



**Application Notes for Configuring Frontier Communications 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 6.2.1 - Issue 1.0**

**Abstract**

These Application Notes describe the procedures for configuring Frontier Communications 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 6.2.1.

The test was performed to verify SIP trunk features including basic calls, call forward (all calls, busy, no answer), call transfer (blind and consult), conference, voice mail, etc. The calls were placed to and from the PSTN with various Avaya endpoints.

The Frontier Communications SIP Trunking service provides PSTN access via SIP trunks between the enterprise and the Frontier Communications network as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

## Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing.....	4
2.2.	Test Results .....	6
2.3.	Support.....	6
3.	Reference Configuration.....	7
4.	Equipment and Software Validated .....	9
5.	Configure Avaya Communication Server 1000E .....	11
5.1.	Login to the Avaya Communication Server 1000E .....	11
5.2.	Administer a Node IP Telephony.....	13
5.2.1.	Obtain Node IP address .....	13
5.2.2.	Administer Terminal Proxy Server.....	14
5.2.3.	Administer Quality of Service (QoS) .....	15
5.2.4.	Voice Gateway and Codecs .....	16
5.2.5.	SIP Gateway.....	19
5.2.6.	Synchronize the Node Configuration.....	22
5.3.	Administer Virtual Super-Loop .....	23
5.4.	Enable Voice Codec on Media Gateways.....	23
5.5.	Administer Zones and Bandwidth.....	25
5.5.1.	Bandwidth Zones for virtual SIP trunks .....	26
5.5.2.	Bandwidth Zones for IP Telephones.....	27
5.6.	Virtual D Channel, Routes and Trunks .....	28
5.6.1.	Administer Virtual D-Channel.....	28
5.6.2.	Administer Virtual SIP Routes .....	31
5.6.3.	Administer Virtual Trunks.....	34
5.7.	Administer Dialing Plans .....	37
5.7.1.	Define ESN Access Codes and Parameters (ESN).....	37
5.7.2.	Digit Manipulation Block Index (DMI).....	38
5.7.3.	Route List Block (RLB).....	39
5.7.4.	Outbound Call - Special Number Configuration.....	41
5.7.5.	Outbound Call - Numbering Plan Area Code (NPA) .....	43
5.7.6.	Administer Calling Line Identification Entries.....	43
5.7.7.	Inbound Call Digit Translation .....	45
5.8.	Enable Plug-In for Blind Call Transfer .....	46
5.9.	CS1000 Telephones and Features Settings .....	47
5.9.1.	Example IP Phones with Privacy and Call Forward.....	47
5.9.2.	Example Digital Phone with Call Waiting.....	49
5.9.3.	Analog Fax Line .....	50
6.	Configure Avaya Aura® Session Manager .....	51
6.1.	Avaya Aura® System Manager Login and Navigation .....	52
6.2.	SIP Domain .....	53
6.3.	Locations .....	53

6.4.	Adaptations.....	56
6.5.	SIP Entities.....	58
6.6.	Entity Links.....	62
6.7.	Routing Policies.....	63
6.8.	Dial Patterns.....	64
7.	Configure Avaya Session Border Controller for Enterprise.....	67
7.1.	System Access.....	67
7.2.	System Management.....	68
7.3.	Global Profiles.....	69
7.3.1.	Server Interworking.....	69
7.3.2.	Signaling Manipulation.....	74
7.3.3.	Server Configuration.....	75
7.3.4.	Routing Profiles.....	78
7.3.5.	Topology Hiding.....	80
7.4.	Domain Policies.....	82
7.4.1.	Signaling Rules.....	82
7.4.2.	End Point Policy Groups.....	86
7.5.	Device Specific Settings.....	87
7.5.1.	Network Management.....	87
7.5.2.	Media Interface.....	88
7.5.3.	Signaling Interface.....	89
7.5.4.	End Point Flows.....	91
8.	Frontier Communications SIP Trunking Service Configuration.....	93
9.	Verification Steps.....	93
9.1.	Avaya Communication Server 1000E Verification.....	93
9.1.1.	IP Network Maintenance and Reports Commands.....	93
9.1.2.	System Maintenance Commands.....	94
9.2.	Avaya Aura® Session Manager Verification.....	96
9.3.	Avaya SBCE Verification.....	97
10.	Conclusion.....	99
11.	References.....	100
12.	Appendix A.....	101

# 1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between the Frontier Communications SIP Trunking service and a SIP-enabled enterprise solution consisting of Avaya Communication Server 1000E Release 7.6 (CS1000), Avaya Aura® Session Manager Release 6.3, and Avaya Session Border Controller for Enterprise (Avaya SBCE) 6.2.1. During the interoperability testing, SIP trunk applicable feature test cases were executed to ensure the interoperability between the Frontier Communications network and the Avaya Communication Server 1000E.

The Frontier Communications SIP Trunking service referenced within these Application Notes is designed for enterprise business customers. Customers using this service with the Avaya SIP-enabled enterprise solution are able to place and receive PSTN calls via a broadband WAN connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks such as analog and/or ISDN-PRI trunks. This approach generally results in lower cost for the enterprise.

## 2. General Test Approach and Test Results

A simulated enterprise site containing all the equipment for the Avaya SIP-enabled solution was installed at the Avaya Solution and Interoperability Lab. The site was configured to connect to the Frontier Communications SIP Trunking service by means of a broadband connection to the public Internet.

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

### 2.1. Interoperability Compliance Testing

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

- Incoming PSTN calls to various phone types. All inbound calls from the PSTN were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types. All outbound calls to the PSTN were routed from the enterprise across the SIP trunk to the service provider.
- Phone types used for testing at the enterprise included Avaya 1100 Series IP Telephones (SIP), Avaya 1100 Series IP Telephones (UniStim), Avaya M3904 Digital Telephones, Avaya 2050 IP Softphone, Analog Telephones and Fax machines (Ventafax).
- Proper disconnect when the caller abandons the call before the call is answered.
- Proper disconnect during normal active call termination by the caller or the callee.
- Proper disconnect by the network for calls that are not answered (with voice mail off).

- Proper response to busy end points.
- Proper response/error treatment when dialing invalid PSTN numbers.
- Codecs G729 and G.711U with Voice Activity Detection (VAD) disabled.
- Voice mail and DTMF tone support in both directions (RFC2833) (Leaving voice mail, retrieving voice mail, etc.).
- CallPilot Voice Mail Server (Hosted in the CS1000).
- Outbound Toll-Free calls, interacting with Interactive Voice Response systems (IVR).
- International calls.
- Calling number and calling name blocking (Privacy).
- Call Hold/Resume.
- Call Forward (unconditional, busy, no answer).
- Blind Call Transfers.
- Call Park.
- Consultative Call transfers.
- Station Conference.
- T.38 fax support.
- G.711u fax pass-through support.
- Long duration calls (one hour).
- Early Media transmission.

Items not supported or not tested included the following:

- Inbound toll-free and emergency (911) calls are supported but were not tested as part of the compliance test.
- Operator assisted calls dialing 0 + 10 digits are not supported.

## 2.2. Test Results

Interoperability testing of the Frontier Communications SIP Trunking service completed with successful results for all test cases. The following observations/limitations are noted:

- **Blind Call Transfer to the PSTN:** Plug-in 501 was enabled in the CS1000 to allow users to make blind call (unattended) transfers to the PSTN, even as Frontier did not support SIP UPDATES. See **Section 5.8**. While the plug-in allows CS1000 users to complete the blind call transfer operation, the PSTN user on the first leg of the call will not hear ring back while the second PSTN phone is ringing. Once the second PSTN user answers the call, the talk path between the two PSTN endpoints is established normally. This is a known CS1000 limitation, in cases when UPDATES are not supported by the service provider.
- **T.38 Fax:** On incoming fax calls to the enterprise, the re-INVITE to switch from voice to T.38, which in general is sent by the receiving end, was sent by the CS1000 and the T.38 fax call was successful. On outbound fax calls from the enterprise, Frontier did not send the T.38 re-INVITE as expected, and the T.38 fax call failed. See Annex D in [16] in the **References** section for more information on T.38 call establishment procedures. Outbound fax calls were successfully tested using the G711-passthrough mode.
- **Response to OPTIONS:** During the compliance test, Frontier responded to OPTIONS messages sent from the enterprise with a “403 URI not recognized” message. Since the OPTIONS messages were used to check the status of the network connectivity to the service provider, any response received from Frontier was sufficient to achieve that purpose.
- **Calls to Busy numbers:** Frontier did not send “486 Busy Here” for calls from the enterprise to busy PSTN numbers. Since busy tone was heard by the caller, this observation had no direct impact to the user.
- **Dialed Number Display:** If a CS1000 phone places an outbound call on hold and then retrieves it, the dialed digits are no longer shown on the phone display; the access code for the trunk route (ACOD) is displayed instead. This is a Communication Server 1000 known issue.
- **SIP header optimization:** There are multiple SIP headers used by the CS1000, Session Manager and the Avaya SBCE that at the time of the test had no particular use in the service provider’s network. These headers were removed in order to reduce the size of the packets entering the Frontier network. The CS1000 multipart MIME SDP, which included the x-nt-mcdn-frag-hex, x-nt-esn5-frag-hex, and x-nt-epid-frag was stripped out by using a Session Manager adaptation. See **Section 6.4**.  
In addition, the following headers were removed using Signaling Rules and a Sigma Script in the Avaya SBCE: Alert-Info, AV-Global-Session-ID, Endpoint-View, History-Info, P-AV-Message-ID, P-Charging-Vector, P-Location, User Agent and Remote-Address. See **Sections 7.3.2** and **7.4.1**.

## 2.3. Support

For technical support on the Frontier Communications SIP Trunking service, use the Help and Support links for business customers at <http://www.frontier.com>.

### 3. Reference Configuration

**Figure 1** below illustrates the test configuration used. The test configuration simulates an enterprise site with the Avaya components connected to the Frontier Communications SIP Trunking service through a public Internet high speed connection.

The components used to create the simulated customer site included:

- Avaya Communication Server 1000E (CS1000E).
- Avaya Aura® Session Manager.
- Avaya Aura® System Manager.
- Avaya Session Border Controller for Enterprise (SBCE).
- Avaya 1100-Series IP Telephones (UniStim).
- Avaya 1100-Series Telephones (SIP).
- 2050 Avaya IP Softphone.
- Avaya M3904 Digital telephones.
- Analog Telephones.
- Desktop PCs with Ventafax fax machine emulation software.
- Desktop PC with administration interfaces.

In the sample configuration, the Avaya SBCE constitutes the single point of connection between the public network and the enterprise Local Area Network, containing the Avaya Customer Premise Equipment (CPE). The Avaya SBCE provides security for all SIP and RTP traffic entering the private network, in addition to Network Address Translation (NAT) at both the IP and SIP layers.

