server Interworking	53
7.2.5. Signaling Manipulation.....	60
7.2.6. Server Configuration.....	63
7.3. Domain Policies	66
7.3.1. Application Rules.....	66
7.3.2. Media Rules	67
7.3.3. Signaling Rules	69
7.3.4. Endpoint Policy Groups.....	74
7.3.5. Session Policy	75
7.4. Device Specific Settings	77
7.4.1. Network Management.....	77
7.4.2. Media Interface	78
7.4.3. Signaling Interface.....	79
7.4.4. End Point Flows - Server Flow	79
7.4.5. Session Flows.....	81
8. Configure Gamma SIP Trunking Service	82
9. Verification	83
9.1. Verification Steps.....	83
9.2. Protocol Traces	83
10. Conclusion	88
11. References.....	88

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Gamma SIP Trunking Service (Gamma) and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Communication Server 1000E (CS1000) Release 7.6, Avaya Aura® Session Manager (Session Manager) Release 6.3, and Avaya Session Border Controller for Enterprise (Avaya SBCE) Release 6.2 and various Avaya endpoints.

Gamma SIP Trunking Service referenced within these Application Notes is designed for enterprise business customers. Customers using Gamma 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

Gamma is a member of the Avaya DevConnect Service Provider Program. The general test approach is to connect a simulated enterprise to Gamma 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 Gamma 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 2050PC softphones.
- Inbound toll-free and outgoing emergency calls (E999).
- Dialing plans including local, long distance, international, outgoing toll-free, operator assisted calls, etc.
- Calling Party Name presentation and Calling Party Name restriction.
- Proper codec negotiation with G.711A codec and G.729 codec.
- Proper early media transmission using G.711ALaw codec.
- Proper media transmission using G.711ALaw 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 Transfer, Call Forward and Conferencing.
- Fax call over G.711 pass through and T.38.
- Music on Hold.
- Off-net call transfer using subsequent INVITE method.
- Off-net call forward using Diversion method.
- Mobility Extension (MobX) twining incoming call to cellular phones.
- Response to OPTIONS heartbeat.
- Response to incomplete call attempts and trunk errors.
- Session Timers implementation.

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

- Off-net calls transfer using REFER method is not supported.
- Incoming Toll Free is supported but not tested.

2.2. Test Results

Interoperability testing of Gamma 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 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 displaying Calling Party Name and Calling Party Number of the CS1000 extension. This is a known issue of the CS1000 when it interoperates with Gamma where the proprietary signaling of the CS1000 is not supported. This issue has low user impact, it is listed here simply as an observation.
2. **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.
3. **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.

4. **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.
5. **First few words of Avaya CallPilot announcement is getting clipped** when calling from PSTN to the CallPilot. This issue happens on inbound call to CallPilot via SIP trunk but it's not related to SIP Trunk provider. This issue does not happen on local call in the CS1000 system. This issue has small impact to user and is documented as an observation.
6. **SIP Header Optimization:** SIP header rules were implemented in the Avaya SBCE (Section 7.2.5) and in Session Manager to streamline the SIP header and remove any unnecessary parts. The following headers were removed: X_nt_e164_clid, Alert-Info if they were present in the INVITE. Also the multipart MIME SDP, which included the x-nt-mcdn-frag-hex, x-ntesn5-frag-hex, and x-nt-epid-frag were stripped out. These particular headers and MIME have no real use in the Gamma service provider network.
7. **Session interval time out** (Session Expires header) is set to 3600 seconds from Gamma SIP trunking service to refresh calls that are active more than one hour. However in fact the Gamma SIP proxy does not send re-Invite/Update message to refresh session if the call is active for more than one hour, this results in long duration calls that last longer than one hour not to be released properly the SIP trunk of CS1000 is not released when the far end disconnects the call and vice versa. So far, there is no solution from Gamma for this issue, this issue is documented here for customers to use Gamma SIP trunking service interoperating with Avaya CS1000 to be aware of.

2.3. Support

For technical support on the Avaya products described in these Application Notes visit

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

For technical support on Gamma SIP Trunking Service, please contact Gamma at

<http://www.Gamma.co.uk/support>

3. Reference Configuration

Figure 1 illustrates the sample Avaya SIP-enabled enterprise solution connected to Gamma 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 Gamma 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, Gamma provided the service provider public IP address **88.xxx.xx.201**. This public IP address will be used for the public SIP traffic between the Avaya SBCE and Gamma. The Avaya lab was configured with a SIP domain **avayalab.com** for the enterprise, the Topology-Hiding feature of the Avaya SBCE (see **Section 7.2.3.1**) was used to adapt the enterprise SIP domain to the service provider SIP domain known to Gamma.

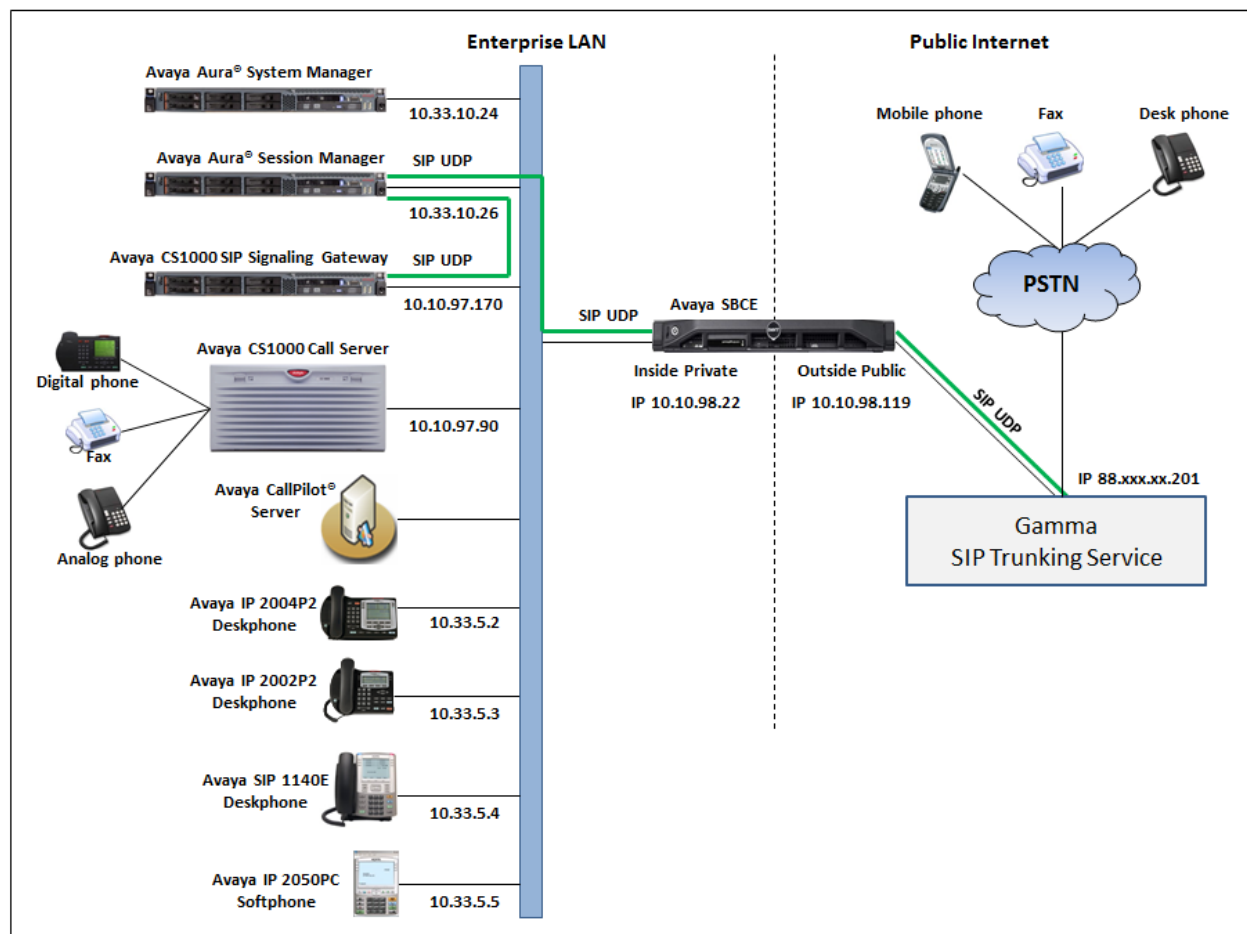


Figure 1: Avaya IP Telephony Network connecting to Gamma SIP Trunking Service

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)	<ul style="list-style-type: none"> • Call Server: 7.65 P GA plus latest DEPLIST Issue: 01 Release: 2013-09-24 (est) • SSG and SLG Server: 7.65.16 GA plus latest Service Pack 3 SP_7.6_3.ntl
Avaya Media Gateway Controller (MGC) Avaya DSP	<ul style="list-style-type: none"> • MGCCDC02 • DSP1AB07
Avaya Aura® Session Manager running on Avaya S8800 Server	6.3.4 – FP3 (6.3.4.4.1830)
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	<ul style="list-style-type: none"> • 2002 p2: 0604DCO (UNISim) • 2004 p2: 0604DCO (UNISim) • 1140: 0625C8Q (UNISim) • 1120: 0624C6Q (UNISim) • 2007: 0621C8Q (UNISim) • SIP 1140: SIP11x0e04.03.12.00
Avaya 2050PC 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
Gamma SIP Trunking Service Components	
Equipment/Software	Release/Version
Ericsson Softswitch	R1G.5R.516.061
Genband Session Border Controller	V8.2

Table 1: Equipment and Software Tested

5. Configure Avaya Communication Server 1000E

This section describes the procedure for configuring the CS1000 for inter-operating with Gamma.

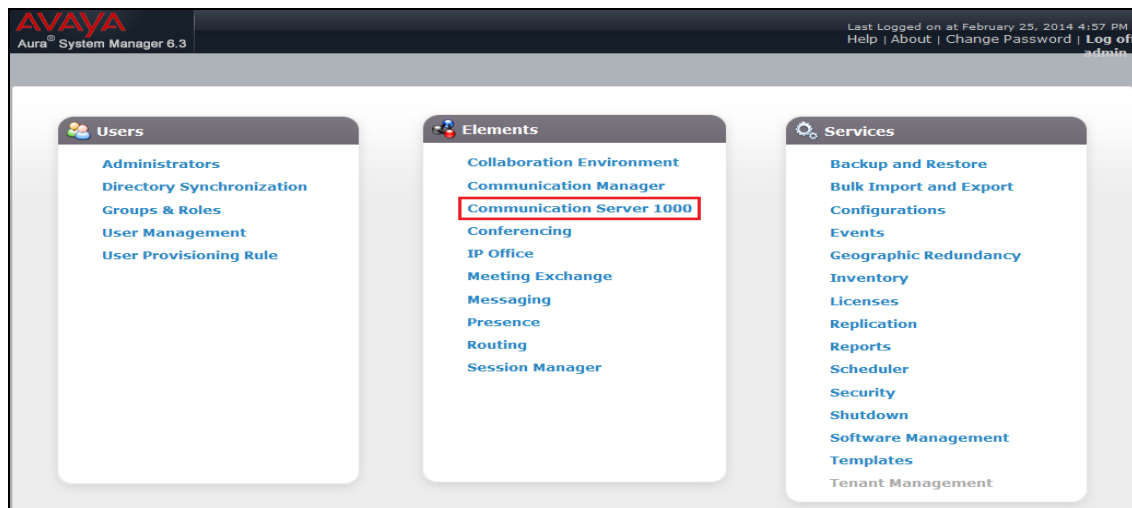
A two-way SIP Trunk was created between the CS1000 and Session Manager to carry traffic to and from the service provider respectively. Incoming calls flow from the Gamma network to the Avaya SBCE to the CS1000 via Session Manager. Incoming calls to the CS1000 may undergo call treatments such as incoming 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 via Session Manager for egress to the Gamma 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 11**.

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 is integrated to Avaya Aura® System Manager, however it still can use as standalone UCM, in the compliance test, UCM is accessed via System Manager. The screen below shows the System Manager home page with Communication Server 1000 entry in the Elements table. Click on the Communication Server 1000 to access to CS1000 UCM, the UCM webpage will be opened in the new 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.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar contains a navigation menu with categories like Network, CS 1000 Services, User Services, and Security. The main content area displays the 'Elements' list. At the top, it shows 'Host Name: 10.33.10.24' and 'User Name: admin'. Below this, there's a search bar with 'Search' and 'Reset' buttons. A table lists the elements:

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

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

The screenshot shows the CS1000 Element Manager System Overview page. The left sidebar contains a navigation menu with categories like UCM Network Services, Home, Links, System, Customers, and Routes and Trunks. The main content area displays the 'System Overview' page. At the top, it shows 'Managing: 10.97.90' and 'Username: admin'. Below this, there's a table with system details:

IP Address	Type	Version	Release
10.97.90	Avaya Communication Server 1000E CPPM Linux	4121	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.

AVAYA CS1000 Element Manager Help | Logout

Managing: 10.10.97.90 Username: admin
System » IP Network » IP Telephony Nodes

IP Telephony Nodes
Click the Node ID to view or edit its properties.

Buttons: Add... Import... Export... Delete Print | Ref

Node ID	Components	Enabled Applications	ELAN IP	Node/TLAN IPv4	Node/TLAN IPv6	Status
2000	1	LTPS, Gateway (SIPGw)	-	10.10.97.168	-	Synchronized
2001	1	LTPS, Gateway (SIPGw)	-	10.10.97.170	-	Synchronized
2003	1	SIP Line, LTPS, Gateway (SIPGw)	-	10.10.97.158	-	Synchronized
2004	1	SIP Line, LTPS, PD, Gateway (SIPGw)	-	10.10.97.190	-	Synchronized
2005	1	SIP Line	-	10.10.97.188	-	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 Gamma. The three highlighted areas in the screen shot below will be configured in the following sections.

AVAYA CS1000 Element Manager Help | Logout

Managing: 10.10.97.90 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 Alternative 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 **Quality of Service (QoS)** link in 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 **Save** button (not shown).