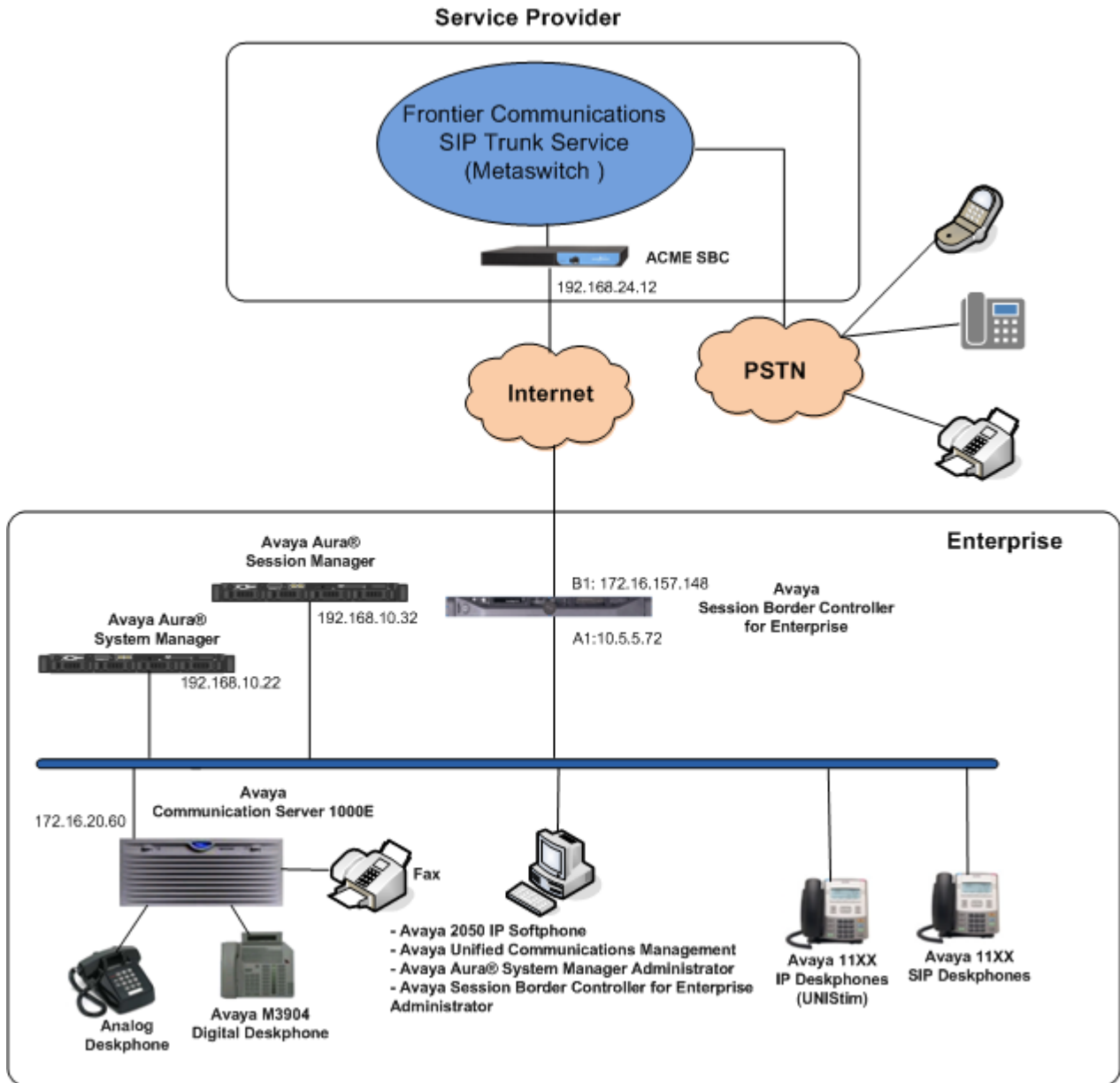
The transport protocol between the Avaya SBCE and Frontier across the public IP network is UDP. The transport protocol between the Avaya SBCE and the enterprise Session Manager across the enterprise IP network is TCP.

One SIP trunk group was created between the CS1000 and Session Manager to carry the traffic to and from the service provider (two-way trunk group).

For inbound calls, the calls flowed from the service provider to the Avaya SBCE, then to Session Manager. Session Manager used the configured dial patterns, routing policies and adaptations to determine the recipient (in this case the CS1000) and on which link to send the call. Once the call arrived at the CS1000, further incoming call treatment, such as incoming digit translations and class of service restrictions are performed.

Outbound calls to the PSTN were first processed by the CS1000 for outbound treatment through the Electronic Switched Network and class of service restrictions. Once the CS1000 selected the proper SIP trunk, the call was routed to Session Manager. Session Manager once again used the configured dial patterns, adaptations, and routing policies to determine the route to the Avaya SBCE for egress to the Frontier network.

For security reasons, any actual public IP addresses used in the configuration have been replaced with private addresses. Similarly, any references to real routable DIDs and PSTN numbers have also been masked to numbers that cannot be routed by the PSTN.



**Figure 1: SIP Enterprise Solution connected to the Frontier Communications SIP Trunking service**



## 4. Equipment and Software Validated

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

Component	Version
<b>Avaya</b>	
Avaya Communication Server 1000E running Co-resident Call Server, Signaling Server and Media Gateway in a single CP-MGS card.	Release 7 Issue 65 P + DepList 1: core Issue: 01 ( <b>created: 2013-12-17 04:32:53 (est)</b> )  Signaling Server: 7.65.16.00 (Service Pack 4)  **See Service Updates & Patches below**
Avaya Aura® Session Manager running on a HP® Proliant DL360 G7 Server.	6.3.SP 5 6.3.5.0.635005
Avaya Aura® System Manager running on a HP® Proliant DL360 G7 Server.	6.3.5 Software Update Rev. 6.3.5.5.2017
Avaya Session Border Controller for Enterprise on a Dell R210 V2 Server	6.2.1.Q07
Avaya Deskphones	1110: 0623C8T (UniStim) 1120: 0624C8T (UniStim) 1165: 0626C8T (UniStim) 1120: 04.01.15.00 (SIP) M3904: --
Avaya 2050 IP Softphone	4.4 Service Pack 1 (Build 067)
<b>Frontier Communications</b>	
Metaswitch CFS Soft Switch	7.3.0.00
Acme Packet Net-Net SBC	6.2m8p4

### Signaling Server Service Updates & Patches:

#### SUs:

cs1000-dmWeb-7.65.16.22-1.i386.000  
tzdata-2013c-2.el5.i386.001  
cs1000-linuxbase-7.65.16.22-02.i386.000  
cs1000-cs1000WebService\_6-0-7.65.16.21-00.i386.000  
cs1000-Jboss-Quantum-7.65.16.22-3.i386.000  
cs1000-pd-7.65.16.21-00.i386.000  
cs1000-shared-carrdtct-7.65.16.21-01.i386.000  
cs1000-shared-tpselect-7.65.16.21-01.i386.000  
cs1000-dbcom-7.65.16.21-00.i386.000  
cs1000-patchWeb-7.65.16.22-1.i386.000  
cs1000-shared-xmsg-7.65.16.21-00.i386.000

cs1000-cs-7.65.P.100-02.i386.000  
cs1000-tps-7.65.16.21-11.i386.000  
cs1000-mscAnnc-7.65.16.21-02.i386.001  
cs1000-mscAttn-7.65.16.21-04.i386.001  
cs1000-mscConf-7.65.16.21-02.i386.001  
cs1000-mscMusc-7.65.16.21-02.i386.001  
cs1000-mscTone-7.65.16.21-03.i386.001  
cs1000-sps-7.65.16.21-8.i386.000  
cs1000-shared-omm-7.65.16.21-2.i386.000  
cs1000-baseWeb-7.65.16.22-1.i386.000  
cs1000-csmWeb-7.65.16.22-1.i386.000  
cs1000-gk-7.65.16.21-01.i386.000  
cs1000-csoneksvrmgr-7.65.16.22-1.i386.000  
cs1000-snmp-7.65.16.21-00.i686.000  
cs1000-emWebLocal\_6-0-7.65.16.22-1.i386.000  
cs1000-ftpkg-7.65.16.22-1.i386.000  
cs1000-ipsec-7.65.16.22-1.i386.000  
cs1000-vtrk-7.65.16.22-4.i386.000  
cs1000-cppmUtil-7.65.16.22-1.i686.000  
cs1000-oam-logging-7.65.16.22-3.i386.000  
cs1000-bcc-7.65.16.22-6.i386.000  
cs1000-emWeb\_6-0-7.65.16.22-5.i386.000

#####

Patches:

p31484\_1

### **MGC Loadware:**

Base loadware version: 100+

DSP1AB07.LW  
DSP2AB07.LW  
DSP3AB07.LW  
DSP4AB07.LW  
DSP5AB07.LW  
UDTCAB21.LW  
MGCCDC03.LW

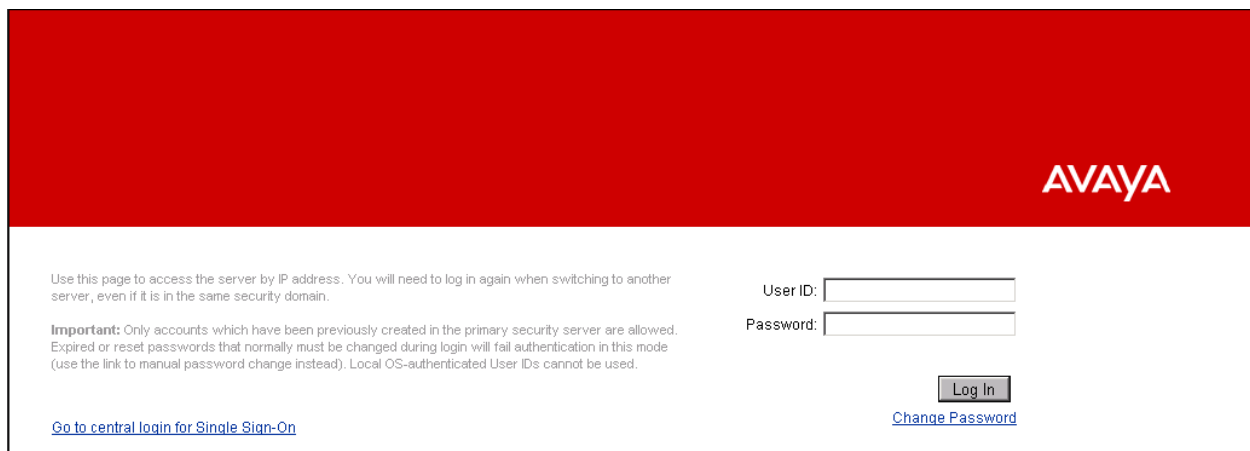
## 5. Configure Avaya Communication Server 1000E

These Application Notes assume that the basic configuration of the Avaya Communication Server 1000 has already been completed. For further information please consult the documentation listed in **References in Section 11**.

This section describes the procedures required in the CS1000 to interoperate with the Frontier Communications SIP Trunking service, where a two-way SIP Trunk was created between the CS1000 and Session Manager to carry traffic to and from the service provider. The section additionally covers administration steps required for extensions used during the tests.

### 5.1. Login to the Avaya Communication Server 1000E

Open an instance of a web browser and connect to the Avaya Unified Communication Management (AUCM) GUI at the following address: <http://<AUCM IP address>> Log in using an appropriate **User ID** and **Password**.



Use this page to access the server by IP address. You will need to log in again when switching to another server, even if it is in the same security domain.

**Important:** Only accounts which have been previously created in the primary security server are allowed. Expired or reset passwords that normally must be changed during login will fail authentication in this mode (use the link to manual password change instead). Local OS-authenticated User IDs cannot be used.

[Go to central login for Single Sign-On](#)

User ID:

Password:

[Change Password](#)

The **Avaya Unified Communications Management Elements** screen is displayed. Click on the **Element Name** corresponding to the **CS1000 Element Type**, as highlighted below.

Host Name: 172.16.20.60 Software Version: 02.30.0086.00(6653) User Name admin

### Elements

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

<input type="checkbox"/>	Element Name	Element Type	Release	Address	Description
<input type="checkbox"/>	<b>EM on cs1k</b>	CS1000	7.6	172.16.21.61	New element.
<input type="checkbox"/>	cs1k.avaya.lab.com (primary)	Linux Base	7.6	172.16.20.61	Base OS element.
<input type="checkbox"/>	172.16.21.62	Media Gateway Controller	7.6	172.16.21.62	New element.

The CS1000 Element Manager **System Overview** page is displayed next, as shown below.

Managing: **172.16.21.61** Username: admin  
System Overview

### System Overview

IP Address: 172.16.21.61  
Type: Avaya Communication Server 1000E CPMG128 Linux  
Version: 4421  
Release: 765 P +

## 5.2. Administer a 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 that the basic configuration has been completed and that a Node has already been created. This section describes the steps for configuring a Node (Node ID 1006) in the CS1000 IP network to work with the Frontier Communications network.

Select **System** → **IP Network** → **Nodes: Servers, Media Cards**. Following is the display of the **IP Telephony Nodes** page. Then click on the Node ID of the CS1000 Element (i.e., 1006).

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation tree with 'Nodes: Servers, Media Cards' selected. The main content area displays the 'IP Telephony Nodes' page. At the top, it shows 'Managing: 172.16.21.61 Username: admin' and the breadcrumb 'System > IP Network > IP Telephony Nodes'. Below this, there are buttons for 'Add...', 'Import...', 'Export...', and 'Delete', along with 'Print | Refresh'. A table lists the nodes:

Node ID	Components	Enabled Applications	ELAN IP	Node/TLAN IPv4	Node/TLAN IPv6	Status
1006	1	SIP Line, LTPS, IP Media Services, Gateway (SIPGw)	-	172.16.20.60	-	Synchronized

Below the table, there are checkboxes for 'Show: Nodes', 'Component servers and cards', and 'IPv6 address'.

The **Node Details** screen is displayed below. The **Node IPv4 Address** is a virtual address which corresponds to the TLAN IP address of the Signaling Server, SIP Signaling Gateway. This IP address will be needed when configuring Session Manager with a SIP Entity for Avaya CS1000E later in **Section 6.5**.