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation menu with options like UCM Network Services, Home, Links, System, Alarms, Maintenance, Core Equipment, Peripheral Equipment, IP Network, Nodes: Servers, Media Cards, Maintenance and Reports, Media Gateways, Zones, Host and Route Tables, and Network Address Translation. The main content area displays the 'Node ID: 2001 - Quality of Service (QoS)' configuration page. The page title is 'Node ID: 2001 - Quality of Service (QoS)'. Below the title, there is a section for 'Diffserv Codepoint (DSCP)'. This section contains several configuration options: 'Enable Avaya automatic QoS' (unchecked), 'Control packets' (20, range 0-63), 'Voice packets' (60, range 0-63), 'VLAN tagging' (unchecked), '802.1Q support' (unchecked), and '802.1Q bits value (802.1P)' (6, range 0-7). A red box highlights the 'Enable Avaya automatic QoS' checkbox and the 'Control packets' and 'Voice packets' input fields.

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 steps.

- 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**. Gamma supports voice codec G.711 and G.729, payload size 20 ms, with Voice Activity Detection (VAD) disabled. The following screenshot shows appropriated voice codec profile configured on the CS1000.

AVAYA CS1000 Element Manager

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

General | Voice Codes | Fax

Voice Codes

Codec G711: ☒ Enabled (required)

Voice payload size: 20 (milliseconds per frame)

Voice payout (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, Gamma supports G.711 codec as default and also supports T.38. The following screenshot shows **Modem/Faxpass-through** is selected for Node **2001**, this enables G.711 codec to be used for fax call between the CS1000 and Gamma. **Note:** The **V.21 Fax tone detection** should be checked to support **T.38 fax**.

AVAYA CS1000 Element Manager

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

General | Voice Codes | Fax

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 synchronizes 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 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).

Gamma supports voice codec G.711 and G.729, payload size 20 ms, with VAD disabled. The screenshot below shows appropriated codec profile configured for Media Gateways.

The screenshot shows the AVAYA CS1000 Element Manager interface. On the left is a navigation menu with 'Media Gateways' highlighted. The main area displays configuration for two codecs: G711 and G729A. For each codec, the 'Select' checkbox is checked. The 'Voice payload size' is set to 20 (ms/frame). The 'Voice playout (jitter buffer) nominal delay' is 40, and the 'maximum delay' is 80. Red text below these settings states 'Modifications may cause changes to dependent settings'. The 'VAD' checkbox is unchecked for both codecs.

For Fax over IP, Gamma supports G.711 codec as default and also does 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 Gamma. **Note:** The **Enable V.21 FAX tone detection** should be checked to enable T.38 fax capability on the Media Gateway, to disable T.38 fax call uncheck this check box.

The screenshot shows the AVAYA CS1000 Element Manager interface with the 'Media Gateways' menu item selected. The main area displays fax configuration settings. The 'Remove DTMF delay (squelch DTMF from TDM to IP)' checkbox is checked. The 'Enable modem/fax pass through mode' and 'Enable V.21 FAX tone detection' checkboxes are both checked and highlighted with a red box. Other settings include 'Fax TCF method' set to 2, 'FAX maximum rate' set to 14400 (bps), 'FAX playout nominal delay' set to 100 (0 - 300 milliseconds), 'FAX no activity timeout' set to 20 (10 - 32000 milliseconds), and 'FAX packet size' set to 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.

Gamma 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 both voice and fax calls.

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

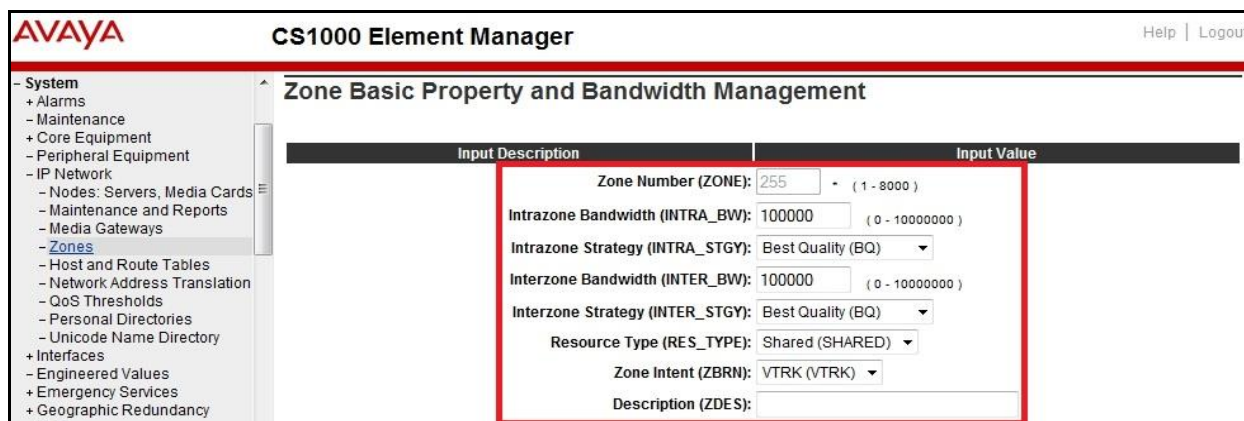
To create a MO zone **10** for VGW and IP phone, select **IP Network** → **Zones** from the left pane then configure as following:

- 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).

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).



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

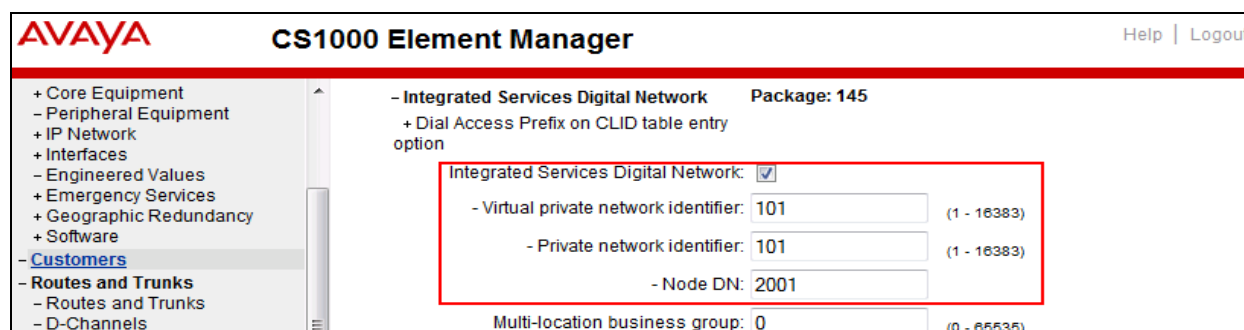
This section describes the steps for establishing a SIP Trunk between the CS1000 SIP Signaling Gateway (SSG) to Session Manager.

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**.



Input Description	Input Value
Integrated Services Digital Network:	<input checked="" type="checkbox"/>
- Virtual private network identifier:	101 (1 - 16383)
- Private network identifier:	101 (1 - 16383)
- Node DN:	2001
Multi-location business group:	0 (0 - 65535)

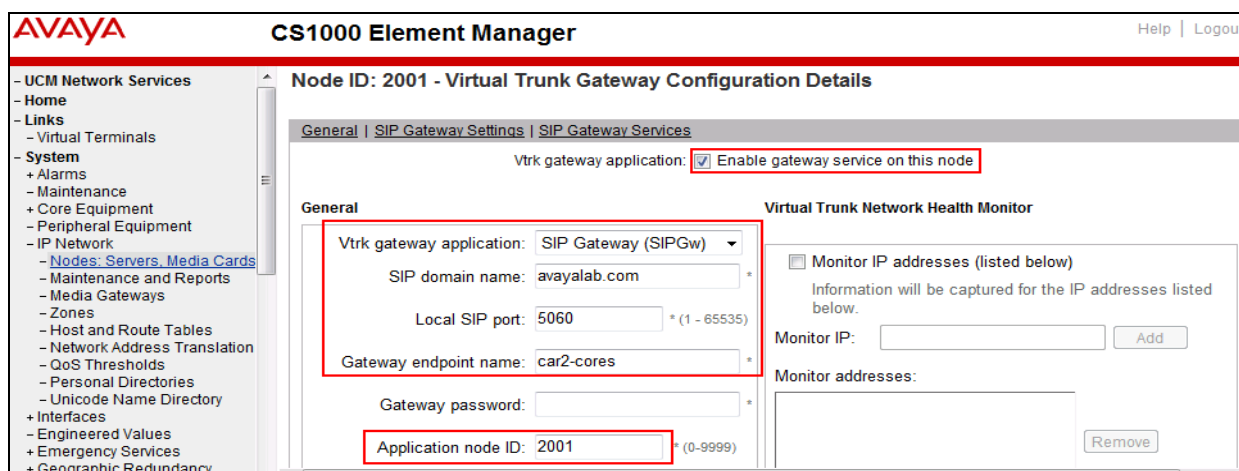
Retain the default values for all remaining fields. Scroll down to the bottom of the screen then click **Save** button (not shown).

5.5.2. Administer SIP Trunk Gateway to the Avaya Aura® Session Manager

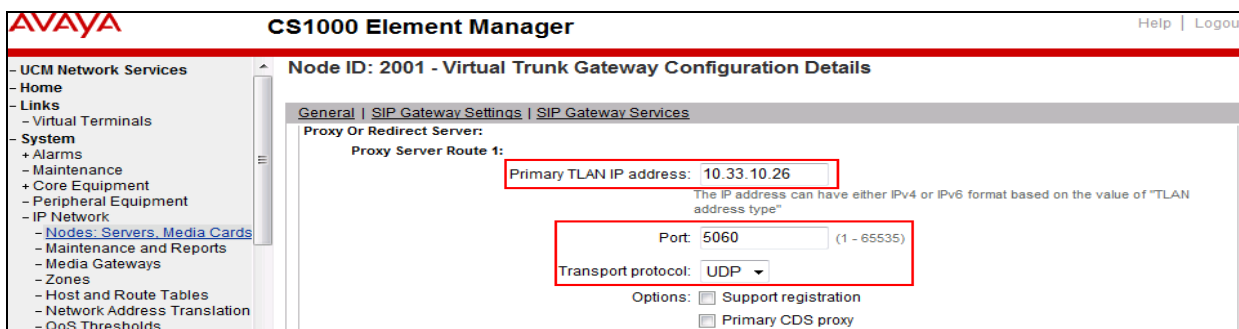
To configure SIP Trunk Gateway, select **IP Network → Nodes: Servers, Media Cards** configuration from the left pane, and in the **IP Telephony Nodes** screen, select the **Node ID 2001**. The **Node Details** screen is displayed as shown in **Section 5.2.1**.

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**.



Click on the **SIP Gateway Settings** tab, under **Proxy or Redirect Server**, enter the IP address 10.33.10.26 of Session Manager as shown in the screenshot below, and retain the default values for the remaining fields.



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 Gamma.

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.

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.

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
 - Digital Trunk Interface
- Dialing and Numbering Plans
 - Electronic Switched Network
 - Flexible Code Restriction
 - Incoming Digit Translation
- Phones
 - Templates
 - Reports
 - Views

D-Channels 101 Property Configuration

- Basic Configuration

Input Description	Input Value
Action Device And Number (ADAN):	DCH
D channel Card Type :	DCIP
Designator:	TelNet
Recovery to Primary:	<input type="checkbox"/>
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:	<input type="button" value="more PRI"/>
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.

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
 - Digital Trunk Interface
- Dialing and Numbering Plans
 - Electronic Switched Network
 - Flexible Code Restriction
 - Incoming Digit Translation
- Phones
 - Templates
 - Reports
 - Views
 - Lists
 - Properties
 - Migration

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 (QMWIO) ☐

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: 97.90 Username: admin
System » Core Equipment » Superloops

Superloops

[Add...](#) [Delete](#) [Refresh](#)

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 **Feature 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 screenshot below. The CS1000 has been pre-configured with music route **51**.

AVAYA CS1000 Element Manager

Help | Logout

- UCM Network Services
- Home
- Links
- Virtual Terminals
+ System
- Customers
- Routes and Trunks
- Routes and Trunks

- 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 the **Customer 1**. Click **Add route** button as shown in the screenshot below.

Customer	Total routes	Total trunks	Action
+ 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 enterprise network. For this compliance test, the default value of 0 ms is used.
- **Calling number dialling plan (CNDP):** UnKnown (UKWN).

AVAYA
CS1000 Element Manager
Help | Logout

- UCM Network Services
- Home
- Links
 - Virtual Terminals
- + System
- 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
 - Properties
 - Migration
- Tools
 - + Backup and Restore
 - Date and Time
 - + Logs and reports
- Security
 - + Passwords
 - + Policies
 - + Login Options

- 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 dialling 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 screenshot below. The IDC is discussed in **Section 5.6.5**.

AVAYA CS1000 Element Manager Help | Logout

- UCM Network Services
- Home
- Links
- Virtual Terminals
+ System
- 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

- 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.

AVAYA CS1000 Element Manager Help | Logout

- UCM Network Services
- Home
- Links
- Virtual Terminals
+ System
- Customers
- Routes and Trunks
- Routes and Trunks
- D-Channels

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.

The screenshot shows the AVAYA CS1000 Element Manager interface. On the left is a navigation menu with options like UCM Network Services, Home, Links, Virtual Terminals, System, Customers, Routes and Trunks (selected), D-Channels, Digital Trunk Interface, and Dialing and Numbering Plans. The main area is titled 'Routes and Trunks' and contains a table with two rows: '+ Customer: 0' and '- Customer: 1'. The '- Customer: 1' row is expanded to show a table of routes. The first route is '+ Route: 51' with Type: MUS and Description: MUS. The second route is '+ Route: 101' with Type: TIE and Description: SIPTRK. Both routes have an 'Add trunk' button next to them. The 'Add trunk' button for Route 101 is highlighted with a red box.

Customer	Total routes	Total trunks	Action
+ Customer: 0	2	32	Add route
- Customer: 1	3	66	Add route

Route	Type	Description	Action
+ Route: 51	MUS	MUS	Edit Add trunk
+ Route: 101	TIE	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). The following values were entered for specified fields 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.