The screenshot shows the AVAYA CS1000 Element Manager interface for the 'Node Details' page. The left sidebar is the same as in the previous screenshot. The main content area displays 'Node Details (ID: 1006 - SIP Line, LTPS, IP Media Services, Gateway (SIPGw))'. The page contains several form fields:

- Node ID: 1006
- Call server IP address: 172.16.21.61
- TLAN address type: IPv4 only (selected)
- Embedded LAN (ELAN): Gateway IP address: 172.16.21.254, Subnet mask: 255.255.255.0
- Telephony LAN (TLAN): Node IPv4 address: 172.16.20.60 (highlighted with a red box), Subnet mask: 255.255.255.0
- Node IPv6 address: (empty field)

At the bottom, there are 'Save' and 'Cancel' buttons. Below the form is the 'Associated Signaling Servers & Cards' section, which includes a table:

Hostname	Type	Deployed Applications	ELAN IP	TLAN IPv4	Role
cs1k	Signaling_Server	SIP Line, LTPS, Gateway, PD, Presence Publisher, IP Media Services	172.16.21.61	172.16.20.61	Leader

## 5.2.2. Administer Terminal Proxy Server

On the **Node Details** page, scroll down and select the **Terminal Proxy Server (TPS)** link as shown below.

AVAYA CS1000 Element Manager

Managing: 172.16.21.61 Username: admin  
System > IP Network > IP Telephony Nodes > Node Details

Node Details (ID: 1006 - SIP Line, LTPS, IP Media Services, Gateway ( SIPGw ))

Subnet mask: 255.255.255.0 \* Subnet mask: 255.255.255.0 \*  
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

\* Required Value. Save Cancel

The **UNISlim Line Terminal Proxy Server (LTPS) Configuration Details** screen is displayed below. Check the **Enable proxy service on this node** check box and then click **Save**.

AVAYA CS1000 Element Manager

Managing: 172.16.21.61 Username: admin  
System > IP Network > IP Telephony Nodes > Node Details > UNISlim Line Terminal Proxy Server (LTPS) Configuration

Node ID: 1006 - UNISlim Line Terminal Proxy Server (LTPS) Configuration Details

Firmware | DTLS | Network Connect Server

UNISlim Line Terminal Proxy Server:  Enable proxy service on this node

**Firmware**

IP address: 0.0.0.0  
Full file path: download/firmwa  
Server Account/User ID:   
Password:

**DTLS**

DTLS policy: Off

Options:  Client authentication  
 Periodic re-keying

**Network Connect Server**

Primary network connect server (TL AN) IP address: 0.0.0.0

\* Required Value. Note: Changes made on this page will NOT be transmitted until the Node is also saved. Save Cancel

### 5.2.3. Administer Quality of Service (QoS)

On the **Node Details** page, scroll down on the top window and select the **Quality of Service (QoS)** link as shown below.

The screenshot shows the AVAYA CS1000 Element Manager interface. The top navigation bar includes the AVAYA logo, the title "CS1000 Element Manager", and "Help | Logout" links. The main content area is titled "Node Details (ID: 1006 - SIP Line, LTPS, IP Media Services, Gateway ( SIPGw ))". The left sidebar contains a tree view with categories like "UCM Network Services", "System", and "Nodes: Servers, Media Cards". The "Quality of Service (QoS)" link is highlighted in red in the sidebar and also in the main content area. The main content area shows "IP Telephony Node Properties" and "Applications (click to edit configuration)". The "Quality of Service (QoS)" link is highlighted in red in the "IP Telephony Node Properties" list. The "Applications" list includes "SIP Line", "Terminal Proxy Server (TPS)", "Gateway (SIPGw)", "Personal Directories (PD)", "Presence Publisher", and "IP Media Services".

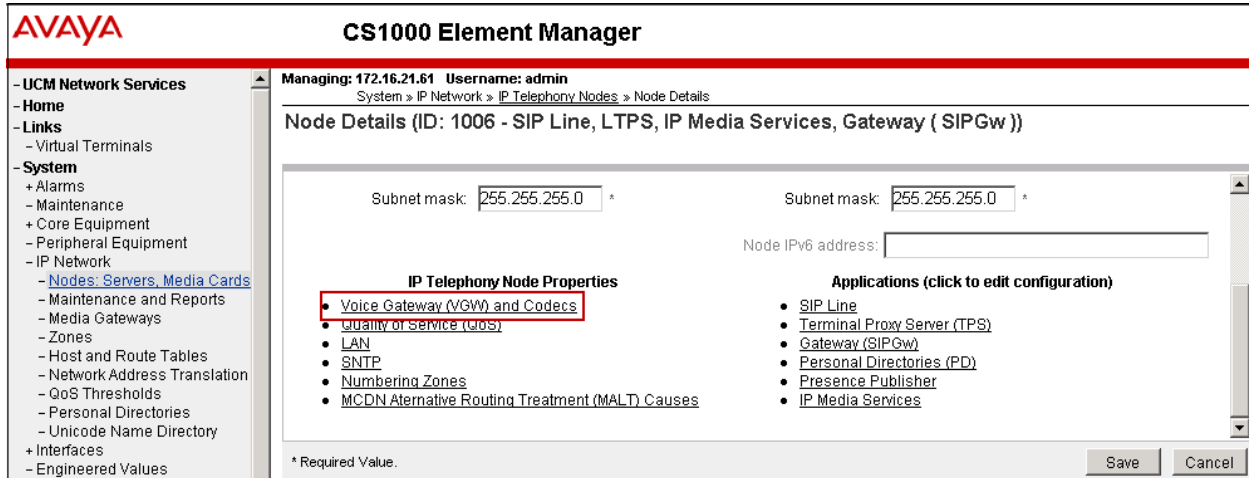
The **Quality of Service (QoS)** screen shown below will be displayed. Default **Diffserv Codepoint (DSCP)** values were used during the tests. Click the **Save** button.

The screenshot shows the AVAYA CS1000 Element Manager interface. The top navigation bar includes the AVAYA logo, the title "CS1000 Element Manager", and "Help | Logout" links. The main content area is titled "Node ID: 1006 - Quality of Service (QoS)". The left sidebar contains a tree view with categories like "UCM Network Services", "System", and "Nodes: Servers, Media Cards". The "Quality of Service (QoS)" link is highlighted in red in the sidebar and also in the main content area. The main content area shows "Diffserv Codepoint (DSCP)" configuration. The "Control packets" field is highlighted in red and contains the value "40". The "Voice packets" field is highlighted in red and contains the value "46". The "802.1Q bits value (802.1P)" field contains the value "5". The "Save" button is highlighted in red.

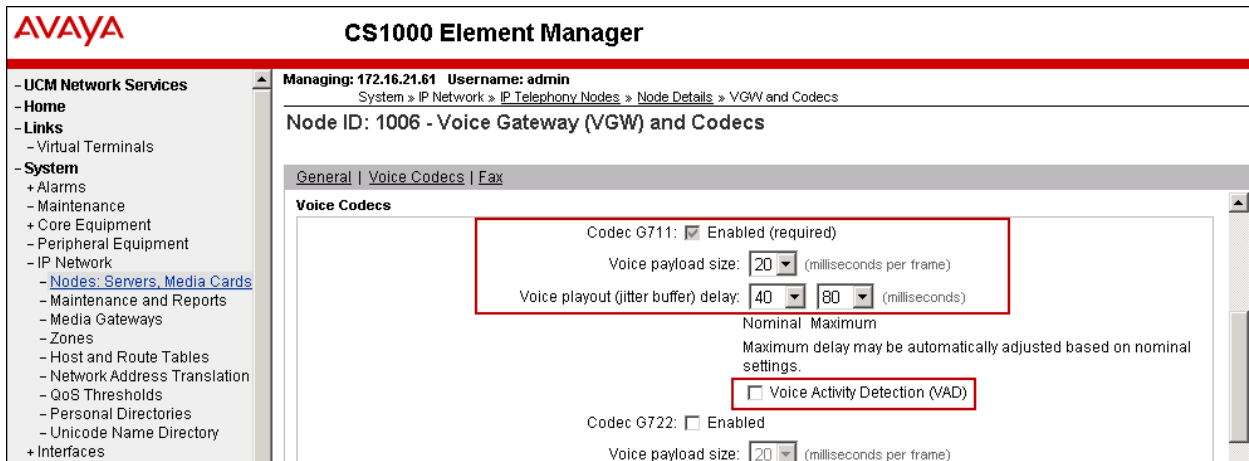
## 5.2.4. Voice Gateway and Codecs

Frontier Communications supports codecs **G.711U** and **G.729A** with **Voice Activity Detection (VAD)** disabled.

On the **Node Details** page, scroll down on the top window and select **Voice Gateway (VGW) and Codecs** as shown.

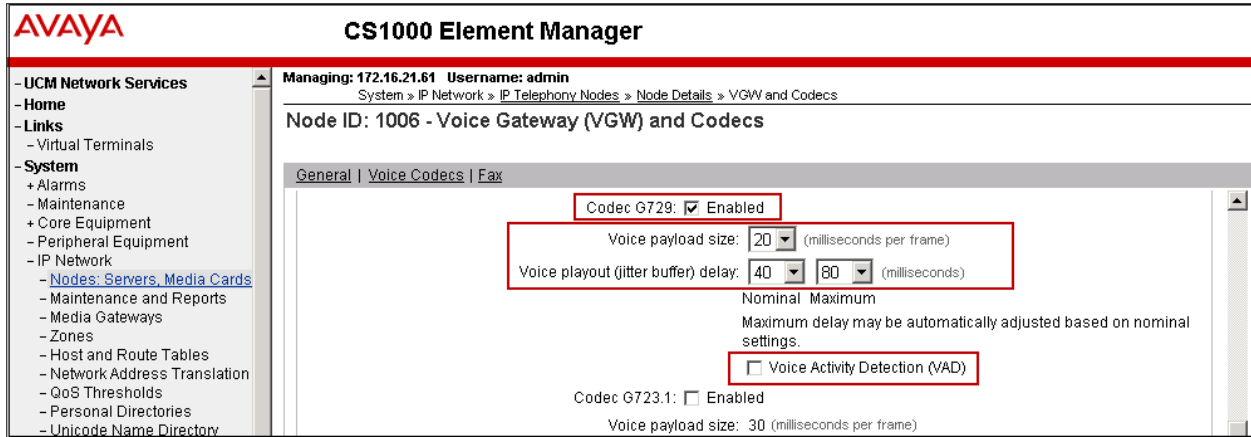


The **Voice Gateway (VGW) and Codec** screen is displayed. Scroll down to the **Voice Codecs** area and set the parameters for codec G.711. Note that **Codec G711** is enabled by default. Ensure that **Voice Activity Detection (VAD)** is unchecked.



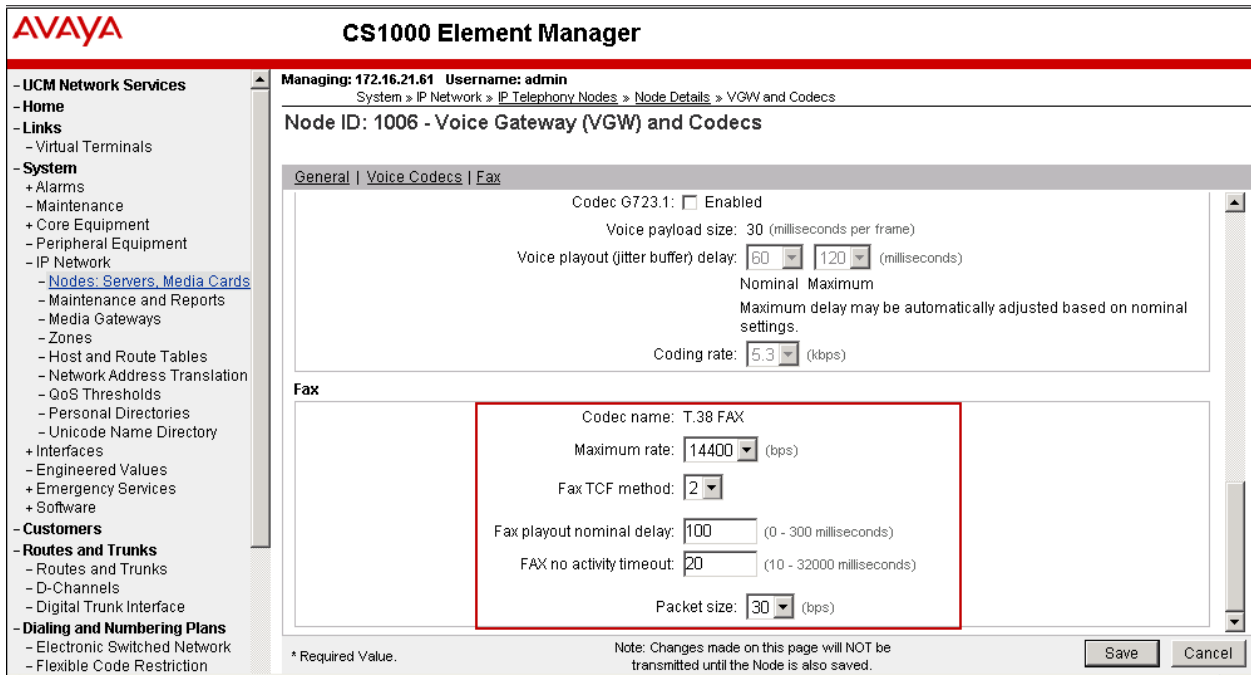


The values for the **G729** Voice Codec are shown. Ensure that **Codec G729** is checked and **Voice Activity Detection (VAD)** is unchecked as shown below.



During the compliance test, Frontier supported T.38 fax calls on the inbound direction to the CS1000 and allowed G711U pass-through fax calls on outbound calls to the PSTN.

Scroll down to the **Fax** section. The screen below shows the default parameters used for T.38 fax in the reference configuration.



Scroll up to the General section, and ensure that the boxes for **Modem/Fax Pass Through** and **V.21 Fax tone detection** are checked. Click the **Save** button.

**AVAYA CS1000 Element Manager**

Managing: 172.16.21.61 Username: admin  
System » IP Network » IP Telephony Nodes » Node Details » VGW and Codecs

Node ID: 1006 - Voice Gateway (VGW) and Codecs

General | Voice Codecs | 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

**Voice Codecs**

Codec G711:  Enabled (required)

Voice payload size: 20 (milliseconds per frame)

Voice playout (jitter buffer) delay: 40 100 (milliseconds)

\* Required Value. Note: Changes made on this page will NOT be transmitted until the Node is also saved.

Save Cancel

## 5.2.5. SIP Gateway

On the **Node Details** page, scroll down on the top window and select **Gateway (SIPGw)**.

**AVAYA CS1000 Element Manager**

Managing: 172.16.21.61 Username: admin  
System » IP Network » IP Telephony Nodes » Node Details

Node Details (ID: 1006 - SIP Line, LTPS, IP Media Services, Gateway (SIPGw))

Subnet mask: 255.255.255.0 \*      Subnet mask: 255.255.255.0 \*  
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

\* Required Value.      Save      Cancel

Under the **General** tab of the **Virtual Trunk Gateway Configuration Details** screen, enter the following values. Use default values for the remaining fields.

- **Vtrk gateway application:** Select *SIP Gateway (SIPGw)*.
- **SIP domain name:** Enter the SIP domain for the customer network. In the sample configuration, *avaya.lab.com* was used.
- **Local SIP port:** Gateway listening port. Port *5087* was used.
- **Gateway endpoint name:** Enter a descriptive name.
- **Application node ID:** Node *1006* is used, as previously seen in **Section 5.2.1**.

Node ID: 1006 - Virtual Trunk Gateway Configuration Details

General | SIP Gateway Settings | SIP Gateway Services

Vtrk gateway application:  Enable gateway service on this node

**General**

Vtrk gateway application: SIP Gateway (SIPGw) ▼  
SIP domain name: avaya.lab.com \*  
Local SIP port: 5087 \* (1 - 65535)  
Gateway endpoint name: CS1KGateway \*  
Gateway password: [ ] \*  
Application node ID: 1006 \* (0-9999)  
Enable failsafe NRS:

Note: FailSafe NRS will be enabled only on those servers in the node where NRS application is not deployed.

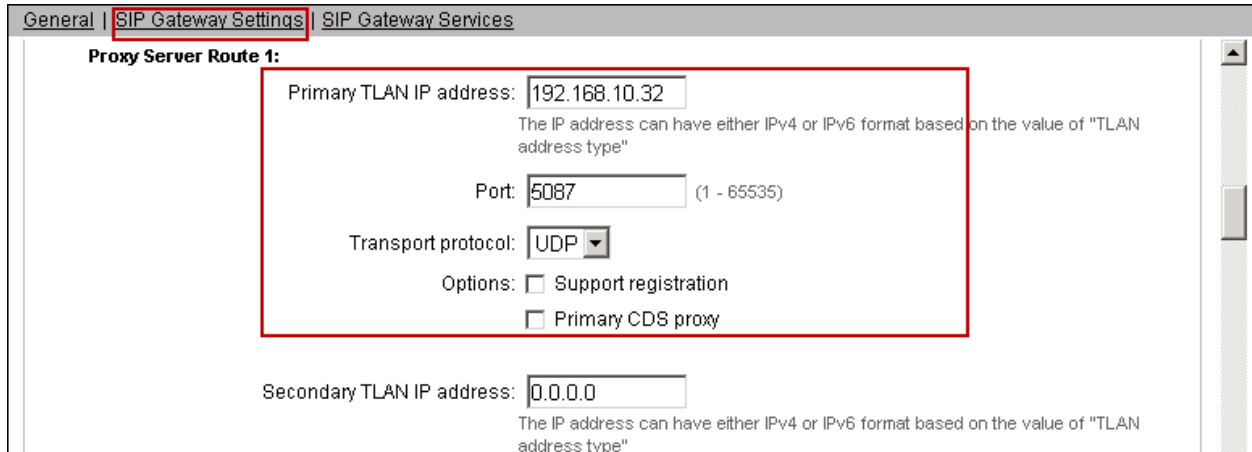
**Virtual Trunk Network Health Monitor**

Monitor IP addresses (listed below)  
Information will be captured for the IP addresses listed below.  
Monitor IP: [ ] Add  
Monitor addresses: [ ] Remove

\* Required Value.      Note: Changes made on this page will NOT be transmitted until the Node is also saved.      Save      Cancel

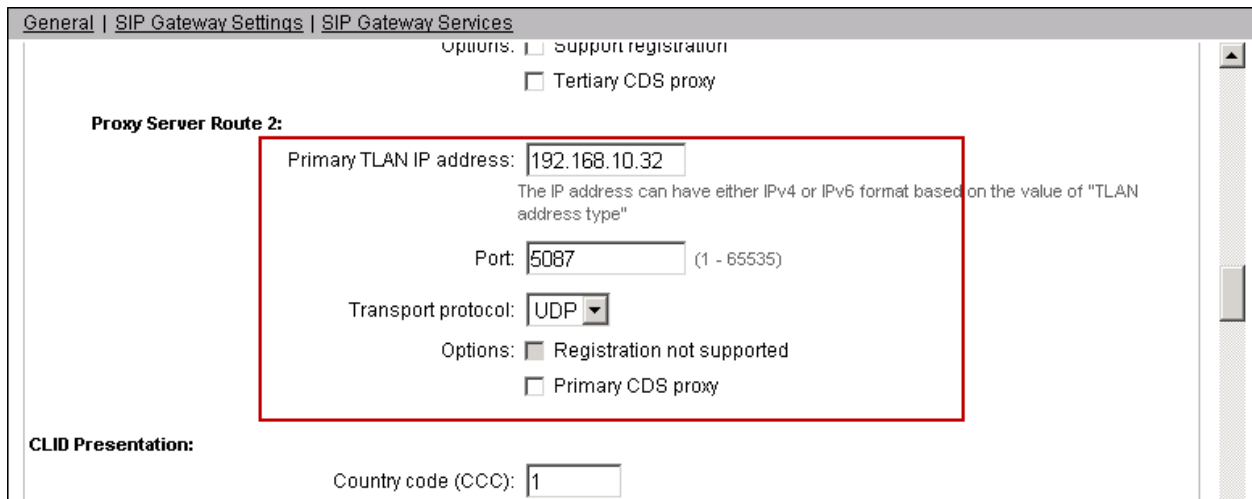
Click on the **SIP Gateway Settings** tab. Enter the following parameters under **Proxy Server Route 1**. Use default values for remaining fields.

- **Primary TLAN IP address:** Enter the IP address of the Session Manager signaling interface. In the sample configuration this is **192.168.10.32**.
- **Port:** Enter the port where SIP traffic will be sent to Session Manager. Port **5087** was used.
- **Transport protocol:** **UDP** was used.
- **Options:** Leave both **Support registration** and **Primary CDS proxy** boxes unchecked.



The screenshot shows the 'SIP Gateway Settings' configuration page. The 'Proxy Server Route 1' section is highlighted with a red box. The fields are: Primary TLAN IP address: 192.168.10.32; Port: 5087; Transport protocol: UDP; Options: Support registration (unchecked), Primary CDS proxy (unchecked). Below this, the Secondary TLAN IP address is 0.0.0.0.

Scroll down and repeat these steps for the **Proxy Server Route 2**.



The screenshot shows the 'SIP Gateway Settings' configuration page for 'Proxy Server Route 2'. The 'Proxy Server Route 2' section is highlighted with a red box. The fields are: Primary TLAN IP address: 192.168.10.32; Port: 5087; Transport protocol: UDP; Options: Registration not supported (checked), Primary CDS proxy (unchecked). Below this, the 'CLID Presentation' section has a Country code (CCC) of 1.

Scroll down to the **SIP URI Map** section. The entries shown below are the default values, used during the compliance test. Click the **Save** button.

General | SIP Gateway Settings | SIP Gateway Services

National (NN):   <CCC><NN>  
International:   <International number>

**SIP URI Map:**

Public E.164 domain names	Private domain names
National: <input type="text"/>	UDP: <input type="text" value="udp"/>
Subscriber: <input type="text"/>	CDP: <input type="text" value="cdp.udp"/>
Special number: <input type="text" value="PublicSpecial"/>	Special number: <input type="text" value="PrivateSpecial"/>
Unknown: <input type="text" value="PublicUnknown"/>	Vacant number: <input type="text" value="PrivateUnknown"/>
	Unknown: <input type="text" value="UnknownUnknown"/>

**SIP Gateway Services**

**SIP Converged Desktop:**  Enable CD service

Service DN:  Used for making VTRK call from agent.

Converged telephone call forward DN:

\* Required Value. Note: Changes made on this page will NOT be transmitted until the Node is also saved.

## 5.2.6. Synchronize the Node Configuration

After completing the previous section, the screen returns to the **Node Details** page shown below. Click the **Save** button.

AVAYA CS1000 Element Manager

Managing: 172.16.21.61 Username: admin  
System » IP Network » IP Telephony Nodes » Node Details

Node Details (ID: 1006 - SIP Line, LTPS, IP Media Services, Gateway ( SIPGw ))

Node ID:  \* (0-9999)

Call server IP address:  \* TLAN address type:  IPv4 only  
 IPv4 and IPv6

**Embedded LAN (ELAN)** **Telephony LAN (TLAN)**

Gateway IP address:  \* Node IPv4 address:  \*

Subnet mask:  \* Subnet mask:  \*

Node IPv6 address:

\* Required Value.

The **Node Saved** screen is displayed. Click on the **Transfer Now** button.

AVAYA CS1000 Element Manager

Managing: 172.16.21.61 Username: admin  
System » IP Network » IP Telephony Nodes » Node Saved

Node Saved

Node ID: 1006 has been saved on the call server.

The new configuration must also be transferred to associated servers and media cards.

You will be given an option to select individual servers, or transfer to all.

You may initiate a transfer manually at a later time.

The **Synchronize Configuration Files** screen is displayed. Check the Signaling Server checkbox and click on **Start Sync**. The **Synchronization Status** field will update from **Sync required** (as shown on the next page) to **Synchronized** (not shown). After synchronization completes, check the Signaling Server check box and click on the **Restart Applications**.

AVAYA CS1000 Element Manager

Managing: 172.16.21.61 Username: admin  
System » IP Network » IP Telephony Nodes » Synchronize Configuration Files

Synchronize Configuration Files (Node ID <1006>)

Note: Select components to synchronize their configuration files with call server data. This process transfers server INI files to selected components, and requires a restart\* of applications on affected server(s) when complete.

<input checked="" type="checkbox"/>	Hostname	Type	Applications	Synchronization Status
<input checked="" type="checkbox"/>	cs1k	Signaling_Server	SIP Line, LTPS, Gateway, PD, Presence Publisher, IP Media Services	Sync required

\* Application restart is only required for initial system configuration or if changes have been made to general LAN configurations, SNMP settings, SIP and H323 Gateway settings, network connectivity related parameters like ports and IP address, enabling or disabling services, or adding or removing application servers.