The screenshot shows the AVAYA CS1000 Element Manager interface for 'Customer 1, Route 101, Trunk 1 Property Configuration'. The left navigation menu is the same as the previous screenshot. The main area is titled 'Customer 1, Route 101, Trunk 1 Property Configuration' and contains a 'Basic Configuration' section. The fields in this section are: 'Auto increment member number' (checked), 'Trunk data block' (IPTI), 'Terminal number' (100 0 01 00), 'Designator field for trunk' (SIPTRK), 'Extended trunk' (VTRK), 'Member number' (1), 'Level 3 Signaling' (dropdown), 'Card density' (8D), 'Start arrangement Incoming' (Immediate (IMM)), 'Start arrangement Outgoing' (Immediate (IMM)), 'Trunk group access restriction' (1), and 'Channel ID for this trunk' (1). The 'Class of Service' field is at the bottom with an 'Edit' button. The 'Trunk data block', 'Designator field for trunk', 'Extended trunk', 'Member number', and 'Start arrangement Incoming' fields are highlighted with a red box.

Basic Configuration

Auto increment member number: ☒

Trunk data block:

Terminal number:

Designator field for trunk:

Extended trunk:

Member number: *

Level 3 Signaling:

Card density:

Start arrangement Incoming:

Start arrangement Outgoing:

Trunk group access restriction:

Channel ID for this trunk:

Class of Service:

The Media Security (sRTP) has to be disabled at the trunk level by editing the **Class of Service** (CLS) at the bottom of the basic trunk configuration page. Click **Edit** button to configure (not shown). For **Media Security**, 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).

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 a prefix what was assigned by the service provider, in this case it is digits 122XXX. 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 the security reason the last 3 digits is hidden by XXX but in the real deployment it should be entered with full 6 digits, e.g. 248123.
- **Home Location Code:** Input prefix that was assigned by the service provider, in this case it is 6 digits 122XXX. 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 a prefix that was assigned by the service provider, in this case it is 6 digits 122XXX. 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**.
- **Calling Party Name Display:** Uncheck the **Roman characters** field.
- Click **Save** button (not shown).

AVAYA CS1000 Element Manager Help | Logout

Edit Calling Line Identification 0

General Properties

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

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

Home Location Code: (1-7 digits)

Local Steering Code: (1-7 digits)

Use DN as DID:

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: ☐

CPND Name:

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.

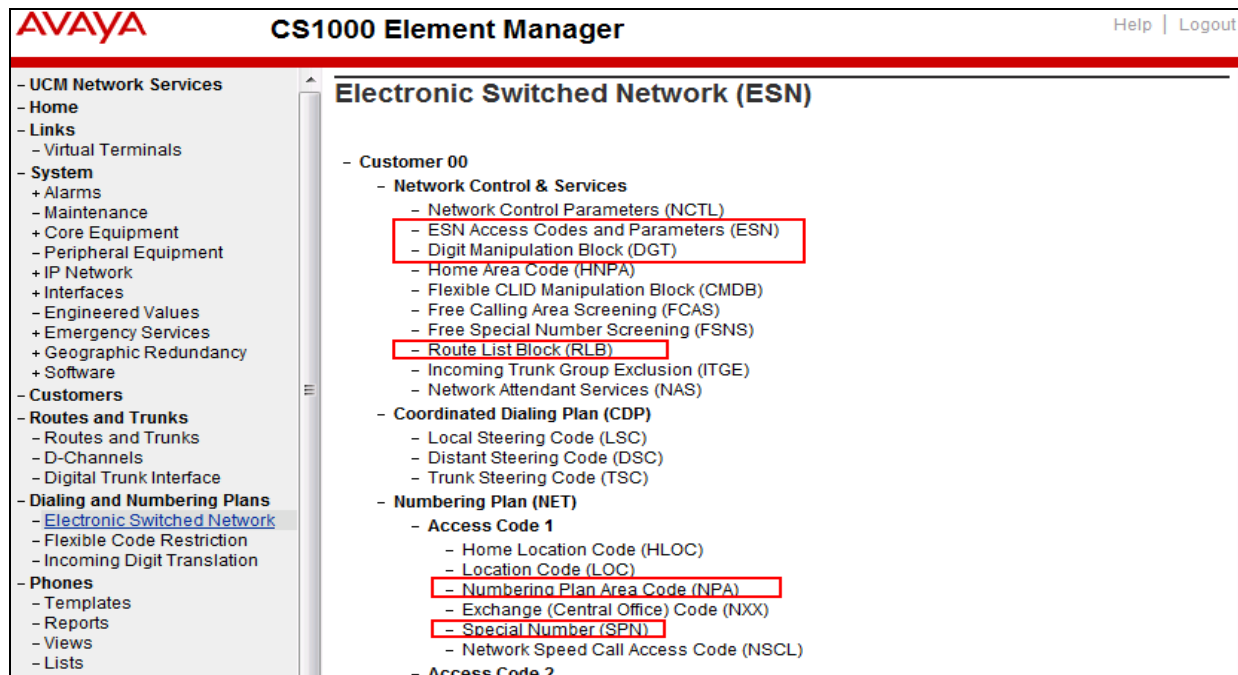
```
>ld 15
CDB000
MEM AVAIL: (U/P): 35600176      USED U P: 8325631 954062      TOT: 44879869
DISK SPACE NEEDED: 1722 KBYTES
REQ: chg
TYPE: net

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

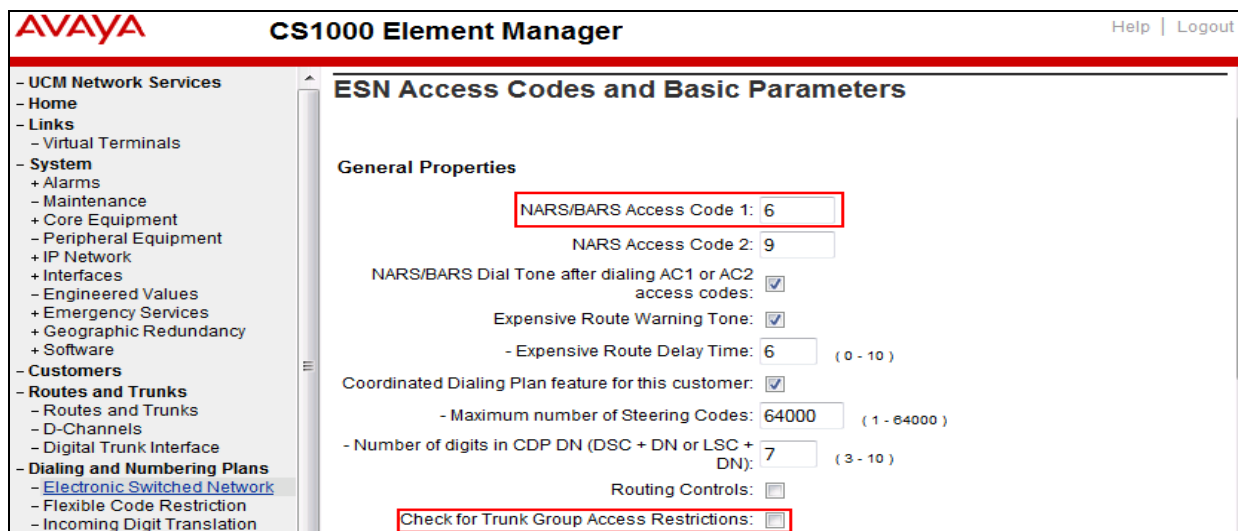
5.6. Administer Dialing Plans

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.



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).



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 screenshot below shows **DMI 1** is created with following values.

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

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

Managing: 197.90 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)

Submit

Refresh

Delete

Cancel

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**).

AVAYA CS1000 Element Manager Help | Logout

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 Gamma.

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 (DCNO) 0** was created. Detailed configuration of the DCNO is shown in screenshot below. The **Incoming Digits** can be added to map to the **Converted Digits** which would be the CS1000 DN. This DCNO has been assigned to Route 101 as shown in **Section 5.5.6**.

In the following configuration, incoming calls from PSTN with prefix **4412XXXXX55** will be translated to local CS1000 DN **46XX**. The prefix 44 is the country code of England and the DDI rang number is from 12xxxxxx55 to 12xxxxxx59.

	Incoming Digits ▲	Converted Digits	CPND Name	CPND language
18 <input checked="" type="radio"/>	4412 55	4685		
19 <input type="radio"/>	4412 56	4686		
20 <input type="radio"/>	4412 57	4689		
21 <input type="radio"/>	4412 58	4650		
22 <input type="radio"/>	4412 59	4699		

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 assistant, **011** prefix for international call, **1** for national long distance call, **411** for directory assistant 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 this 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 this defined by the special number:** NONE.
- **Route list index:** 101, created in Section 5.6.4.

Special Number: 999

- **Flexible length:** 3.
- **Type of call this defined by the special number:** NONE.
- **Route list index:** 101, created in Section 5.6.4.

AVAYA CS1000 Element Manager

Special Number List

Please enter a Special Number to Add

Special Number	Flexible length	International dialing plan	Type of call that is defined by the special number	Route list index
Special Number -- 0	0	NO	NONE	101
Special Number -- 1	0	NO	NONE	101
Special Number -- 999	3	NO	NONE	101

6. Configure Avaya Aura® Session Manager

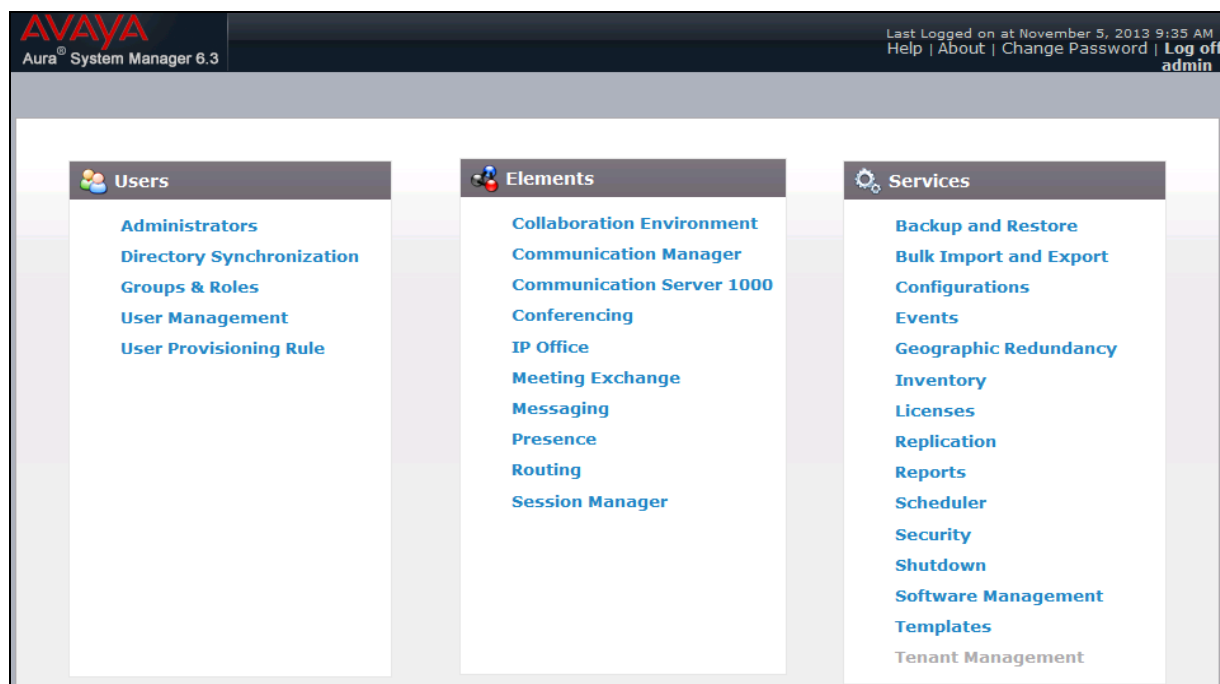
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain.
- Logical/physical Location that can be occupied by SIP Entities.
- SIP Entities corresponding to the CS1000, Session Manager and the Avaya SBCE.
- Entity Links, which define the SIP Trunk parameters used by Session Manager when routing calls to/from SIP Entities.
- Routing Policies, which control call routing between the SIP Entities.
- Dial Patterns, which govern to which SIP Entity a call is routed.
- Session Manager, corresponding to the Session Manager server to be managed by System Manager.

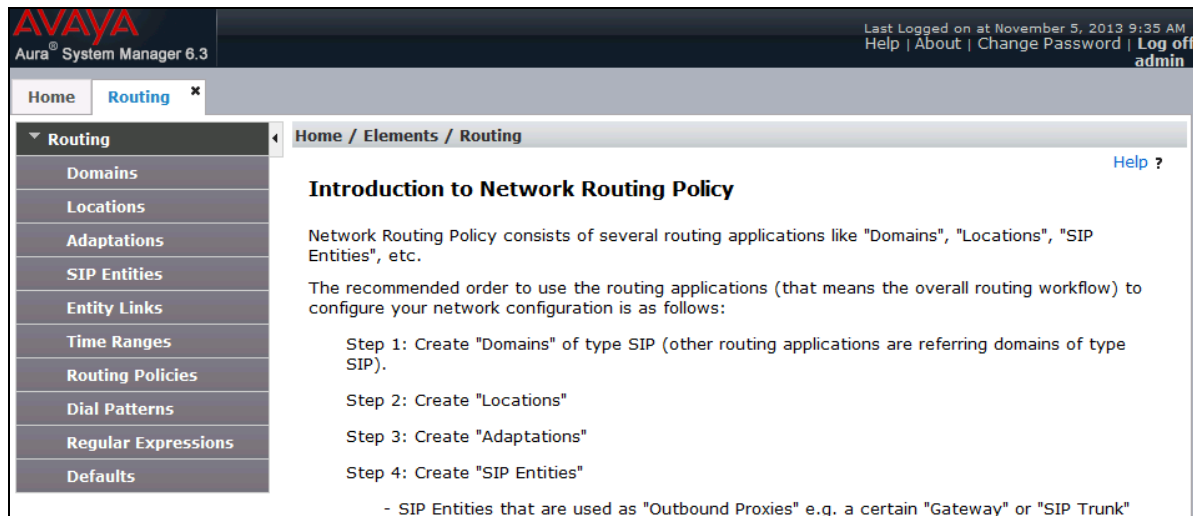
It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, Location, SIP entities, and Session Manager itself. However, each item should be reviewed to verify the configuration.

6.1. Avaya Aura® System Manager Login and Navigation

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



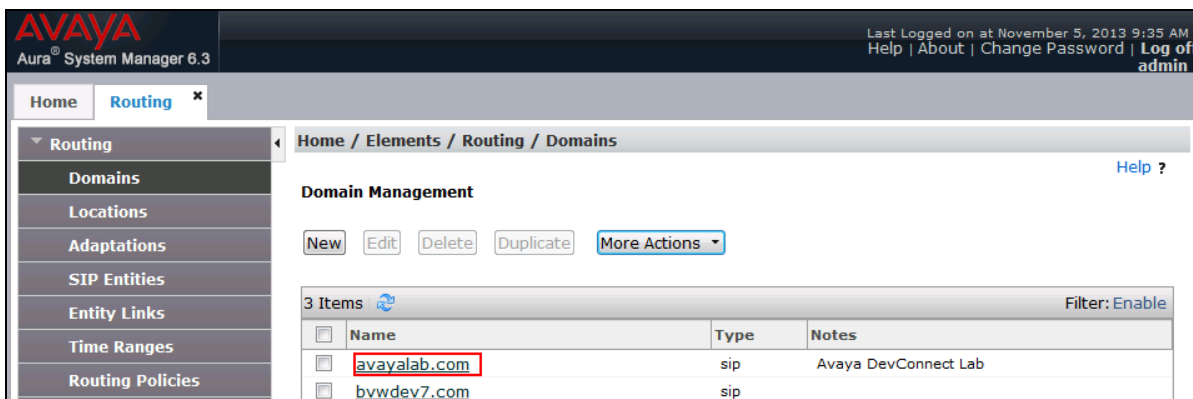
Most of the configuration items are performed in the Routing Element. Click on **Routing** in the **Elements** column to bring up the **Introduction to Network Routing Policy** screen. The navigation tree displayed in the left pane will be referenced in subsequent sections to navigate to items requiring configuration.



6.2. Specify SIP Domain

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

The following screen shows the list of configured SIP domains. The domain **avayalab.com** is an enterprise private SIP domain, which is defined to route incoming calls to the CS1000. Incoming calls were received with service provider public IP address **88.xx.xxx.201** which will be translated by the Avaya SBCE to **avayalab.com** to route to Session Manager. The enterprise SIP domain **avayalab.com** will be translated by the Avaya SBCE to **88.xx.xxx.201** to route to Gamma networks.



6.3. Add Location

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

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

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

In the **Location Pattern** section, click **Add** and enter the following values:

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

Displayed below are the screenshots for location **Belleville** which includes all equipment on the **10.10.97.***, **10.10.98.*** and **10.33.*** subnets including the CS1000, Session Manager, Avaya SBCE and IP phones. Click **Commit** to save.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The top navigation bar includes the Avaya logo, 'Aura System Manager 6.3', and a user status bar indicating 'Last Logged on at November 5, 2013 9:35 AM' with links for 'Help', 'About', 'Change Password', and 'Log off admin'. The left-hand navigation pane shows a tree structure with 'Routing' expanded, containing sub-items like 'Domains', 'Locations', 'Adaptations', 'SIP Entities', 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Regular Expressions', and 'Defaults'. The main content area is titled 'Home / Elements / Routing / Locations' and features a 'Location Details' section with 'Commit' and 'Cancel' buttons. The 'General' section contains a red-bordered box around the 'Name' field (set to 'Belleville') and the 'Notes' field (set to 'GSSCP Belleville'). Below this is the 'Dial Plan Transparency in Survivable Mode' section with an 'Enabled' checkbox and fields for 'Listed Directory Number' and 'Associated CM SIP Entity'. The 'Overall Managed Bandwidth' section includes 'Managed Bandwidth Units' (set to 'Kbit/sec'), 'Total Bandwidth' (10000000), 'Multimedia Bandwidth' (10000000), and a checked checkbox for 'Audio Calls Can Take Multimedia Bandwidth'. The 'Per-Call Bandwidth Parameters' section includes fields for 'Maximum Multimedia Bandwidth (Intra-Location)' (2000 Kbit/Sec), 'Maximum Multimedia Bandwidth (Inter-Location)' (2000 Kbit/Sec), '* Minimum Multimedia Bandwidth' (64 Kbit/Sec), and '* Default Audio Bandwidth' (80 Kbit/Sec).

Continued from the screenshot above, the Location Pattern section is displayed as the screen below.

IP Address Pattern	Notes
* 10.33.*	
* 10.10.97.*	
* 10.10.98.*	

6.4. Add Adaptations

There is an adaptation that needs to be created for the Avaya SBCE SIP entity in **Section 6.5** below. The adaptation is used to remove MIME part from SIP INVITE message of outbound calls.

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

The screen below shows the adaptation **Remove-MIME** that will be applied in Avaya SBCE SIP entity with **Module Name** selected as “DigitConversionAdapter”, **Module Parameter Type** selected as “Name-Value-Parameter”, and “**MIME**” is set to “no” in the table.

Adaptation Details

General

* Adaptation Name: Remove-MIME

Module Name: DigitConversionAdapter

Module Parameter Type: Name-Value Parameter

Name	Value
MIME	no

Egress URI Parameters:

Notes:

6.5. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it which includes the CS1000 and the Avaya SBCE. Navigate to **Routing → SIP Entities** in the left navigation pane and click on **New** button in the right pane (not shown).

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

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Select **Session Manager** for Session Manager and **Other** for the CS1000 and the Avaya SBCE.
- **Location:** Select the Location defined previously.
- **Time Zone:** Select the time zone for the Location above.

The following screen shows the addition of SIP Entity for Session Manager. The IP address of Session Manager signaling interface is entered for **FQDN or IP Address**. The **SIP Link Monitoring** is kept as default **Use Session Manager Configuration**.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left navigation pane has 'Routing' selected, and the 'SIP Entities' sub-menu is active. The main content area is titled 'SIP Entity Details' and 'General'. The following fields are highlighted with red boxes:

- Name:** SM63
- FQDN or IP Address:** 10.33.10.26
- Type:** Session Manager (dropdown)
- Notes:** SM R6.3
- Location:** Belleville (dropdown)
- Time Zone:** America/Toronto (dropdown)
- SIP Link Monitoring:** Use Session Manager Configuration (dropdown)

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

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

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

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

The compliance testing used **Port** entry **UDP/5060** connecting to the CS1000 for the internal enterprise calls. The **Port** entry **UDP/5060** is for connecting to the Avaya SBCE for the external PSTN calls.

Port

TCP Failover port:

TLS Failover port:

4 Items Filter: Enable

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

The following section shows the addition of SIP Entity **car2-cores** for the CS1000. The **FQDN or IP Address** field is set to the IP address of the CS1000 Node IP as **10.10.97.170**, as obtained in **Section 5.2.1**. Select **Type** is **Other**, and select “**Belleville**” as defined in **Section 6.3** in the **Location** field. In the compliance testing, a single SIP Entity was created for both incoming and outgoing calls in appropriate to the SIP Trunk created on the CS1000 in **Section 5.5**. The **SIP Link Monitoring** was set to **Use Session Manager Configuration** as default. This setting allows Session Manager to periodically send OPTIONS heartbeat to check for the status of the SIP Trunk.

AVAYA
Aura® System Manager 6.3

Last Logged on at April 21, 2014 1:54 PM
Help | About | Change Password | Log off admin

Home **Routing**

Home / Elements / Routing / SIP Entities

SIP Entity Details [Help ?](#)

General

* Name: car2-cores

* FQDN or IP Address: 10.10.97.170

Type: Other

Notes: CS1000 Car2-Cores CPPM

Adaptation:

Location: Belleville

Time Zone: America/Toronto

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

Credential name:

Call Detail Recording: none

CommProfile Type Preference:

Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

The following screens show the addition of SIP Entities **SBCE62** for the Avaya SBCE. The **FQDN or IP Address** field is set to the IP address of the private network interfaces as **10.10.98.22**. Select “**Other**” in the **Type** field, “**Remove-MIME**” in the **Adaptation** field as defined in **Section 6.4**, and “**Belleville**” in the **Location** field. The **SIP Link Monitoring** was set to **Link Monitoring Enabled**.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left navigation pane is expanded to 'Routing', and the 'SIP Entities' sub-menu is selected. The main pane displays the 'SIP Entity Details' form for 'SBCE62'. The form includes the following fields and values:

- Name:** SBCE62
- * FQDN or IP Address:** 10.10.98.22
- Type:** Other
- Notes:** SIP Entity link for SBCE62
- Adaptation:** Remove-MIME
- Location:** Belleville
- Time Zone:** America/Toronto
- * SIP Timer B/F (in seconds):** 4
- Credential name:** (empty)
- Call Detail Recording:** none
- CommProfile Type Preference:** (empty)
- Loop Detection Mode:** Off
- SIP Link Monitoring:** Link Monitoring Enabled

6.6. Add Entity Links

A SIP Trunk between Session Manager and a telephony system is described by an Entity Link. From Session Manager to the CS1000, one Entity Link was created for internal enterprise traffics. Session Manager will also have one Entity Link to the Avaya SBCE for external service provider traffics.

To add an Entity Link, navigate to **Routing → Entity Links** in the left navigation pane and click on the **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For the CS1000, this must match the SIP Trunk configuration in **Section 5.5**.
- **SIP Entity 2:** Select the name of the other system. For the CS1000, select the SIP Entities **car2-cores** as defined in **Section 5**. For the Avaya SBCE, select the SIP Entities **SBCE62** as defined in **Section 6.55**.

- **Port:** Port number on which the other system receives SIP requests from Session Manager. For the CS1000, this must match the SIP Trunk configuration in **Section 5.5**.
- **Connection Policy:** Select **Trusted**. **Note:** If **Trusted** is not selected, all calls from the associated SIP Entity specified in **Section 6.55** will be requested to process authentication.

Click **Commit** to save (not shown).

The following screenshots illustrate the Entity Link from Session Manager to the CS1000 and also to the Avaya SBCE.

Entity Links between Session Manager and the CS1000 for enterprise calls on **Port** entry use **UDP/5060**:

The screenshot shows the 'Entity Links' configuration interface. At the top, there is a section 'Override Port & Transport with DNS SRV:' with an unchecked checkbox. Below this are 'Add' and 'Remove' buttons. A table lists one item with the following details:

	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
<input type="checkbox"/>	SM63	UDP	* 5060	car2-cores	* 5060	trusted	<input type="checkbox"/>

Below the table, it says 'Select : All, None'. The entire row in the table is highlighted with a red rectangle.

Entity Links between Session Manager and the Avaya SBCE for service provider calls on **Port** entry use **UDP/5060**:

The screenshot shows the 'Entity Links' configuration interface, similar to the previous one. It shows a link between SM63 and SBCE62:

	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service
<input type="checkbox"/>	SM63	UDP	* 5060	SBCE62	* 5060	trusted	<input type="checkbox"/>

Below the table, it says 'Select : All, None'. The entire row in the table is highlighted with a red rectangle.

6.7. Add Routing Policies

Routing Policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 5**. A separate Routing Policy was added to route incoming calls to the CS1000 and outgoing calls to the Avaya SBCE.

To add a Routing Policy, navigate to **Routing → Routing Policies** in the left navigation pane and click on the **New** button in the right pane (not shown). The following screen is displayed then fills in the following:

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

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

In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Select the appropriate SIP Entity to which this routing policy applies and click **Select**. The selected SIP Entity displays on the **Routing Policy Details** page as shown below. Use default values for remaining fields. Click **Commit** to save.

The following screens show the Routing Policies used in the compliance testing.

Routing Policy **Inbound_To_car2_cores** for incoming calls to the CS1000:

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left navigation pane is expanded to 'Routing', and the 'Routing Policies' sub-item is selected. The main content area displays the 'Routing Policy Details' for the policy 'Inbound_To_car2_cores'. The 'General' section contains the following fields:

- Name:** Inbound_To_car2_cores (highlighted with a red box)
- Disabled:** ☐
- Retries:** 0
- Notes:** Inbound Route to CS1K76 cores fr

The 'SIP Entity as Destination' section has a 'Select' button. Below it is a table listing available SIP entities:

Name	FQDN or IP Address	Type	Notes
car2-cores (highlighted with a red box)	10.10.97.170 (highlighted with a red box)	Other	CS1K Car2-Cors CPPM card