### 5.3. Administer Virtual Super-Loop

Select **System** → **Core Equipments** → **Superloops** from the left pane to display the **Superloops** screen. If the Superloop does not exist, click “**Add**” button to create a new one. In the sample configuration, Superloop 4 is used by the Media Gateway, Superloop 8 is used by the IP phones and Superloop 48 is used by virtual SIP trunks.

Managing: 172.16.21.61 Username: admin  
System » Core Equipment » Superloops

#### Superloops

Add... Delete Refresh

	Superloop Number	Superloop Type
1	4	IPMG
2	8	Virtual
3	12	Virtual
4	16	Phantom
5	48	Virtual
6	52	Virtual

### 5.4. Enable Voice Codec on Media Gateways.

From the left menu of the Element Manager page, select **System** → **IP Network** → **Media Gateways**. Click the link under the **Type** field on the Media Gateway to be modified.

Managing: 172.16.21.61 Username: admin  
System » IP Network » Media Gateways

#### Media Gateways

Add... Digital Trunking... Reboot Delete Virtual Terminal More Actions Refresh

	IPMG	IP Address	Zone	Type
0	004.00	172.16.21.62	0	MGS

Under **VGW and IP phone codec profile** ensure that the boxes for **Enable modem/fax pass through mode** and **Enable V.21 FAX tone detection** are checked.

**AVAYA CS1000 Element Manager**

**- VGW and IP phone codec profile**

- Enable echo canceller
- Echo canceller tail delay: 128 (milliseconds)
- Enable dynamic attenuation
- Voice activity detection threshold: 1 (0 - 4 DBM)
- Idle noise level: 0 (0 - 1 DBM)
- R factor calculation
- DTMF tone detection
- Enable low latency mode
- Remove DTMF delay (squelch DTMF from TDM to IP)
- Enable modem/fax pass through mode**
- Enable V.21 FAX tone detection**
- Fax TCF method: 2
- FAX maximum rate: 14400 (bps)
- FAX playout nominal delay: 100 (0 - 300 milliseconds)
- FAX no activity timeout: 20 (10 - 32000 milliseconds)
- FAX packet size: 30

Scroll down and expand the **Codec G711** section. Note that G711 is enabled by default. Uncheck **VAD** for codec **G711**. Expand **Codec G729A**, ensure that the **Select** box is checked for **Codec G729A** and uncheck **VAD** for codec **G729A** as shown below. Scroll down to the bottom of the page and click **Save** (not shown).

**AVAYA CS1000 Element Manager**

**- Codec G711** **Select**

Codec name: G711

Voice payload size: 20 (ms/frame)

Voice playout (jitter buffer) nominal delay: 40

Voice playout (jitter buffer) maximum delay: 80

VAD

**- Codec G729A** **Select**

Codec name: G729A

Voice payload size: 20 (ms/frame)

Voice playout (jitter buffer) nominal delay: 40

Voice playout (jitter buffer) maximum delay: 80

VAD

+ Codec G723.1 **Select**

+ Codec T38 FAX **Select**



## 5.5. Administer Zones and Bandwidth

Zone configuration can be used to control codec selection and bandwidth management. To configure, select **System** → **IP Network** → **Zones** on the left panel. Click on **Bandwidth Zones** as shown below.

The screenshot shows the AVAYA CS1000 Element Manager interface. The top header includes the AVAYA logo, the title 'CS1000 Element Manager', and a 'Help' link. Below the header, the left sidebar contains a navigation tree with the following items: - UCM Network Services, - Home, - Links, - Virtual Terminals, - System, + Alarms, - Maintenance, - Core Equipment, - Loops, - Superloops, - MSDLMISP Cards, - Conference/TDS/Multifrequen, - Tone Senders and Detectors, - Peripheral Equipment, - IP Network, - Nodes: Servers, Media Cards, - Maintenance and Reports, - Media Gateways, - Zones (highlighted), and - Host and Route Tables. The main content area displays the 'Zones' title and the following text: 'Zones are used to group related information for either bandwidth or dial plan numbering purposes.' Below this, there are two sub-sections: 'Bandwidth Zones' (highlighted with a red box) and 'Numbering Zones'. The text for 'Bandwidth Zones' reads: 'Bandwidth zones are used for alternate routing of calls between IP stations and also for bandwidth management.' The text for 'Numbering Zones' reads: 'Numbering zones are used to route calls through a centralized call server.'

On the **Bandwidth Zones** screen (not shown), select **Add** to create a new zone, or select a specific zone and click on **Edit** and **Zone Basic Properties and Bandwidth Management** (not shown) to modify an existing one.

### 5.5.1. Bandwidth Zones for virtual SIP trunks

The screen below shows the settings for zone 2, used by the virtual trunk to the service provider. The **INTRA\_STGY** and **INTER\_STGY** fields are set to **Best Bandwidth (BB)**. By setting this, codec G.729 is preferred over codec G.711 on calls over the virtual trunk, which was the codec order preferred by Frontier. **ZBRN** is set to **VTRK**.

AVAYA CS1000 Element Manager

Managing: 172.16.21.61 Username: admin  
System » IP Network » Zones » Bandwidth Zones » Bandwidth Zones 2 » Edit Bandwidth Zone » Zone Basic Property and Bandwidth Management

#### Zone Basic Property and Bandwidth Management

Input Description	Input Value
Zone Number (ZONE):	2 * (1 - 8000)
Intrazone Bandwidth (INTRA_BW):	1000000 (0 - 10000000)
Intrazone Strategy (INTRA_STGY):	Best Bandwidth (BB)
Interzone Bandwidth (INTER_BW):	1000000 (0 - 10000000)
Interzone Strategy (INTER_STGY):	Best Bandwidth (BB)
Resource Type (RES_TYPE):	Shared (SHARED)
Zone Intent (ZBRN):	VTRK (VTRK)
Description (ZDES):	VTRKZONE_G729_FIRST

Submit Refresh Cancel

The screen below shows the settings for zone 4, which was alternatively used during the compliance test for the verification of voice codec G.711U. In this case the **INTRA\_STGY** and **INTER\_STGY** fields are set to **Best Quality (BQ)**. By setting this, codec G.711 is preferred over codec G.729 on calls over the virtual trunk.

AVAYA CS1000 Element Manager

Managing: 172.16.21.61 Username: admin  
System » IP Network » Zones » Bandwidth Zones » Zone Basic Property and Bandwidth Management

#### Zone Basic Property and Bandwidth Management

Input Description	Input Value
Zone Number (ZONE):	4 * (1 - 8000)
Intrazone Bandwidth (INTRA_BW):	1000000 (0 - 10000000)
Intrazone Strategy (INTRA_STGY):	Best Quality (BQ)
Interzone Bandwidth (INTER_BW):	1000000 (0 - 10000000)
Interzone Strategy (INTER_STGY):	Best Quality (BQ)
Resource Type (RES_TYPE):	Shared (SHARED)
Zone Intent (ZBRN):	VTRK (VTRK)
Description (ZDES):	VTRK_Zone_G711_First

\* Required value. Save Cancel

## 5.5.2. Bandwidth Zones for IP Telephones

Two bandwidth zones (zones 1 and 5) were similarly created for the use of IP telephones in the CS1000.

The screen below shows the settings for zone 5, which uses G.711 as the preferred codec. The **INTRA\_STGY** and **INTER\_STGY** fields are set to *Best Quality (BQ)*. **ZBRN** is set to *MO* for IP telephones.

AVAYA CS1000 Element Manager

Managing: 172.16.21.61 Username: admin  
System > IP Network > Zones > Bandwidth Zones > Bandwidth Zones 5 > Edit Bandwidth Zone > Zone Basic Property and Bandwidth Management

### Zone Basic Property and Bandwidth Management

Input Description	Input Value
Zone Number (ZONE):	5 (1 - 8000)
Intrazone Bandwidth (INTRA_BW):	1000000 (0 - 10000000)
Intrazone Strategy (INTRA_STGY):	Best Quality (BQ)
Interzone Bandwidth (INTER_BW):	1000000 (0 - 10000000)
Interzone Strategy (INTER_STGY):	Best Quality (BQ)
Resource Type (RES_TYPE):	Shared (SHARED)
Zone Intent (ZBRN):	MO (MO)
Description (ZDES):	IPPHONES_G711_FIRST
Location Name (ZNAME):	
Reserved BW Block Size (RESERVED_BW_SIZE):	0 (200 - 9999999)

Submit Refresh Cancel

The screen below shows the settings for zone 1, which uses G.729 as the preferred codec. The **INTRA\_STGY** and **INTER\_STGY** fields are set to *Best Bandwidth (BB)*. **ZBRN** is set to *MO* for IP telephones.

AVAYA CS1000 Element Manager

Managing: 172.16.21.61 Username: admin  
System > IP Network > Zones > Bandwidth Zones > Bandwidth Zones 1 > Edit Bandwidth Zone > Zone Basic Property and Bandwidth Management

### Zone Basic Property and Bandwidth Management

Input Description	Input Value
Zone Number (ZONE):	1 (1 - 8000)
Intrazone Bandwidth (INTRA_BW):	1000000 (0 - 10000000)
Intrazone Strategy (INTRA_STGY):	Best Bandwidth (BB)
Interzone Bandwidth (INTER_BW):	1000000 (0 - 10000000)
Interzone Strategy (INTER_STGY):	Best Bandwidth (BB)
Resource Type (RES_TYPE):	Shared (SHARED)
Zone Intent (ZBRN):	MO (MO)
Description (ZDES):	IPPHONES_G729_FIRST
Location Name (ZNAME):	
Reserved BW Block Size (RESERVED_BW_SIZE):	0 (200 - 9999999)

Submit Refresh Cancel

## 5.6. Virtual D Channel, Routes and Trunks

### 5.6.1. Administer Virtual D-Channel

Select **Routes and Trunks** → **D-Channels** from the left pane to display the **D-Channels** screen. In the **Choose a D-Channel Number** field, select an available D-channel from the drop-down list as shown below. Click on the **to Add** button.

**AVAYA** **CS1000 Element Manager** Help

Managing: **172.16.21.61** Username: admin  
Routes and Trunks » D-Channels

### D-Channels

**Maintenance**

- [D-Channel Diagnostics](#) (LD 96)
- [Network and Peripheral Equipment](#) (LD 32, Virtual D-Channels)
- [MSDL Diagnostics](#) (LD 96)
- [TMDI Diagnostics](#) (LD 96)
- [D-Channel Expansion Diagnostics](#) (LD 48)

**Configuration**

Choose a D-Channel Number:  and type:

- Channel: 0	Type: DCH	Card Type: DCIP	Description: VoIP	<input type="button" value="Edit"/>
- Channel: 96	Type: DCH	Card Type: DCIP	Description: SIPL_DCH	<input type="button" value="Edit"/>

The **D-Channels 0 Property Configuration** screen is displayed next. The screen below shows the settings for **D-Channel 0**, added for testing. Enter the following values for the specified 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

**D-Channels 0 Property Configuration**

**- Basic Configuration**

Input Description	Input Value
Action Device And Number (ADAN):	DCH
D channel Card Type:	DCIP
Designator:	VoIP
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="text"/> <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
Central Office switch type:	100% compatible with Bellcore standard (STD)
Integrated Services Signaling Link Maximum:	4000 Range: 1 - 4000
Signalling server resource capacity:	3700 Range: 0 - 3700

On the previous screen, scroll down and expand the **Basic options (BSCOPT)** section. Click on the **Edit** button for the **Remote Capabilities** attribute as shown below.

**- Basic options (BSCOPT)**

Primary D-channel for a backup DCH:  Range: 0 - 254

- PINX customer number:

- Progress signal:

- Calling Line Identification:

- Output request Buffers:

- D-channel transmission Rate:

- Channel Negotiation option:

- Remote Capabilities:

**+ - Change protocol timer value (TIMR)**

- B channel Service messaging.:

**+ Advanced options (ADVOPT)**

**- Feature Packages**

The **Remote Capabilities Configuration** page will appear. Check **MWI** and **ND2** (if mailboxes are present on the CS1K Call Pilot) checkboxes as shown below. Click on the **Return – Remote Capabilities** button (not shown).