At the top right of the page, there are links for 'Help ?', 'Commit', and 'Cancel'. The top status bar indicates the user is logged in as 'admin' and the last login was on November 5, 2013 at 9:35 AM.

Routing Policy **Outbound_To_Gamma** for outgoing calls to the Avaya SBCE:

AVAYA
Aura® System Manager 6.3

Last Logged on at March 28, 2014 2:59 PM
Help | About | Change Password | Log off admin

Home Routing

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit Cancel

General

* Name: Outbound_To_Gamma

Disabled: ☐

* Retries: 0

Notes: Outbound route to SCBE62

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
SBCE62	10.10.98.22	Other	SIP Entity link for SBCE62

6.8. Add Dial Patterns

Dial Patterns are needed to route specific calls through Session Manager. For the compliance testing, Dial Patterns were needed to route calls from the CS1000 to Gamma and vice versa. Dial Patterns define which Routing Policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a Dial Pattern, navigate to **Routing** → **Dial Patterns** in the left navigation pane and click on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

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

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

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

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

Two examples of the dial patterns used for the compliance testing are shown below, one for outgoing calls from the enterprise to the PSTN and one for incoming calls from the PSTN to the enterprise. Other outgoing dial patterns e.g. **00** international calls, **100** operator calls, etc., were similarly defined.

The first example shows a Dial Pattern for incoming calls that 12-digit DID numbers start with

44 which is UK country code to SIP domain **avayalab.com** (after being translated by the Avaya SBCE from the service provider public IP address (88.xxx.xxx.201). The Dial Pattern uses the Route Policy **Inbound_To_car2_cores** as defined in **Section 6.77**. These DID numbers are assigned to the enterprise by Gamma.

The screenshot shows the 'Dial Pattern Details' page in the Avaya Aura System Manager 6.3. The 'General' tab is active. The 'Pattern' field is set to '44', with 'Min' and 'Max' both set to '12'. The 'SIP Domain' is set to 'avayalab.com'. The 'Notes' field contains '44 - UK country code'. The 'Routing Policies' table below shows one item: 'Belleville' with 'Routing Policy Name' 'Inbound_To_car2_cores' and 'Routing Policy Destination' 'car2-cores'.

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
Belleville	GSSCP Belleville	Inbound_To_car2_cores	0	<input type="checkbox"/>	car2-cores	Inbound to CS1000 cores

The second example shows the Dial Pattern for outgoing calls that 13-digit dialed numbers begin with digit **0**. The Dial Pattern uses Routing Policy **Outbound_To_Gamma** as defined in **Section 7** to route outgoing calls to the Avaya SBCE.

The screenshot shows the 'Dial Pattern Details' page in the Avaya Aura System Manager 6.3. The 'General' tab is active. The 'Pattern' field is set to '0', with 'Min' set to '1' and 'Max' set to '13'. The 'SIP Domain' is set to 'avayalab.com'. The 'Notes' field is empty. The 'Routing Policies' table below shows one item: 'Belleville' with 'Routing Policy Name' 'Outbound_To_GAMMA' and 'Routing Policy Destination' 'SBCE62'.

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
Belleville	GSSCP Belleville	Outbound_To_GAMMA	0	<input type="checkbox"/>	SBCE62	Outbound route to SCBE62

6.9. Add Avaya Aura® Session Manager

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

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

- **SIP Entity Name:** Select the SIP Entity created for Session Manager.
- **Description:** Add a brief description (optional).
- **Management Access Point Host Name/IP:** Enter the IP address of the Session Manager management interface.

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

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

In **Monitoring** section, verify **Enable Monitoring** is checked.

Use default values for the remaining fields. Then click **Save** (not shown).

The screenshots below show Session Manager values.

AVAYA
Aura® System Manager 6.3

Last Logged on at November 5, 2013 10:19 AM
Help | About | Change Password | Log off admin

Home Session Manager

Session Manager Administration

Home / Elements / Session Manager / Session Manager Administration

View Session Manager

General | Security Module | NIC Bonding | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server | Expand All | Collapse All

General

SIP Entity Name SM63

Description

Management Access Point Host Name/IP 10.33.10.25

Direct Routing to Endpoints Enable

VMware Virtual Machine

Security Module

SIP Entity IP Address 10.33.10.26

Network Mask 255.255.255.0

Default Gateway 10.33.10.1

Call Control PHB 46

QOS Priority 6

Speed & Duplex Auto

VLAN ID

* SIP Firewall Configuration Rule Set for SM63

Monitoring

Enable Monitoring ☒

Proactive cycle time (secs) 900

Reactive cycle time (secs) 120

Number of Retries 1

7. 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. and Error! Reference source not found. in **Section 11**.

The compliance testing comprised the configuration of 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 Gamma:

- 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 Session Manager:

- 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

7.1. Log into Avaya Session Border Controller for Enterprise

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

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



AVAYA

Session Border Controller for Enterprise

Log In

Session expired, please sign in again.

Username:

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 ASBCE will appear as shown below.

Session Border Controller for Enterprise AVAYA

Dashboard

Administration
Backup/Restore
System Management
‣ Global Parameters
‣ Global Profiles
‣ SIP Cluster
‣ Domain Policies
‣ TLS Management
‣ Device Specific Settings

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

[Add](#)

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 AVAYA

System Management

Dashboard
Administration
Backup/Restore
System Management
‣ Global Parameters
‣ Global Profiles
‣ SIP Cluster
‣ Domain Policies
‣ TLS Management
‣ Device Specific Settings

Devices **Updates** **SSL VPN** **Licensing**

Device Name (Serial Number)	Management IP	Version	Status	
SBCE62 (PC331040089)	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.

System Information: SBCE62

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
----	-------------

7.2. Global Profiles

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

7.2.1. Uniform Resource Identifier (URI) Groups

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

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

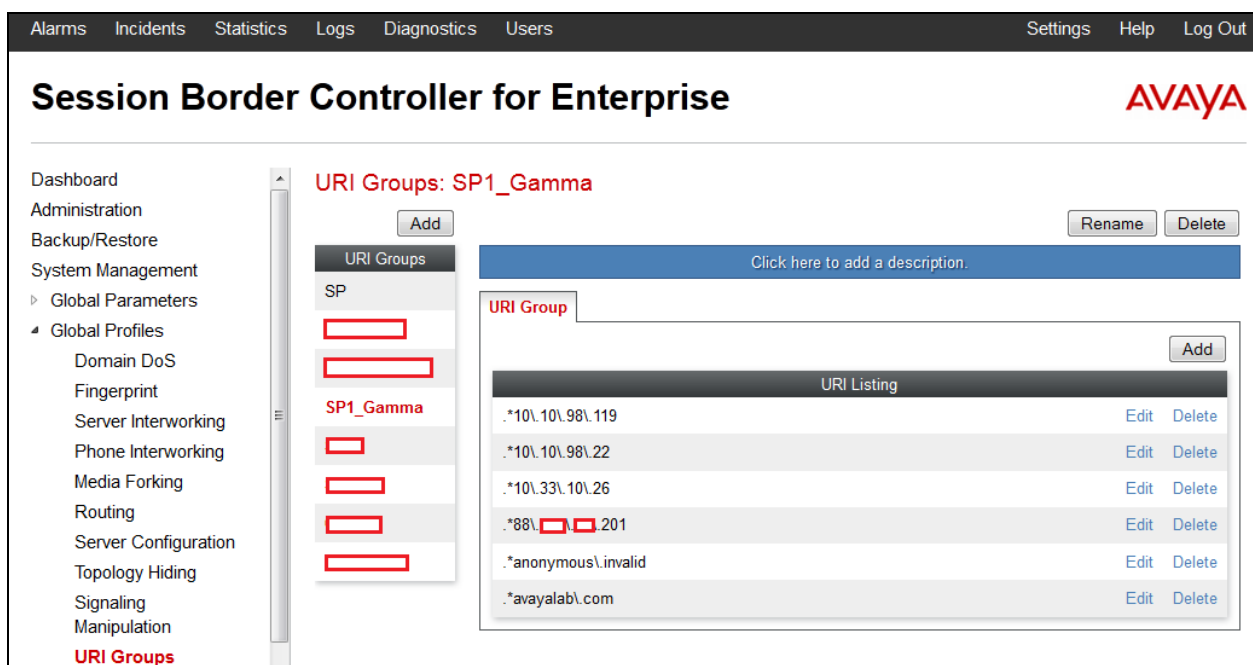
In the compliance testing, a URI Group named **SP1_Gamma** was added with following URI type **Regular Expression**:

- “***10\33\10\26**” – the IP addresses of URI-Host in OPTIONS heartbeat originated by Session Manager.

- “.*10\10\98\119” – the public IP address of ASBCE.
- “.*10\10\98\22” – the internal IP address of ASBCE.
- “.*88\xxx\xx\201” – 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 Gamma. If there is a match, the Avaya SBCE will apply the appropriate Routing profile (see **Section 7.2.2**) and Server Flow (see **Section 7.4.4**) to route incoming and outgoing calls to the right destination.

The screenshot below illustrates the URI listing for URI Group **SP1_Gamma**.



7.2.2. Routing Profiles

Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby as certain 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.

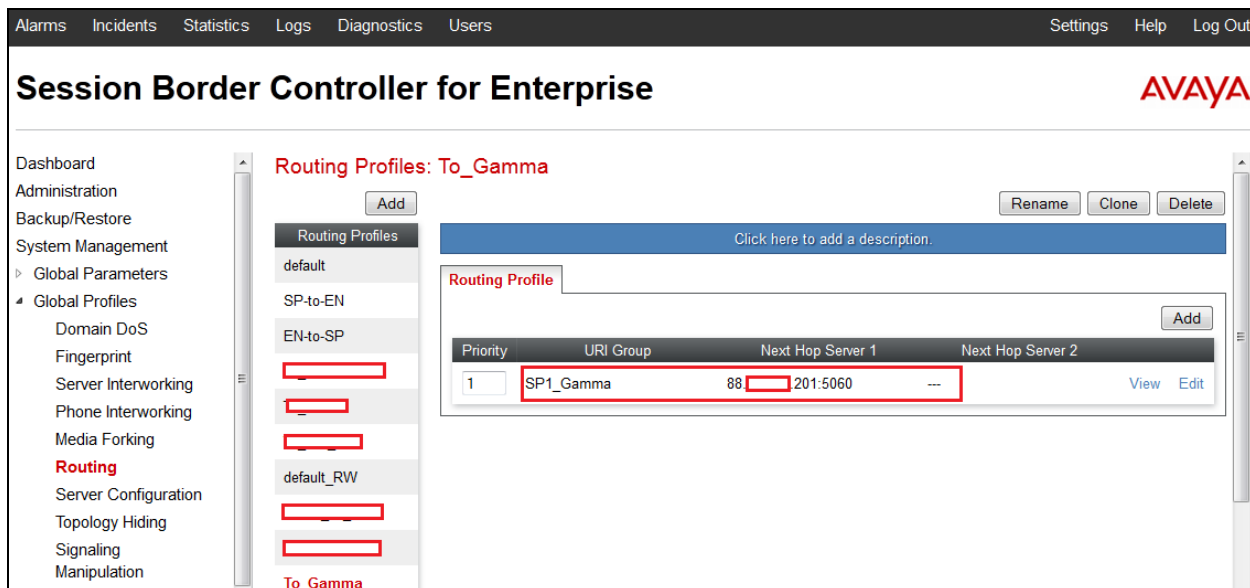
To create a Routing profile, select **System Management** → **Global Profiles** → **Routing** then click on the **Add** button.

In the compliance testing, a Routing profile **To_Gamma** was created to be used in conjunction with the Server Flow (see **Section 7.4.4**) defined for the CS1000. This entry is to route outgoing calls from the enterprise to Gamma.

In the opposite direction, a Routing profile **To_SM63_CAR276** was created to be used in conjunction with the Server Flow (see **Section 7.4.4**) defined for Gamma. This entry is to route incoming calls from Gamma to the enterprise.

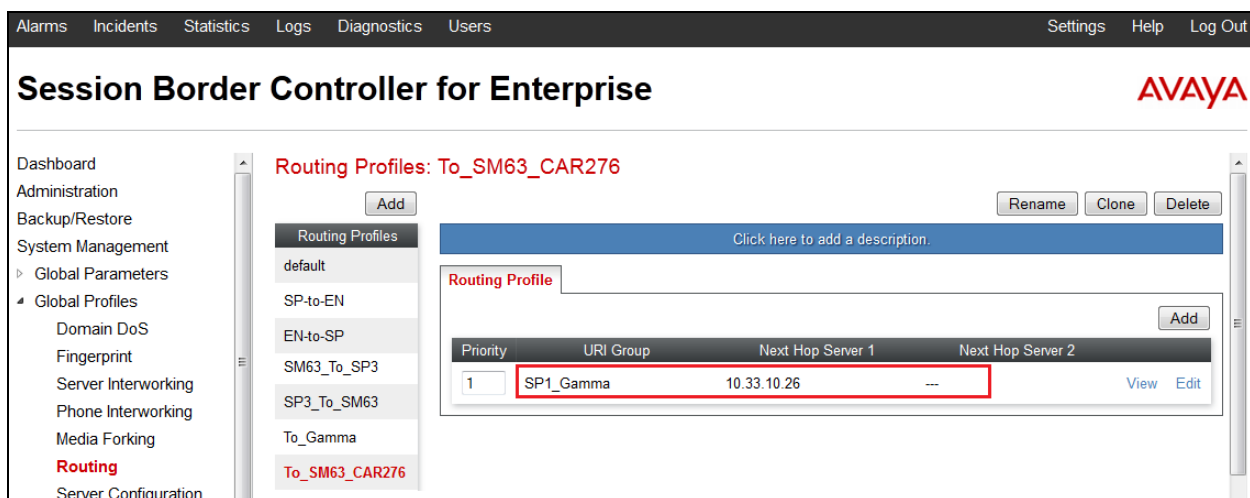
7.2.2.1 Routing Profile for Gamma

The screenshot below illustrates the **System Management → Global Profiles → Routing: To_Gamma**. If there is a match between the SIP domain in the “To” header with the URI Group **SP1_Gamma** defined in **Section 7.2.1**, the call will be routed to the **Next Hop Server 1** which is the proxy IP address of Gamma Trunk Server on port **5060**.



7.2.2.2 Routing Profile for Avaya Aura® Session Manager

The Routing Profile **To_SM63_CAR276** in the screenshot below was defined to route calls where the SIP domain in the “To” header matches the URI-Group **SP1_Gamma** defined in **Section 7.2.1**, to **Next Hop Server 1** which is the IP address of Session Manager on port 5060.



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

7.2.3.1 Topology Hiding Profile for Gamma

Topology Hiding profile **Topo_Gamma** was defined for outgoing calls to Gamma to:

- Mask URI-Host of the “Request-Line” and “To” headers with service provider public IP address **88.xxx.xx.201** to meet the requirements of Gamma.
- Change the “From” header added by the CS1000 with external IP address of ASBCE known to Gamma.

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_Gamma**

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left sidebar shows the navigation menu with 'Topology Hiding' selected under 'Global Profiles'. The main content area is titled 'Topology Hiding Profiles: Topo_Gamma' and includes an 'Add' button. Below this, a list of profiles shows 'Topo_Gamma' selected. The 'Topology Hiding' tab is active, displaying a table of SIP headers and their replacement values.

Header	Criteria	Replace Action	Overwrite Value
To	IP/Domain	Overwrite	88. [redacted] 201
SDP	IP/Domain	Auto	---
Referred-By	IP/Domain	Overwrite	10.10.98.119
Record-Route	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	88. [redacted] 201
Refer-To	IP/Domain	Overwrite	88. [redacted] 201
From	IP/Domain	Overwrite	10.10.98.119
Via	IP/Domain	Auto	---

7.2.3.2 Topology Hiding Profile for the CS1000

Topology Hiding profile **Topo_CAR276** was defined for incoming calls to the CS1000 to:

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

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

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with options like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, Routing, Server Configuration, Topology Hiding (highlighted), Signaling Manipulation, and URI Groups. The main content area is titled 'Topology Hiding Profiles: Topo_CAR276'. It features an 'Add' button and a list of profiles: default, Topo_Gamma, and Topo_CAR276 (highlighted). The 'Topology Hiding' tab is active, showing a table with the following data:

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

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

Notes:

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

7.2.4. 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_Gamma** and **Inter_CAR276** were created for Gamma (Trunk Server) and the CS1000 (Call Server).

7.2.4.1 Server Interworking Profile for Gamma

Server Interworking profile **Inter_Gamma** was defined to match the specification of **Gamma**. 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.

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 responds 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 = Checked.**
- **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_Gamma**.

Editing Profile: Inter_GAMMA

General

Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
URI Group	None
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
Re-Invite Handling	<input type="checkbox"/>
T.38 Support	<input checked="" type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543

Next

Editing Profile: Inter_GAMMA

X

Privacy

Privacy Enabled

☐

User Name

P-Asserted-Identity

☐

P-Preferred-Identity

☐

Privacy Header

DTMF

DTMF Support

☒ None

☐ SIP NOTIFY

☐ SIP INFO

Back

Finish

Advanced settings:

- **Record Routes = Both Sides.** The Avaya SBCE will send the “Record-Route” header to both the CS1000 and Gamma.
- **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_GAMMA

Record Routes	<input type="radio"/> None <input type="radio"/> Single Side <input checked="" type="radio"/> Both Sides
Topology Hiding: Change Call-ID	<input checked="" type="checkbox"/>
Call-Info NAT	<input type="checkbox"/>
Change Max Forwards	<input checked="" type="checkbox"/>
Include End Point IP for Context Lookup	<input type="checkbox"/>
OCS Extensions	<input type="checkbox"/>
AVAYA Extensions	<input type="checkbox"/>
NORTEL Extensions	<input type="checkbox"/>
Diversion Manipulation	<input type="checkbox"/>
Diversion Header URI	<input type="text"/>
Metaswitch Extensions	<input type="checkbox"/>
Reset on Talk Spurt	<input type="checkbox"/>
Reset SRTP Context on Session Refresh	<input type="checkbox"/>
Has Remote SBC	<input checked="" type="checkbox"/>
Route Response on Via Port	<input type="checkbox"/>
Cisco Extensions	<input type="checkbox"/>

Finish

7.2.4.2 Server Interworking Profile for the CS1000

Server Interworking profile **Inter_CAR276** was similarly defined to match the specification of the CS1000 and T.38 is checked to support T.38 fax call.

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

Next

Editing Profile: Inter_CAR276

X

Privacy

Privacy Enabled

☐

User Name

P-Asserted-Identity

☐

P-Preferred-Identity

☐

Privacy Header

DTMF

DTMF Support

☒ None

☐ SIP NOTIFY

☐ SIP INFO

Back

Finish

Editing Profile: Inter_CAR276

X

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

☐

Finish

7.2.5. Signaling Manipulation

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

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

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

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

In the compliance testing, a SigMa script named **Sig_Gamma** was created for Server Configuration for Gamma and described detail as following:

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the product name and the Avaya logo. A left sidebar contains a navigation menu with categories like Dashboard, Administration, Backup/Restore, System Management, and Global Profiles. The 'Signaling Manipulation' option is highlighted in red. The main content area is titled 'Signaling Manipulation Scripts: Sig_Gamma' and features buttons for Upload, Add, Download, Clone, and Delete. A blue bar prompts the user to 'Click here to add a description.' Below this, a tab labeled 'Signaling Manipulation' is active, showing a script configuration. The script is defined within a session named 'ALL' and consists of two main actions: 'act on message' for inbound traffic and 'act on request' for outbound traffic. The inbound action filters for 'INBOUND' direction and 'AFTER_NETWORK' entry point, then applies a series of regex replacements to the 'Request_Line', 'From', 'To', 'Contact', and 'P-Asserted-Identity' headers. The outbound action filters for 'OUTBOUND' direction and 'POST_ROUTING' entry point, then removes several unwanted headers including 'History-Info', 'Alert-Info', 'x-nt-e164-clid', 'P-AV-Message-Id', 'P-Charging-Vector', 'Av-Global-Session-ID', 'Remote-Address', and 'P-Location'. An 'Edit' button is located at the bottom right of the script editor.

Session Border Controller for Enterprise

Signaling Manipulation Scripts: Sig_Gamma

Upload Add Download Clone Delete

Click here to add a description.

Signaling Manipulation

```
within session "ALL"
{
  act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
  {
    %HEADERS["Request_Line"][1].URI.USER.regex_replace("(\\+)", "");
    %HEADERS["From"][1].URI.USER.regex_replace("(\\+)", "");
    %HEADERS["To"][1].URI.USER.regex_replace("(\\+)", "");
    %HEADERS["Contact"][1].URI.USER.regex_replace("(\\+)", "");
    %HEADERS["P-Asserted-Identity"][1].URI.USER.regex_replace("(\\+)", "");
  }
  act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    // 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]);
    remove(%HEADERS["Remote-Address"][1]);
    remove(%HEADERS["P-Location"][1]);
  }
}
```

Edit

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 from the CS1000 and the manipulation will be done on the header of the INVITE message to remove unwanted headers for regular outbound call.

```
act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
{
    //Remove unwanted Headers for regular outbound call
    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["Remote-Party-ID"][1]);
    remove(%HEADERS["P-Charging-Vector"][1]);
    remove(%HEADERS["Av-Global-Session-ID"][1]);
    remove(%HEADERS["P-Location"][1]);
    remove(%HEADERS["Remote-Address"][1]);
}
```

SIP INVITE message from Gamma contains the “+” sign in the front of number, this plus sign must be removed so that inbound call can be routed to CS1K by using Session Manager. The script below is to remove the “+” sign in the front of calling and called number for inbound call in the Request-Line, From, To, Contact and P-Asserted-Identity headers.