**AVAYA CS1000 Element Manager** Help | Logout

- Media Gateways
- Zones
- Host and Route Tables
- Network Address Translation
- QoS Thresholds
- Personal Directories
- Unicode Name Directory
- + Interfaces
- Engineered Values
- + Emergency Services
- + Software
- **Customers**
- **Routes and Trunks**
- Routes and Trunks
- **D-Channels**
- Digital Trunk Interface
- **Dialing and Numbering Plans**
- Electronic Switched Network
- Flexible Code Restriction
- Incoming Digit Translation
- **Phones**
- Templates
- Reports

Diversion info. is sent using object identifier (DV10)  
 Rerouting requests processed using integer value (DV21)  
 Rerouting requests processed using object identifier (DV20)  
 Diversion info. sent. rerouting requests processed (DV31)  
 EuroISDN - div. info sent. rerouting req. processed (DV30)  
 Call transfer notification and invocation to EuroISDN (ECTO)  
 Malicious call identification (MCID)  
 MCDN QSIG conversion (MQC)  
 Remote D-channel is on a MSDL card (MSL)  
 **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)

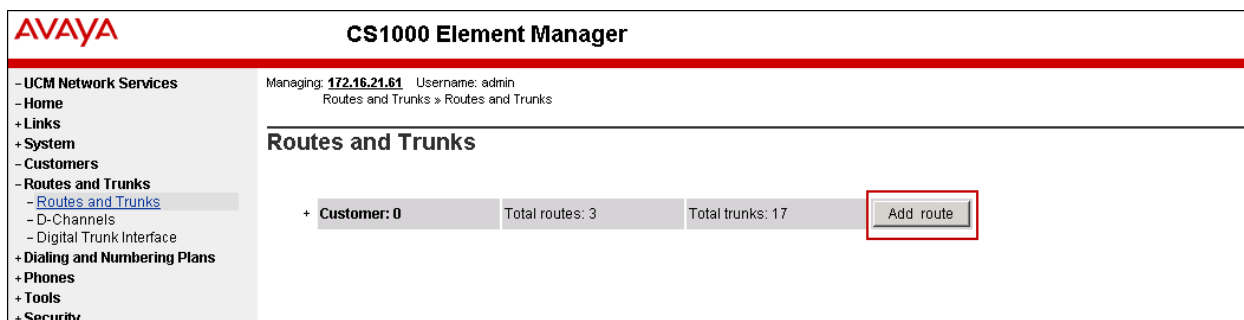
Scroll down to expand the **Advanced options (ADVOPT)** section. The entries shown below are the default values, used during the compliance test. Click on the **Submit** button (not shown).

**- Advanced options (ADVOPT)**

- Layer 3 call control message count per 5 second time interval:  Range: 60 - 350
- Number of Status Enquiry Messages sent within 128 ms:
- Map channel number to timeslots on a PRI2 loop:

## 5.6.2. Administer Virtual SIP Routes

Select **Routes and Trunks** → **Routes and Trunks** from the left pane to display the **Routes and Trunks** screen. In this example, **Customer 0** is being used. Click on the **Add route** button as shown below.



The **Customer 0, New Route Configuration** screen is displayed next. 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 below.

- **Route number (ROUT):** Select an available route number. Route **0** was used.
- **Designator field for trunk (DES):** A descriptive text.
- **Trunk type (TKTP):** *TIE*.
- **Incoming and outgoing trunk (ICOG):** *Incoming and Outgoing (IAO)*.
- **Access Code for the trunk route (ACOD):** An available access code.
- Check the box **The route is for a virtual trunk route (VTRK)**, to enable four additional fields to appear.
- For the **Zone for codec selection and bandwidth management (ZONE)** field, enter **2** (created in **Section 5.5.1**).
- For the **Node ID of signalling server of this route (NODE)** field, enter the node number **1006** (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. Scroll down to the bottom of the screen.
- **Mode of operation (MODE):** *Route uses ISDN Signalling Link (ISLD)*.
- **D channel number (DCH):** D-Channel number **0** (created in **Section 5.6.1**).
- **Interface type for route (IFC):** *Meridian M1 (SL1)*.

**AVAYA** CS1000 Element Manager Help | Logout

---

**Customer 0, Route 0 Property Configuration**

**- Basic Configuration**

Route data block (RDB) (TYPE): RDB

Customer number (CUST): 00

Route number (ROUT): 0

Designator field for trunk (DES): SERVICE PROVIDE

Trunk type (TKTP): TIE

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

Access code for the trunk route (ACOD): 7916 \*

Trunk type M911P (M911P):

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

- Zone for codec selection and bandwidth management (ZONE): 00002 (0 - 8000)

- Node ID of signaling server of this route (NODE): 1006 (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 (SBMM):

Integrated services digital network option (ISDN):

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

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

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

- **Network calling name allowed (NCNA):** Check box.
- **Network call redirection (NCRD):** Check box.
- **Insert ESN access code (INAC):** Check box.

**AVAYA** CS1000 Element Manager Help

---

**- Private network identifier (PNI):** 00001 (0 - 32700)

- Network calling name allowed (NCNA):

- Network call redirection (NCRD):

-- Trunk route optimization (TRO):

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

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

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

- Insert ESN access code (INAC):

- Integrated service access route (ISAR):

- Display of access prefix on CLID (DAPC):

- Mobile extension route (MBXR):

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

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

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

**+ Basic Route Options**

**+ Network Options**

**+ General Options**

**+ Advanced Configurations**



Under **Basic Route Options** set the following:

- **North American toll scheme (NATL):** Check box.
- **Incoming DID digit conversion on this route (IDC):** Check box.
- **Day IDC tree number (DCNO):** Enter **0**. This is defined later in **Section 5.7.7**.
- **Night IDC tree number (NDNO):** Enter **0**.

Click on the **Submit** button.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation tree with categories like UCM Network Services, Home, Links, System, Customers, Routes and Trunks, Dialing and Numbering Plans, Phones, and Tools. The main content area is titled 'Basic Route Options' and contains several configuration fields. The 'Calling number dialing plan (CNDP)' is set to 'Unknown (UKWN)'. The 'Attendant announcement (ATAN)' is set to 'No Attendant Announcement. (NO)'. The 'Billing number required (BILN)', 'Call detail recording (CDR)', 'Controls or timers (CNTL)', and 'Conventional (Tie trunk only) (CNVT)' options are all unchecked. The 'North American toll scheme (NATL)' checkbox is checked and highlighted with a red box. The 'Incoming DID digit conversion on this route (IDC)' checkbox is also checked and highlighted with a red box. Below this, the 'Day IDC tree number (DCNO)' and 'Night IDC tree number (NDNO)' are both set to '0', with a range of '(0 - 254)' indicated next to each. The 'Display external dialed digits (DEXT)' option is unchecked. The 'Multifrequency compelled or MFC signaling (MFC)' is set to 'No MFC (NO)'. The 'Process notification networked calls (PNNC)' option is unchecked. At the bottom of the configuration area, there are four buttons: 'Submit', 'Refresh', 'Delete', and 'Cancel'. The 'Submit' button is highlighted with a red box.

### 5.6.3. Administer Virtual Trunks

Select **Routes and Trunks** → **Routes and Trunks** from the left pane. On the **Routes and Trunks** screen, expand **Customer 0**. On the newly created **Route 0**, click the **Add trunk** button.

The screenshot shows the AVAYA CS1000 Element Manager interface. The top header includes the AVAYA logo, the title 'CS1000 Element Manager', and a 'Help' link. Below the header, the user information 'Managing: 172.16.21.61 Username: admin' and the breadcrumb 'Routes and Trunks > Routes and Trunks' are displayed. The main content area is titled 'Routes and Trunks' and contains a table with the following data:

Customer	Total routes	Total trunks	Actions	
- Customer: 0	3	17	Add route	
+ Route: 0	Type: TIE	Description: SERVICE PROVIDER	Edit	Add trunk
+ Route: 1	Type: IMUS	Description: MUSIC	Edit	Add trunk
+ Route: 96	Type: TIE	Description: SIPL_ROUTE	Edit	Add trunk

The **Customer 0, Route 0, Trunk 1 Property Configuration** screen is displayed on the next page. Enter the following values for the specified fields and retain the default values for the remaining fields. The **Multiple trunk input number (MTINPUT)** field (not shown) may be used to add multiple trunks in a single operation, or repeat the operation to add each trunk. In the sample configuration, 11 trunks were created.

- **Trunk data block (TYPE):** *IPTI* (IP Trunk).
- **Terminal Number (TN):** Available terminal number (created in **Section 5.3**).
- **Designator field for trunk (DES):** A descriptive text.
- **Extended Trunk (XTRK):** *VTRK* (Virtual trunk).
- **Member number (RTMB):** Current route number and starting member.
- **Start arrangement Incoming (STRI):** *Immediate (IMM)*.
- **Start arrangement Outgoing (STRO):** *Immediate (IMM)*.
- **Trunk Group Access Restriction (TGAR):** Desired trunk group access restriction level.
- **Channel ID for this trunk (CHID):** An available starting channel ID.

**AVAYA CS1000 Element Manager**

Managing: 172.16.21.61 Username: admin  
Routes and Trunks > Routes and Trunks > Customer 0, Route 0, Trunk 1 Property Configuration

### Customer 0, Route 0, Trunk 1 Property Configuration

**- 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:

**+ Advanced Trunk Configurations**

Click on **Edit Class of Service** (shown on previous screen). For **Media Security**, select **Media Security Never (MSNV)**, for **Restriction Level**, select **Unrestricted (UNR)**. Use default for remaining values. Click on **Return Class of Service** and then click on the **Save** button (not shown).

**AVAYA CS1000 Element Manager** Help

- UCM Network Services
- Home
- Links
  - Virtual Terminals
- System
  - + Alarms
  - Maintenance
  - + Core Equipment
  - Peripheral Equipment
  - + IP Network
  - + Interfaces
  - Engineered Values
  - + Emergency Services
  - + Software
- Customers
- Routes and Trunks
  - [Routes and Trunks](#)
  - D-Channels
  - Digital Trunk Interface
- Dialing and Numbering Plans
  - Electronic Switched Network
  - Flexible Code Restriction
  - Incoming Digit Translation
- Phones
  - Templates
  - Reports
  - Views
  - Lists
  - Properties
  - Migration
- Tools
  - + Backup and Restore
  - Date and Time

- Centrex Switchhook Flash: Centrex Switchhook Flash Denied (HFSD)
 

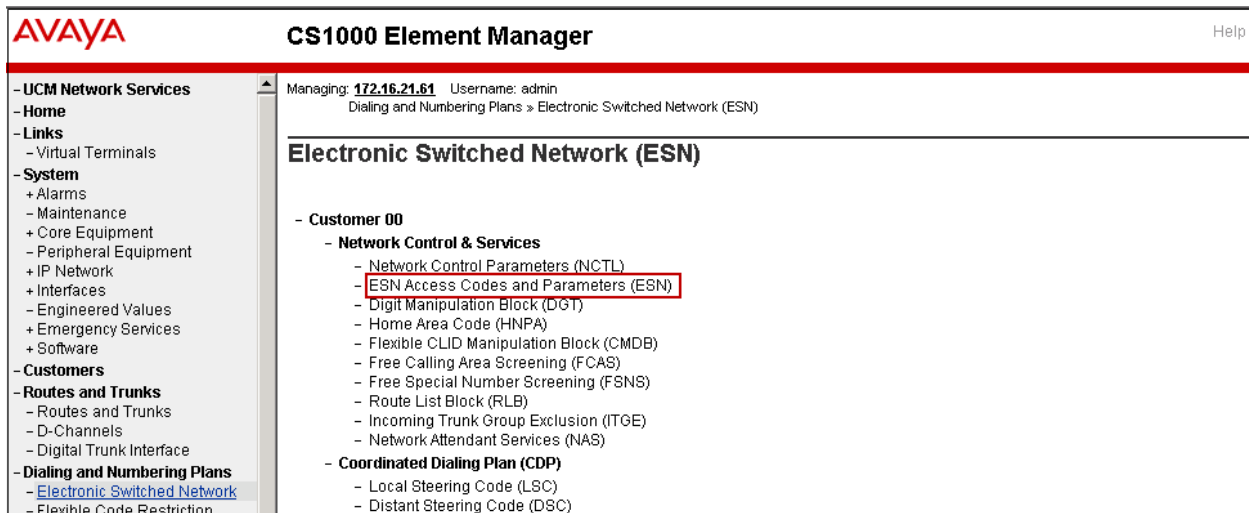
- Dial Pulse: Dial Pulse (DIP)
- DTR PAD value:
- Echo Canceling: Echo Canceling Denied (ECD)
- Hong Kong DTI:
- Loop Break Supervised COT:
- Make-break ratio for dial pulse: 10 pulses per second (P10)
- Manual Incoming: Manual Incoming Denied (MID)
- Media Security: **Media Security Never (MSNV)**
- Network Hook Flash Over M911P:
- Polarity:
- Priority: Low Priority (LPR)
- Restriction level: **Unrestricted (UNR)**
- Reversed Ear Piece: Reversed Ear Piece denied (XREP)
- Short or long line:
- Transmission Class of Service: Non-Transmission Compensated (NTC)
  - Warning Tone: Warning Tone Allowed (WTA)
  - Reversed Ear Piece: Reversed Ear Piece denied (XREP)
  - ARF Supervised COT:

## 5.7. Administer Dialing Plans

This section describes how to administer dialing plans on the CS1000.

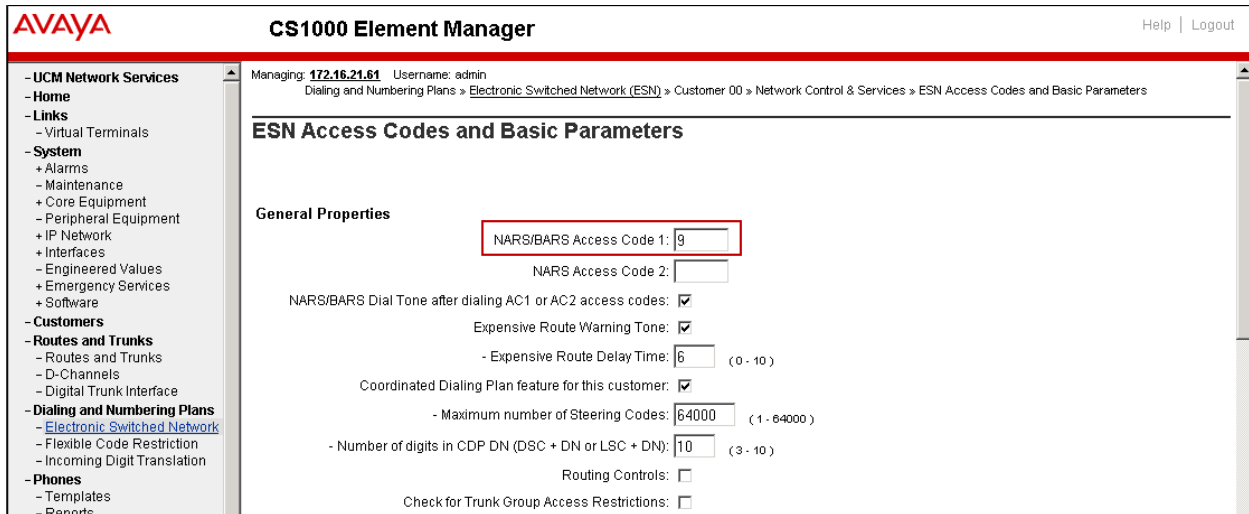
### 5.7.1. Define ESN Access Codes and Parameters (ESN)

Select **Dialing and Numbering Plans** → **Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen. Select **ESN Access Codes and Parameters (ESN)** as shown below.



The screenshot shows the AVAYA CS1000 Element Manager interface. The left navigation pane is expanded to 'Dialing and Numbering Plans' > 'Electronic Switched Network'. The main content area shows a tree view for 'Customer 00' with 'ESN Access Codes and Parameters (ESN)' highlighted in a red box. The breadcrumb trail is: Managing: 172.16.21.61 Username: admin > Dialing and Numbering Plans > Electronic Switched Network (ESN).

In the **ESN Access Codes and Basic Parameters** page, under **NARS/ BARS Access Code 1**, define the one or two digit code that the user will need to enter on outbound PSTN calls prior to the destination number. In the reference configuration, **9** was used. Click **Submit** (not shown).



The screenshot shows the AVAYA CS1000 Element Manager interface. The left navigation pane is expanded to 'Dialing and Numbering Plans' > 'Electronic Switched Network' > 'Flexible Code Restriction'. The main content area shows the 'ESN Access Codes and Basic Parameters' configuration page. The 'NARS/BARS Access Code 1' field is highlighted in a red box and contains the value '9'. Other fields include 'NARS Access Code 2', 'NARS/BARS Dial Tone after dialing AC1 or AC2 access codes' (checked), 'Expensive Route Warning Tone' (checked), 'Expensive Route Delay Time' (6), 'Coordinated Dialing Plan feature for this customer' (checked), 'Maximum number of Steering Codes' (64000), 'Number of digits in CDP DN (DSC + DN or LSC + DN)' (10), 'Routing Controls' (unchecked), and 'Check for Trunk Group Access Restrictions' (unchecked).

## 5.7.2. Digit Manipulation Block Index (DMI)

Select **Dialing and Numbering Plans** → **Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen. Select **Digit Manipulation Block (DGT)** as shown below.

AVAYA CS1000 Element Manager Help

Managing: **172.16.21.61** Username: admin  
Dialing and Numbering Plans » Electronic Switched Network (ESN)

### Electronic Switched Network (ESN)

- Customer 00
  - Network Control & Services
    - Network Control Parameters (NCTL)
    - ESN Access Codes and Parameters (ESN)
    - **Digit Manipulation Block (DGT)**
    - Home Area Code (HNPA)
    - Flexible CLID Manipulation Block (CMDB)
    - Free Calling Area Screening (FCAS)
    - Free Special Number Screening (FSNS)
    - Route List Block (RLB)
    - Incoming Trunk Group Exclusion (ITGE)
    - Network Attendant Services (NAS)

In the **Please choose the Digit Manipulation Block Index** drop-down field, select an available DMI from the list and click **to Add** as shown below.

AVAYA CS1000 Element Manager Help

Managing: **172.16.21.61** Username: admin  
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » Digit Manipulation Block List

### Digit Manipulation Block List

Please choose the

- + Digit Manipulation Block Index -- 1
- + Digit Manipulation Block Index -- 2

The example below shows **Digit manipulation Block Index number 1**, previously added.

Enter **0** for the **Number of leading digits to be deleted** field and select **NPA (NPA)** for the **Call Type to be used by the manipulated digits** as shown below. Click **Submit**

AVAYA CS1000 Element Manager Help | Logout

Managing: 172.16.21.61 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: [text box]

IP Special Number:

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

Submit Refresh Delete Cancel

### 5.7.3. Route List Block (RLB)

This section shows how to add a Route List Block (RLB) associated with the DMI created in **Section 5.7.2**. Select **Dialing and Numbering Plans** → **Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen. Select **Route List Block (RLB)** as shown below.

AVAYA CS1000 Element Manager

Managing: 172.16.21.61 Username: admin  
Dialing and Numbering Plans > Electronic Switched Network (ESN)

### Electronic Switched Network (ESN)

- Customer 00

- Network Control & Services
  - Network Control Parameters (NCTL)
  - ESN Access Codes and Parameters (ESN)
  - Digit Manipulation Block (DGT)
  - Home Area Code (HNPA)
  - Flexible CLID Manipulation Block (CMDB)
  - Free Calling Area Screening (FCAS)
  - Free Special Number Screening (FSNS)
  - Route List Block (RLB)
  - Incoming Trunk Group Exclusion (ITGE)
  - Network Attendant Services (NAS)

Enter an available value in the **Please enter a route list index** box and click the **to Add** button as shown below.

AVAYA CS1000 Element Manager

Managing: 172.16.21.61 Username: admin  
Dialing and Numbering Plans > Electronic Switched Network (ESN) > Customer 00 > Network Control & Services > Route List Blocks

**Route List Blocks**

Please enter a route list index:  (0 - 1999)

+ Route List Block Index -- 1 Edit

+ Route List Block Index -- 2 Edit

The example below shows **Route List Block Index 1**, previously added.

Enter the following values for the specified fields, and retain the default values for the remaining fields as shown below.

- **Digit Manipulation Index (DMI): 1** (created in Section 5.7.2)
- **Route number (ROUT): 0** (created in Section 5.6.2)

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

AVAYA CS1000 Element Manager Help | Logout

Managing: 172.16.21.61 Username: admin  
Dialing and Numbering Plans > Electronic Switched Network (ESN) > Customer 00 > Network Control & Services > Route List Blocks > Route List Block Index 1

**Route List Block Index 1**

**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 - 255)

**Options**

Local Termination entry:

Route Number: 0

Skip Conventional Signaling:

Display Originator's Information:

Use Tone Detector:

Conversion to LDN:

Expensive Route:

Strategy on Congestion: No Reroute (NRR)

QSIG Alternate Routing Causes: QSIG Alternate Routing Cause 1



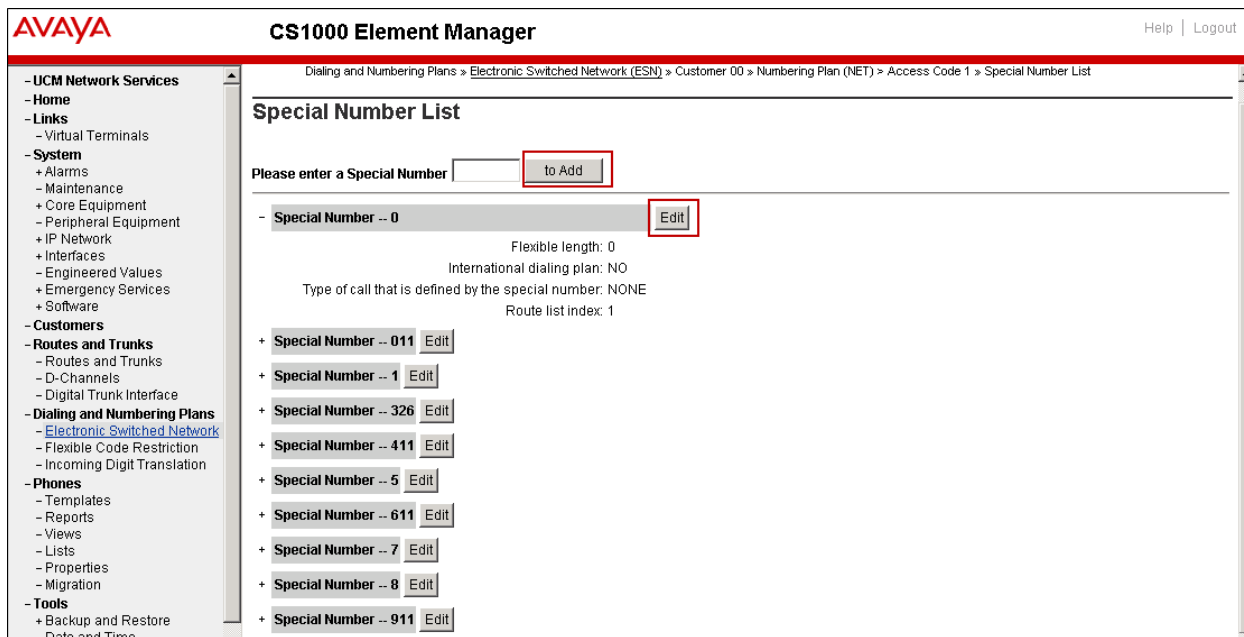
#### 5.7.4. Outbound Call - Special Number Configuration.

There are special numbers which were configured to be used for the compliance testing, such as **0** to reach Service Provider operator, **0+10** digits to reach Service Provider operator assistant, **011** prefix for international calls, **1** for national long distance calls, **411**, **911** and so on. Calls to special numbers shown here are for reference only and may not have been tested for various reasons. Refer to section **Items not supported or not tested in Section 2.1**.

Select **Dialing and Numbering Plans** → **Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen. Select **Special Number (SPN)** as shown below.

The screenshot shows the Avaya CS1000 Element Manager interface. The top header includes the Avaya logo, the title 'CS1000 Element Manager', and 'Help | Logout'. Below the header, the main content area is titled 'Electronic Switched Network (ESN)'. The left sidebar contains a navigation menu with categories like 'UCM Network Services', 'Home', 'Links', 'System', 'Customers', 'Routes and Trunks', 'Dialing and Numbering Plans', 'Phones', 'Tools', and 'Security'. The 'Dialing and Numbering Plans' category is expanded, showing 'Electronic Switched Network' as the selected option. The main content area displays the configuration for 'Customer 00', with a tree view of options including 'Network Control & Services', 'Coordinated Dialing Plan (CDP)', and 'Numbering Plan (NET)'. Under 'Numbering Plan (NET)', there are sub-sections for 'Access Code 1' and 'Access Code 2'. The 'Special Number (SPN)' option is highlighted with a red box.

Add a new number by entering it in the **Please enter a Special Number** box and click to **Add** or click **Edit** to view or change a special number that has been previously configured. The screen below shows the various dial strings already configured.