```
act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
{
    %HEADERS["Request_Line"][1].URI.USER.regex_replace("(\\+)", "");
    %HEADERS["From"][1].URI.USER.regex_replace("(\\+)", "");
    %HEADERS["To"][1].URI.USER.regex_replace("(\\+)", "");
    %HEADERS["Contact"][1].URI.USER.regex_replace("(\\+)", "");
    %HEADERS["P-Asserted-Identity"][1].URI.USER.regex_replace("(\\+)", "");
}
```

7.2.6. Server Configuration

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

To create a Server Configuration entry, select **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_Gamma** for Gamma and server entry **SM63** for Session Manager.

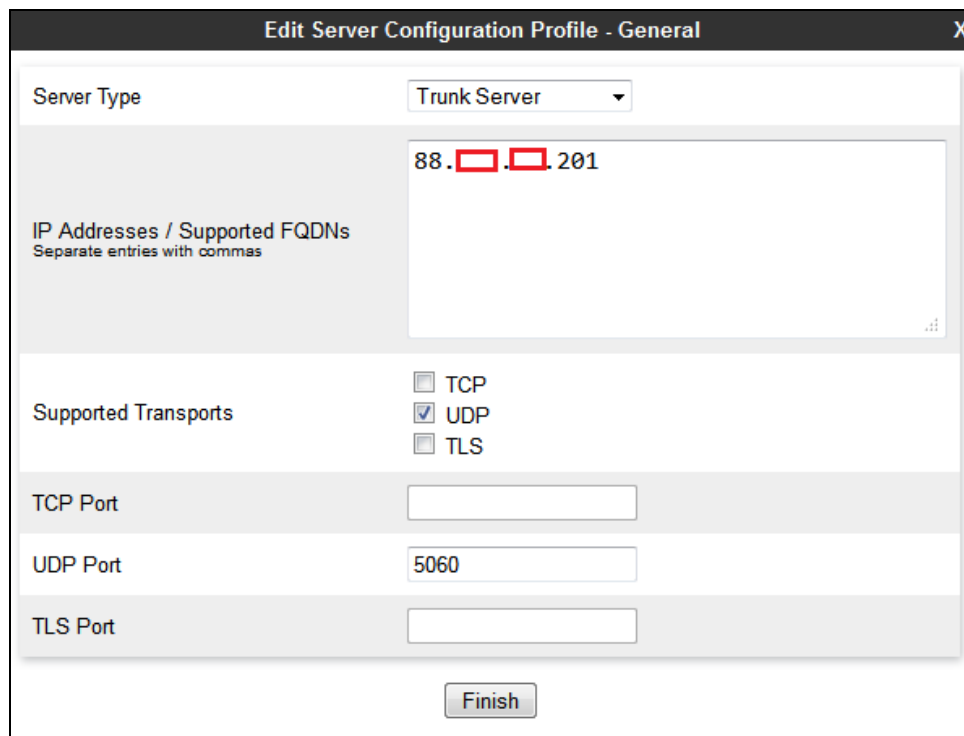
7.2.6.1 Server Configuration for Gamma

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

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows "Session Border Controller for Enterprise" and the Avaya logo. A left sidebar lists navigation options: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles (expanded), Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, Routing, and Server Configuration (highlighted in red). The main content area is titled "Server Configuration: Ser_GAMMA" and features an "Add" button, a "Server Profiles" list with "SM63" and "Ser_GAMMA" (highlighted in red), and buttons for "Rename", "Clone", and "Delete". The "Advanced" tab is selected, showing configuration details for "Ser_GAMMA": Server Type (Trunk Server), IP Addresses / FQDNs (88. [redacted].201), Supported Transports (UDP), and UDP Port (5060). An "Edit" button is located at the bottom right of the configuration table.

Server Type	Trunk Server
IP Addresses / FQDNs	88. [redacted].201
Supported Transports	UDP
UDP Port	5060

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



Edit Server Configuration Profile - General

Server Type: Trunk Server

IP Addresses / Supported FQDNs
Separate entries with commas
88.1.1.201

Supported Transports:
☐ TCP
☒ UDP
☐ TLS

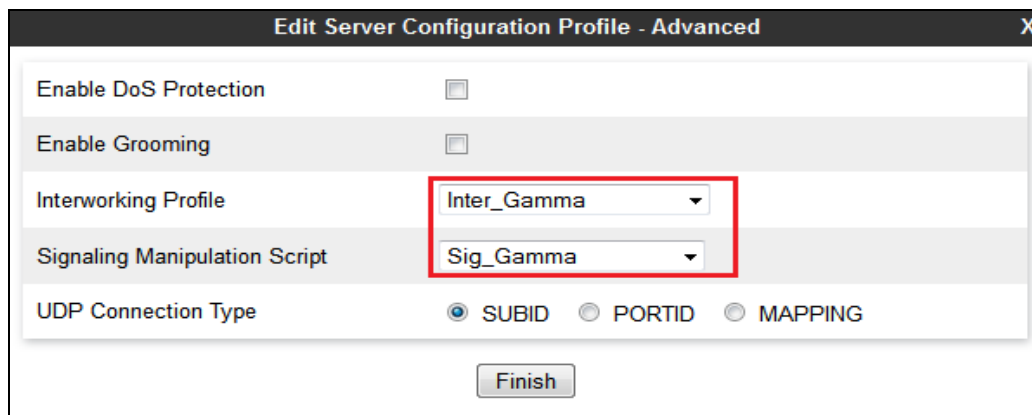
TCP Port:

UDP Port: 5060

TLS Port:

Finish

Under **Advanced** tab, for Interworking Profile drop down list, select **Inter_Gamma** as defined in **Section 7.2.4.1** and for Signaling Manipulation Script drop down list, select **Sig_Gamma** as defined in **Section 7.2.5**. These configurations are applied to the specific SIP profile and SigMa rules for the traffic from and to Gamma. 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_Gamma

Signaling Manipulation Script: Sig_Gamma

UDP Connection Type: ☒ SUBID ☐ PORTID ☐ MAPPING

Finish

7.2.6.2 Server Configuration for Avaya Aura® Session Manager

The Server Configuration **SM63** was added for Session Manager, it is discussed in detail as below. Only the **General** and **Advanced** tabs required provisioning. The **Heartbeat** tab is kept as disabled as default to allow the Avaya SBCE to forward the OPTIONS heartbeat from Gamma to Session Manager to query for the status of the SIP Trunk.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays "Session Border Controller for Enterprise" and the Avaya logo. On the left, a sidebar menu lists various management options, with "Server Configuration" highlighted in red. The main content area is titled "Server Configuration: SM63" and features an "Add" button. Below this, a list of server profiles is shown, with "SM63" selected. To the right, the configuration details for "SM63" are displayed under the "General" tab. The configuration includes: Server Type (Call Server), IP Addresses / FQDNs (10.33.10.26), Supported Transports (UDP), TCP Port (5060), and UDP Port (5060). Buttons for "Rename", "Clone", "Delete", and "Edit" are visible.

Server Type	Call Server
IP Addresses / FQDNs	10.33.10.26
Supported Transports	UDP
TCP Port	5060
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, Session Manager was configured with transport protocol **UDP** and listens on port **5060**. For detailed configuration, refer to **Section 6.6**. Click **Finish** button to save and close the window.

The screenshot shows the "Edit Server Configuration Profile - General" dialog box. A blue warning banner at the top states: "This profile is in use by a SIP Cluster or is associated with a Turing Test Use Case in Media Rules and the Server Type cannot be changed." The configuration fields are as follows: Server Type (Call Server), IP Addresses / Supported FQDNs (10.33.10.26), Supported Transports (UDP selected), TCP Port (5060), UDP Port (5060), and TLS Port (empty). A "Finish" button is located at the bottom.

Server Type	Call Server
IP Addresses / Supported FQDNs	10.33.10.26
Supported Transports	<input checked="" type="checkbox"/> UDP
TCP Port	5060
UDP Port	5060
TLS Port	

Under **Advanced** tab, for Interworking Profile drop down list, select **Intel_CAR276** as defined in **Section 7.2.4.2** and for Signaling Manipulation Script drop down list select **None**. The other settings are kept as default. Click **Finish** button to save and close the window.

Enable DoS Protection ☐

Enable Grooming ☐

Interworking Profile Inter_CAR276

Signaling Manipulation Script None

UDP Connection Type ☒ SUBID ☐ PORTID ☐ MAPPING

Finish

7.3. Domain Policies

Domain Policies feature configures various rule sets (policies) to control unified communications based upon criteria of communication sessions originating from or terminating at the enterprise. These criteria can be used to trigger policies which, in turn, activate various security features of the 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.

7.3.1. 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_Gamma** for the new rule then click on the **Finish** button.

Clone Rule

Rule Name default

Clone Name AppR_Gamma

Finish

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_Gamma** are set high enough to be considered non-blocking.

Application Type	In	Out	Maximum Concurrent Sessions	Maximum Sessions Per Endpoint
Audio	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	1000	100
Video	<input type="checkbox"/>	<input type="checkbox"/>		
IM	<input type="checkbox"/>	<input type="checkbox"/>		

Miscellaneous

CDR Support: ☒ None, ☐ CDR w/ RTP, ☐ CDR w/o RTP

RTCP Keep-Alive: ☐

Finish

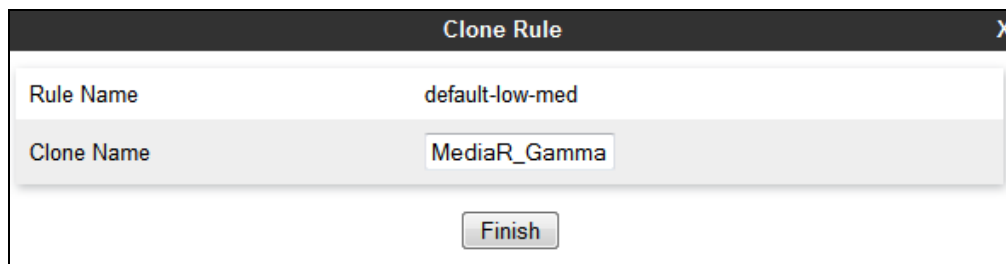
7.3.2. Media Rules

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

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

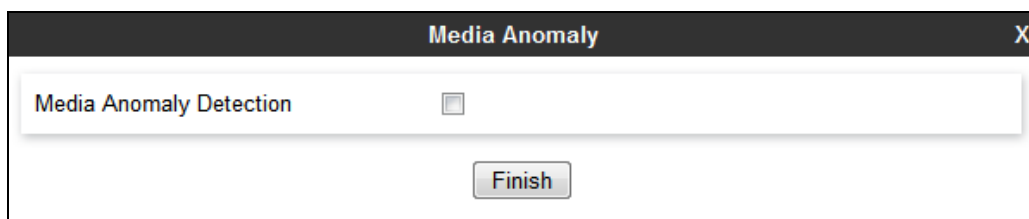
Enter a descriptive name e.g. **MediaR_Gamma** for the new rule then click **Finish** button.



The 'Clone Rule' dialog box has a title bar with 'Clone Rule' and a close button 'X'. It contains two input fields: 'Rule Name' with the value 'default-low-med' and 'Clone Name' with the value 'MediaR_Gamma'. A 'Finish' button is located at the bottom right.

When the RTP changes in event of 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.

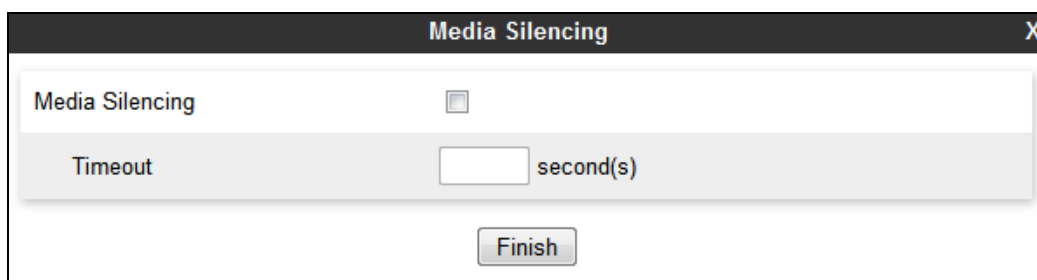
To modify Media Anomaly, select the **Media Anomaly** tab and click on the **Edit** button (not shown). Then uncheck **Media Anomaly Detection** and click on the **Finish** button.



The 'Media Anomaly' dialog box has a title bar with 'Media Anomaly' and a close button 'X'. It contains a checkbox labeled 'Media Anomaly Detection' which is currently unchecked. A 'Finish' button is located at the bottom right.

On the Avaya SBCE, 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 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.



The 'Media Silencing' dialog box has a title bar with 'Media Silencing' and a close button 'X'. It contains a checkbox labeled 'Media Silencing' which is currently unchecked. Below it is a 'Timeout' field with an input box and the text 'second(s)'. A 'Finish' button is located at the bottom right.

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 service provider. The following screen shows the QoS values used for the compliance testing.

7.3.3. Signaling Rules

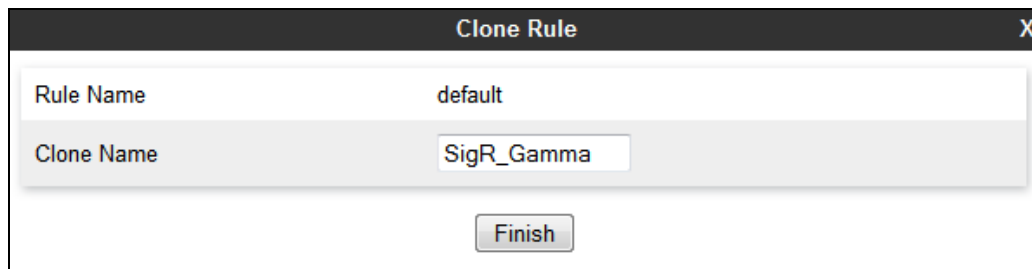
Signaling Rules define actions to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. When SIP signaling packets are received by the Avaya SBCE, they are parsed and “pattern-matched” against the particular signaling criteria defined 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 Gamma and the CS1000.

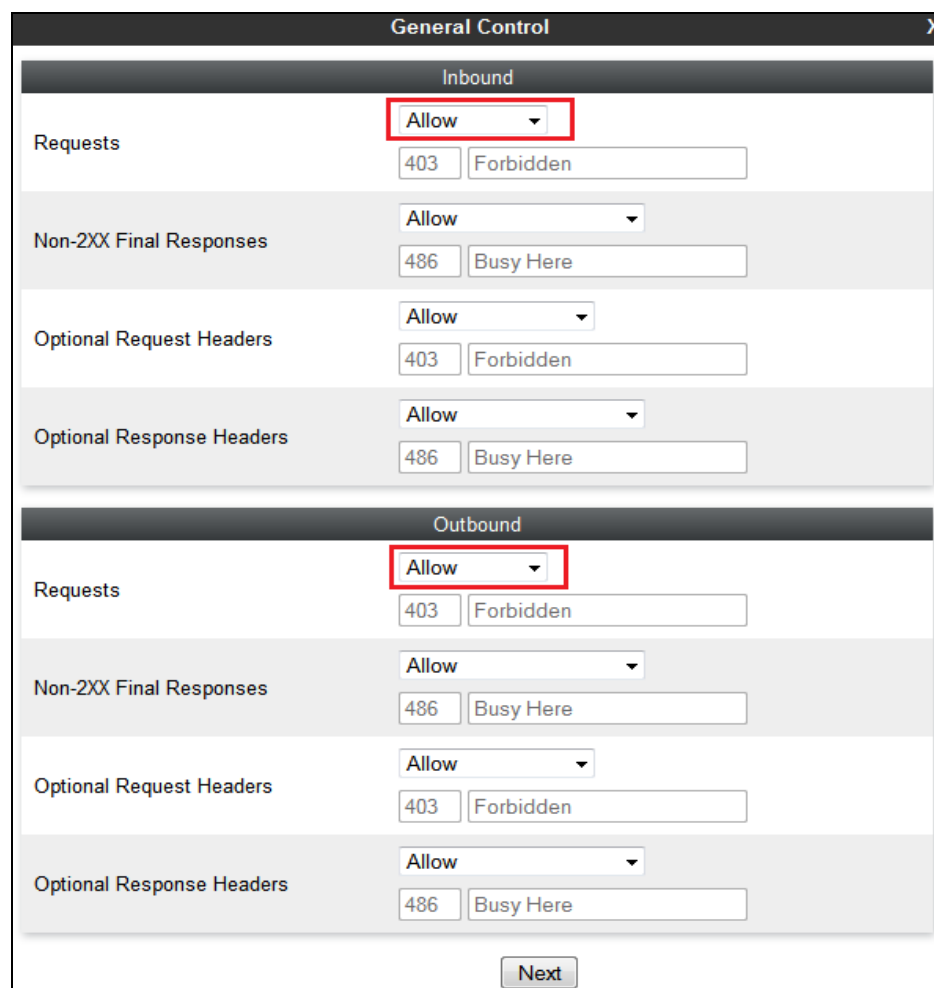
7.3.3.1 Signaling Rule for Gamma

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



The 'Clone Rule' dialog box is shown. It has a title bar with 'Clone Rule' and a close button 'X'. Inside, there are two input fields: 'Rule Name' with the value 'default' and 'Clone Name' with the value 'SigR_Gamma'. Below these fields is a 'Finish' button.

The **SigR_Gamma** was configured to allow the Avaya SBCE to accept inbound and outbound call requests from Gamma. Cloning the Signaling Rule default, the **SigR_Gamma** will block all requests with a “403 Forbidden”. To start accepting calls, go to **General** tab, click on the **Edit** button (not shown). Then change **Inbound** and **Outbound Request** to **Allow** as shown in following screenshot.



The 'General Control' window is shown, divided into 'Inbound' and 'Outbound' sections. In the 'Inbound' section, the 'Requests' dropdown is set to 'Allow' (highlighted with a red box). Below it, there are input fields for '403' and 'Forbidden'. The 'Non-2XX Final Responses' dropdown is set to 'Allow', with input fields for '486' and 'Busy Here'. The 'Optional Request Headers' dropdown is set to 'Allow', with input fields for '403' and 'Forbidden'. The 'Optional Response Headers' dropdown is set to 'Allow', with input fields for '486' and 'Busy Here'. The 'Outbound' section has identical settings, with the 'Requests' dropdown also set to 'Allow' (highlighted with a red box). At the bottom of the window is a 'Next' button.

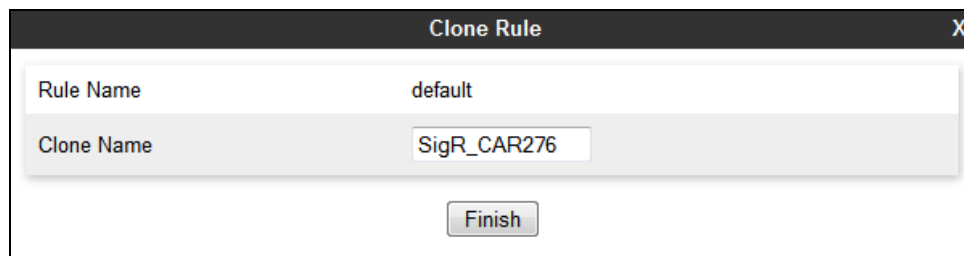
On the **Signaling QoS** tab, select the proper Quality of Service (QoS). The Avaya SBCE can be configured to mark the Differentiated Services Code Point (DSCP) in the IP packet header with specific values to support Quality of Services policies for signaling. The following screen shows the QoS value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



The image shows a 'Signaling QoS' configuration window. At the top, there is a title bar with 'Signaling QoS' and a close button 'X'. Below the title bar, there is a section for 'Enabled' with a checked checkbox. Underneath, there are three radio buttons: 'ToS', 'DSCP', and 'DSCP'. The 'DSCP' radio button is selected and highlighted with a red box. Below the radio buttons, there are three rows of configuration options. The first row is 'Precedence' with a dropdown menu set to 'Routine' and a text box containing '000'. The second row is 'ToS' with a dropdown menu set to 'Minimize Delay' and a text box containing '1000'. The third row is 'Value' with a dropdown menu set to 'EF' and a text box containing '101110'. The 'DSCP' radio button and the 'Value' dropdown menu are both highlighted with red boxes. At the bottom of the window, there is a 'Finish' button.

7.3.3.2 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.



The image shows a 'Clone Rule' window. At the top, there is a title bar with 'Clone Rule' and a close button 'X'. Below the title bar, there is a section for 'Rule Name' with a text box containing 'default'. Underneath, there is a section for 'Clone Name' with a text box containing 'SigR_CAR276'. At the bottom of the window, there is a 'Finish' button.

This **SigR_CAR276** is configured to allow the Avaya SBCE to accept inbound and outbound call requests from the CS1000. Cloning the Signaling Rule **default**, the **SigR_CAR276** will block all requests with a “403 Forbidden”. To start accepting calls, select **SigR_CAR276** then go to **General** tab, click on the **Edit** button (not shown). Then change **Inbound-Requests** and **Outbound-Requests** to **Allow** as shown in following screenshot.

The screenshot displays the 'General Control' configuration window for 'SigR_CAR276'. The window is divided into two main sections: 'Inbound' and 'Outbound'. Each section contains four rows of configuration options. In both sections, the 'Requests' dropdown is set to 'Allow' and is highlighted with a red rectangle. The 'Non-2XX Final Responses' dropdown is set to 'Allow'. The 'Optional Request Headers' dropdown is set to 'Allow', and the 'Optional Response Headers' dropdown is set to 'Allow'. Below each dropdown, there are two input fields: '403' and 'Forbidden' for requests, and '486' and 'Busy Here' for responses. At the bottom of the window, there is a 'Next' button.

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

Next

On the **Signaling QoS** tab, select the proper Quality of Service (QoS). The ASBCE 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.

The screenshot shows a window titled "Signaling QoS" with a close button (X) in the top right corner. The window contains the following configuration options:

- Enabled:** A checkbox that is checked, highlighted with a red rectangle.
- ToS:** A radio button option, currently unselected.
- Precedence:** A dropdown menu set to "Routine" and a text box containing "000".
- ToS:** A dropdown menu set to "Minimize Delay" and a text box containing "1000".
- DSCP:** A radio button option that is selected, highlighted with a red rectangle.
- Value:** A dropdown menu set to "EF", highlighted with a red rectangle, and a text box containing "101110".
- Finish:** A button at the bottom center of the window.

7.3.4. Endpoint Policy Groups

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

Two Endpoint Policy Groups were separately created for Gamma 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).

7.3.4.1 Endpoint Policy Group for Gamma

The following screen shows **PolicyG_Gamma** created for Gamma.

- Set Application Rule to **AppR_Gamma** which was created in **Section 7.3.1**.
- Set Media Rule to **MediaR_Gamma** which was created in and **Section 7.3.2**.
- Set Signaling Rule to **SigR_Gamma** which was created in **Section 7.3.3.1**.
- Set **Border** and **Time of Day** rules to **default**.
- Set **Security** rule to **default-med**.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows 'Session Border Controller for Enterprise' and the Avaya logo. A left sidebar contains a navigation menu with categories like Dashboard, Administration, Backup/Restore, System Management, and Domain Policies. The 'Domain Policies' section is expanded, showing 'End Point Policy Groups' in red. The main content area is titled 'Policy Groups: PolicyG_Gamma' and features an 'Add' button, a 'Filter By Device...' dropdown, and buttons for 'Rename', 'Clone', and 'Delete'. Below this, a table lists various policy groups, with 'PolicyG_Gamma' highlighted in red. A 'Policy Group' detail box is open, showing a table with columns: Order, Application, Border, Media, Security, Signaling, and Time of Day. The table contains one row for 'PolicyG_Gamma' with the following values: Order 1, Application AppR_Gamma, Border default, Media MediaR_Gamma, Security default-med, Signaling SigR_Gamma, and Time of Day default. The table also includes 'Edit' and 'Clone' links for each row.

Order	Application	Border	Media	Security	Signaling	Time of Day
1	AppR_Gamma	default	MediaR_Gamma	default-med	SigR_Gamma	default

7.3.4.2 Endpoint Policy Group for the CS1000

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

- Set Application Rule to **AppR_Gamma** which was created in **Section 7.3.1**.
- Set Media Rule to **MediaR_Gamma** which was created in and **Section 7.3.2**.
- Set Signaling Rule **SigR_CAR276** which was created in **Section 7.3.3.2**.
- Set the **Border** and **Time of Day** rules to **default**.
- Set the **Security** rule to **default-low**.

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays "Session Border Controller for Enterprise" and the Avaya logo. On the left, a sidebar menu lists various configuration areas, with "End Point Policy Groups" highlighted. The main content area is titled "Policy Groups: PolicyG_CAR276" and shows a list of policy groups. A table lists the policy groups, with "PolicyG_CAR276" selected. The table has columns for Order, Application, Border, Media, Security, Signaling, and Time of Day. The selected policy group "PolicyG_CAR276" has the following configuration:

Order	Application	Border	Media	Security	Signaling	Time of Day
1	AppR_Gamma	default	MediaR_Gamma	default-low	SigR_CAR276	default

7.3.5. Session Policy

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

In the compliance testing, the Session Policy **SP1_Gamma** was created to match the codec configuration on Gamma. The policy also allows the Avaya SBCE to anchor media for off-net call forward and call transfer scenarios.

To clone a common Session Policy which applies to both Gamma 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_Gamma** for the new policy and click on the **Finish** button.

The screenshot shows a "Clone Policy" dialog box. It has two input fields: "Policy Name" with the value "default" and "Clone Name" with the value "SP1_Gamma". There is a "Finish" button at the bottom right.

Gamma supports voice codec G.711Alaw and G.729. To define **Codec Prioritization** for Audio Codec, select the profile **SP1_Gamma** 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 Gamma and vice versa.

Audio Codec	
Codec Prioritization	<input checked="" type="checkbox"/>
Allow Preferred Codecs Only	<input type="checkbox"/>
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	<input type="checkbox"/>
Allow Preferred Codecs Only	<input type="checkbox"/>
Preferred Codec #1	CelB (25)
Preferred Codec #2	None
Preferred Codec #3	None
Preferred Codec #4	None
Preferred Codec #5	None

Finish

Under **Media** tab of the Session Policy **SP1_Gamma** created above, click on the **Edit** button (not shown) then check on **Media Anchoring** to allow the Avaya SBCE to anchor media for off-net call forward and call transfer scenarios.

Media Anchoring	<input checked="" type="checkbox"/>
Media Forking Profile	None

Finish

7.4. Device Specific Settings

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

7.4.1. Network Management

Network Management 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 **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 the **Figure 1**.

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

Session Border Controller for Enterprise

AVAYA

Dashboard
Administration
Backup/Restore
System Management
‣ Global Parameters
‣ Global Profiles
‣ SIP Cluster
‣ Domain Policies
‣ TLS Management
‣ Device Specific Settings
  Network Management
  Media Interface
  Signaling Interface
  Signaling Forking
  End Point Flows
  Session Flows
  Relay Services
  SNMP

Network Management: SBCE62

Devices
SBCE62

Network Configuration Interface Configuration

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: 255.255.255.192 A2 Netmask: B1 Netmask: 255.255.255.224 B2 Netmask:

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
<input type="text"/>		<input type="text"/>	B1	Delete
<input type="text"/>		<input type="text"/>	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**.

Session Border Controller for Enterprise

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

Dashboard Administration Backup/Restore System Management Global Parameters Global Profiles SIP Cluster Domain Policies TLS Management Device Specific Settings

Network Management: SBCE62

Devices SBCE62

Network Configuration Interface Configuration

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

Network Management

7.4.2. Media Interface

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.

Session Border Controller for Enterprise

Alarms Incidents Statistics Logs Diagnostics Users Settings Help Log Out

Dashboard Administration Backup/Restore System Management Global Parameters Global Profiles SIP Cluster Domain Policies TLS Management Device Specific Settings

Media Interface: SBCE62

Devices SBCE62

Media Interface

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

Add

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

Media Interface

7.4.3. Signaling Interface

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.

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

7.4.4. 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 Gamma and Session Manager.

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_Gamma** created in **Section 0** which the Server Flow associates to.
- **URI Group:** Select the URI Group **SP1_Gamma** created in **Section 7.2.1**.

- **Received Interface:** Select the Signaling Interface created in **Section 7.4.3** which is the Server Configuration is designed to receive SIP signaling from.
- **Signaling Interface:** Select the Signaling Interface created in **Section 7.4.3** which is the Server Configuration is designed to send the SIP signaling to.
- **Media Interface:** Select the Media Interface created in **Section 7.4.2** which is the Server Configuration is designed to send the RTP to.
- **End Point Policy Group:** Select the End Point Policy Group created in **Section 7.3.4**.
- **Routing Profile:** Select the Routing Profile created in **Section 7.2.2** which is used to which is the Server Configuration is designed to route the calls to.
- **Topology Hiding Profile:** Select the Topology Hiding profile created in **Section 7.2.3** 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 **From_Gamma** for Gamma.

Edit Flow: From_Gamma	
Flow Name	From_Gamma
Server Configuration	Ser_Gamma
URI Group	SP1_Gamma
Transport	*
Remote Subnet	*
Received Interface	InsideSignaling
Signaling Interface	OutsideSignaling
Media Interface	OutsideMedia
End Point Policy Group	PolicyG_Gamma
Routing Profile	To_SM63_CAR276
Topology Hiding Profile	Topo_Gamma
File Transfer Profile	None
<input type="button" value="Finish"/>	

The following screen shows the Server Flow named **From_CAR276** for Session Manager.

The screenshot shows a window titled "Edit Flow: From_CAR276" with a close button (X) in the top right corner. The window contains a list of configuration parameters, each with a label and a value field (either a text box or a dropdown menu). The parameters are:

Parameter	Value
Flow Name	From_CAR276
Server Configuration	SM63
URI Group	SP1_Gamma
Transport	*
Remote Subnet	*
Received Interface	OutsideSignaling
Signaling Interface	InsideSignaling
Media Interface	InsideMedia
End Point Policy Group	PolicyG_CAR276
Routing Profile	To_Gamma
Topology Hiding Profile	Topo_CAR276
File Transfer Profile	None

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

7.4.5. Session Flows

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

A common Session Flow **SP1** was created for both the Gamma 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 7.2.1** to assign to the Session Flow as the source URI Group.
- **URI Group #2:** Select the URI Group created in **Section 7.2.1** to assign to the Session Flow as the destination URI Group.

- **Session Policy:** Select the Session Policy created in **Section 7.3.5** to assign to the Session Flow.
- Click 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**.

8. Configure Gamma SIP Trunking Service

Gamma 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 side. Gamma will provide the customer with the necessary information to configure the SIP Trunk connection from enterprise to the Gamma network.

The information provided by Gamma includes:

- IP address of the Gamma 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.

9. 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.

9.1. 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.

9.2. 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:001613xxx5258@88.xxx.xx.201;user=phone SIP/2.0
From: "Avaya CS1K" <sip:1229xxx455@10.10.98.119;user=phone>;tag=34fc690-aa610a87-13c4-
55013-2e30b6-edba675-2e30b6
To: <sip:001613xxx5258@88.xxx.xx.201;user=phone>
CSeq: 1 INVITE
Call-ID: 603ce02631d60d3a68d54679d6c59945
Contact: <sip:1229xxx455@10.10.98.119:5060;transport=udp;user=phone;gsid=d7c8d130-b6a8-11e3-
87c0-e41f13b32ca8>
Record-Route: <sip:10.10.98.119:5060;ipcs-line=34773;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-s1632-001173561140-1--s1632-
Privacy: none
P-Asserted-Identity: "Avaya CS1K" <sip:1229xxx455@10.10.98.119;user=phone>
Content-Type: application/sdp
Content-Length: 265

v=0
o=- 1389 1 IN IP4 10.10.98.119
s=-
c=IN IP4 10.10.98.119
t=0 0
m=audio 35460 RTP/AVP 0 8 18 101 111
c=IN IP4 135.10.98.119
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 200 OK responded from Gamma to the CS1000

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.10.98.119:5060;branch=z9hG4bK-s1632-001173561140-1--s1632-
Record-Route: <sip:10.10.98.119:5060;ipcs-line=34773;lr;transport=udp>
To: <sip:001613xxx5258@88.xx.xx.201;user=phone>;tag=3605021206-788390
From: "Avaya CS1K" <sip:1229xxx455@10.10.98.119;user=phone>;tag=34fc690-aa610a87-13c4-
55013-2e30b6-edba675-2e30b6
Call-ID: 603ce02631d60d3a68d54679d6c59945
CSeq: 1 INVITE
Allow: CANCEL, ACK, INVITE, BYE, OPTIONS, REGISTER, NOTIFY, INFO, REFER,
SUBSCRIBE, PRACK, UPDATE, MESSAGE, PUBLISH
Contact: <sip:001613xxx5258@88.xxx.xx.201:5060>
Content-Type: application/sdp
Accept: application/sdp
Content-Length: 214

v=0
o=MSX24 8052347426352810953 1 IN IP4 88.xxx.xx.201
s=sip call
c=IN IP4 88.xxx.xx.202
t=0 0
m=audio 6570 RTP/AVP 8 101
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=sendrecv
```

c) SIP INVITE message from Gamma to the CS1000

```
INVITE sip:+441229xxx455@10.10.98.119;user=phone SIP/2.0
Max-Forwards: 69
Session-Expires: 3600;refresher=uac
Min-SE: 600
Supported: timer, 100rel
To: <sip:+441229xxx455@88.xxx.xx.201:5060;user=phone>
From: <sip:+1613xxx5258@88.xxx.xx.201>;tag=3605021507-753535
P-Asserted-Identity: <sip:+1613xxx5258@88.xxx.xx.201;user=phone>
Call-ID: 2495552-3605021507-753526@MSX24.mydomain.com
CSeq: 1 INVITE
Allow: CANCEL, ACK, INVITE, BYE, OPTIONS, REGISTER, NOTIFY, INFO, REFER,
SUBSCRIBE, PRACK, UPDATE, MESSAGE, PUBLISH
Via: SIP/2.0/UDP 88.xxx.xx.201:5060;branch=z9hG4bK3904823dfed3b87a6320ff7ebe0ea63d
Contact: <sip:+1613xxx5258@88.xxx.xx.201:5060>
Content-Type: application/sdp
Accept: application/sdp
Content-Length: 261

v=0
o=MSX24 8050381936581726982 1 IN IP4 88.xxx.xx.201
s=sip call
c=IN IP4 88.xxx.xx.202
t=0 0
m=audio 7360 RTP/AVP 8 18 101
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=sendrecv
```

d) SIP 200 OK responded by the CS1000 to Gamma captured at the Avaya SBCE

```
SIP/2.0 200 OK
From: <sip:1613xxx5258@88.xxx.xx.201>;tag=3605021507-753535
To: <sip:441229xxx455@88.xxx.xx.201:5060;user=phone>;tag=34fcf50-aa610a87-13c4-55013-2e31e3-8ca21b4-2e31e3
CSeq: 1 INVITE
Call-ID: 2495552-3605021507-753526@MSX24.mydomain.com
Contact: <sip:441229xxx455;phone-context=UnknownUnknown@10.10.98.119:5060;transport=udp;user=phone;gsid=8b4d8b10-b6a9-11e3-87c0-e41f13b32ca8>
Record-Route: <sip:10.10.98.119:5060;transport=udp;lr;ipcs-line=34805>
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
Via: SIP/2.0/UDP 88.xxx.xx.201:5060;branch=z9hG4bK3904823dfed3b87a6320ff7ebe0ea63d
Require: timer
Server: AVAYA-SM-6.3.4.0.634014
Privacy: none
P-Asserted-Identity: "xo i2007" <sip:441229xxx455;phone-context=UnknownUnknown@88.xxx.xx.201:5060;user=phone>
Remote-Address: 10.33.5.8:5201:1:2
Content-Type: application/sdp
P-Location: SM;origlocname="Belleville";origsiglocname="Belleville";origmedialocname="Belleville";termlocname="Belleville";termsiglocname="Belleville";termmedialocname="Belleville";smaccounting="true"
P-AV-Message-Id: 1_2
Av-Global-Session-ID: 8b4d8b10-b6a9-11e3-87c0-e41f13b32ca8
Content-Length: 239

v=0
o=- 1390 1 IN IP4 10.10.98.119
s=-
c=IN IP4 10.10.98.119
t=0 0
m=audio 35464 RTP/AVP 8 101 111
c=IN IP4 135.10.98.119
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=rtpmap:111 X-nt-inforeq/8000
a=ptime:20
a=sendrecv
```

10. Conclusion

These Application Notes describe the configuration necessary to connect the Avaya Communication Server 1000E Release 7.6, Avaya Aura® Session Manager Release 6.3 and the Avaya Session Border Controller for Enterprise Release 6.2 to Gamma SIP Trunking Service. Gamma 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 Gamma SIP Trunking Service is considered compliant with the Avaya Communication Server 1000E Release 7.6, Avaya Aura® Session Manager Release 6.3 and the Avaya Session Border Controller for Enterprise Release 6.2.

11. References

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

- [1] *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® Session 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/>.

©2014 Avaya Inc. All Rights Reserved.

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

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