For **Special Number 0** enter the following values:

- **Flexible length: 0**
- **CallType: NONE**
- **Route list index: 1**, created in **Section 5.7.3**

The values for other special numbers used during the tests were as follows (not shown):

#### Special Number: 011

- **Flexible length: 15**
- **CallType: NONE**
- **Route list index: 1**

#### Special Number: 1

- **Flexible length: 11**
- **CallType: NATL**
- **Route list index: 1**

#### Special Number: 411

- **Flexible length: 3**
- **CallType: NONE**
- **Route list index: 1**

### Special Number: 5

- Flexible length: 10
- CallType: LOCL
- Route list index: 1

### Special Number: 911

- Flexible length: 3
- CallType: NONE
- Route list index: 1

## 5.7.5. Outbound Call - Numbering Plan Area Code (NPA)

The **Numbering Plan Area Code (NPA)** was not used for Outbound Calls. The Special Numbers defined above in **Section 5.7.4** allowed the user to dial any Numbering Plan Area Code (NPA) when dialing **9+1** for long distance calls, **9+5** for local calls, etc.

## 5.7.6. Administer Calling Line Identification Entries

Select **Customers** → **00** → **ISDN and ESN Networking** (not shown). Click on **Calling Line Identification Entries** as shown below.

The screenshot displays the AVAYA CS1000 Element Manager interface. The top navigation bar includes the AVAYA logo, the title 'CS1000 Element Manager', and 'Help | Logout'. A left sidebar contains a tree view with categories: '- UCM Network Services', '- Home', '- Links', '- Virtual Terminals', '+ System', '- Customers', '+ Routes and Trunks', '+ Dialing and Numbering Plans', '+ Phones', '+ Tools', and '+ Security'. The main content area is titled 'Options' and contains several checked options: 'Transfer on ringing of supervised external trunks', 'Connection of supervised external trunks', 'Coordinated dialing plan routing', and 'Integrated services digital network'. Below these are settings for 'Microsoft converged office dialing plan' (set to 'Private dialing plan') and 'Private dialing plan for non-DID users' (with radio buttons for 'Coordinated dialing plan' and 'Uniform dialing plan'). There are also checkboxes for 'Extended Local Calls' and 'Extended Local Calls for IMS Line user', and a text field for 'Extended Local Calls Route list index'. The 'Calling Line Identification' section includes a dropdown for 'Information for incoming/outgoing calls' (set to 'No manipulation is done'), a 'Size' field (set to 256), and a 'Country code' field. A red box highlights the 'Calling Line Identification Entries' link at the bottom of this section. At the bottom right of the main content area are 'Save' and 'Cancel' buttons.

Click **Add** on the **Calling Line Identification Entries** screen.

The screenshot shows the AVAYA CS1000 Element Manager interface. The top navigation bar includes the AVAYA logo, the title 'CS1000 Element Manager', and 'Help | Logout'. The left sidebar contains a menu with options like '- UCM Network Services', '- Home', '- Links', '+ System', '- Customers', '+ Routes and Trunks', '+ Dialing and Numbering Plans', '+ Phones', '+ Tools', and '+ Security'. The main content area is titled 'Calling Line Identification Entries' and includes a search section with 'Start range' and 'End range' input fields, a 'Search' button, and a note: ''End range' should not exceed the CLID size specified'. Below the search section, there is a section for 'Calling Line Identification Entries' with an 'Add...' button highlighted by a red box, a 'Delete' button, and a 'Refresh' button.

Add **Entry Id 0** as shown below:

- **National Code:** Enter the three digit area code prefix of the DID number assigned by the service provider, **585** in this example.
- **Local Code:** Enter the seven digit number of the DID assigned by Service Provider, **3211234** in this example.
- **Use DN as DID:** Set to **NO**. The local extension number will not be used as the calling number.

Repeat for each of the DID numbers to be assigned to extensions in the CS1000.

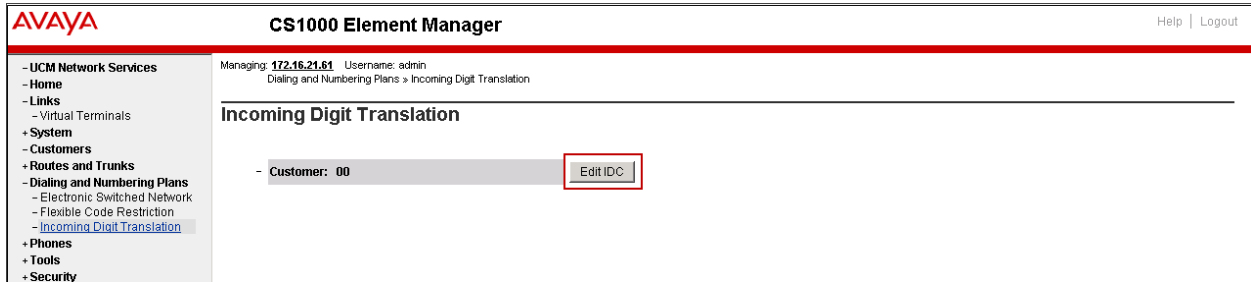
The screenshot shows the AVAYA CS1000 Element Manager interface for the 'New Calling Line Identification' form. The left sidebar is the same as in the previous screenshot. The main content area is titled 'New Calling Line Identification' and contains the following fields and options:

- General Properties:**
  - Entry Id: 0 (0 - 255)
  - National Code: 585 (0 - 999999) Code for national home number
  - Local Code: 3211234 (1-12 digits) Code for home local number or listed DN
  - Local Steering Code: (1-7 digits)
  - Use DN as DID: NO
- 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

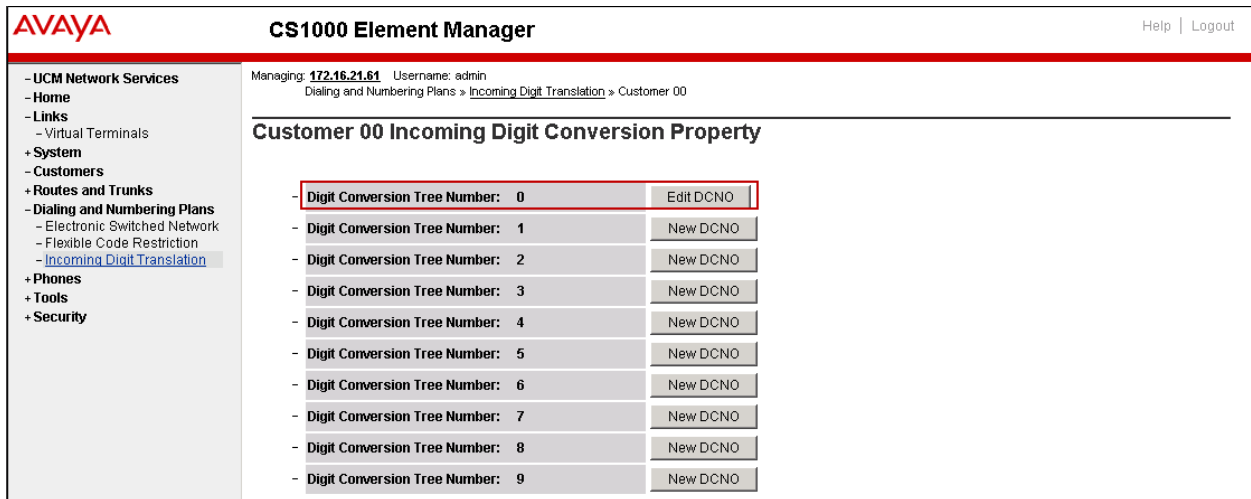
### 5.7.7. Inbound Call Digit Translation

Incoming calls from Frontier to the DID numbers assigned to the enterprise are mapped to extensions in the CS1000 by using the **Incoming Digit Translation** tables.

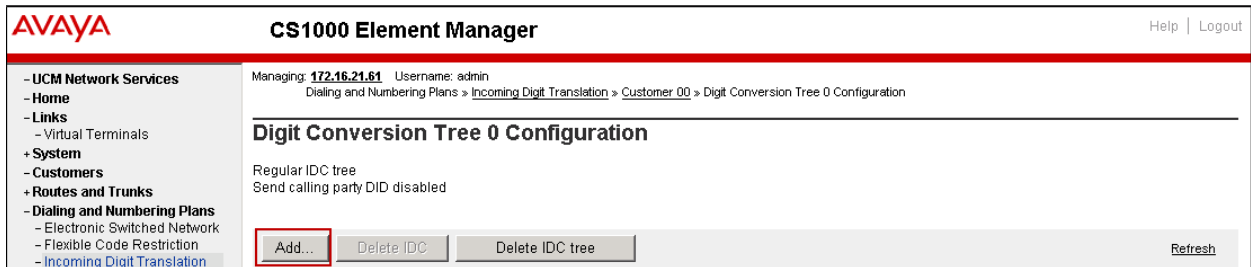
Select **Dialing and Numbering Plans** → **Incoming Digit Translation** from the left pane. Click on **Edit IDC** button under **Customer: 00** as shown below.



Click on **New DCNO** to create a new digit translation mechanism or **Edit DCNO** to modify an existing one. In the reference configuration, **Digit Conversion Tree Number 0** was created as shown below. Note that Digit Conversion Tree number 0 was assigned to Route 0, as shown previously on **Section 5.6.2**.



The **Digit Conversion Tree 0 Configuration** screen will open. Click on the **Add** button.



On the **Incoming Digits** field, enter the Frontier DID number. On the **Converted Digits** field enter the associated CS1000 extension number. Click **Save**. Repeat as necessary for all the Frontier DID numbers to be mapped to CS1000 extensions.

**AVAYA CS1000 Element Manager** Help | Logout

Dialing and Numbering Plans > Incoming Digit Translation > Customer 00 > Digit Conversion Tree 0 Configuration > Add Incoming Digits

### Add Incoming Digits

Incoming Digits:  \*

Converted digits:  \* (0-99999999)

Force storage or removal of data:

In case of conflict between the new and existing Incoming Digits, force storage or removal may result in loss of portions of the tree.

CPND language:  Roman characters

CPND Name:

first name, last name

Expected length:

Display format:

## 5.8. Enable Plug-In for Blind Call Transfer

Plug-in 501 should be enabled in the CS1000 to allow the completion of blind call transfers in scenarios where SIP UPDATES are not supported by the service provider. Note that enabling this plug-in will allow the CS1000 user to complete the transfer operation, but the PSTN user in the first leg of the call will not hear ring back once the call is transferred and while the second PSTN user's phone is ringing. Once the call is answered the talk path between the two PSTN users is established normally.

Go to **System** → **Software** → **Plug-ins**, select **plug-in 501** and click the **Enable** button. The status will change to **Enabled**.

**AVAYA CS1000 Element Manager** Help | Logout

Managing: Username: System > Software > Plug-ins

### Plug-ins

Number	Description	MPLR Number	Status
96	Allow single key sets to dial FFC code for MSB	MPLR31293	Disabled
97	Restrict Hands-free functionality for all IP set types.	MPLR29100	Disabled
98	DTMF for ADL	MPLR25106	Disabled
99	External caller's name gets dropped when goes thru IDC table	MPLR31280	Disabled
100	NO DESCRIPTION	MPLR21979	Disabled
<input checked="" type="checkbox"/> 101	Enables blind transfer to a SIP endpoint even if SIP UPDATE is not supported by the far end	MPLR30070	Enabled
102	CLIR display changed. Disable spaces between character OUT OF AREA. To turn off quotes in words ANONYMOUS and OUT OF AREA enable plug-in 509	MPLR31148	Disabled
103	PRI232 BUG253 from PI 10 Delay in Response at Called IFC	MPLR24744	Disabled
104	UM2K integration problem with S100 Interface	MPLR30004	Disabled
105	PI: MobileX CLID update on mobile after handoff	MPLR30609	Disabled
106	Mobile X Timer MBXT has no effect because no ALERT received	MPLR30310	Disabled
107	ALLOW INTERCEPT TREATMENT CHOICE FOR DNIS CALLS	MPLR15939	Disabled
108	CLIR display changed	MPLR21444	Disabled
109	If C.O. is requesting CNI, CNDN and other digits are sent	MPLR30350	Disabled

## 5.9. CS1000 Telephones and Features Settings

This section illustrates a sampling of the CS1000 telephone types and some of the settings used in the reference configuration, for the verification of the functionality and features described in **Section 2.1**.

### 5.9.1. Example IP Phones with Privacy and Call Forward

Select **Phones** from the left pane. On the **Search For Phones** screen (not shown) the user configuration screen can be retrieved using different search criteria, such as Prime DN, Phone Type, etc. The **Phone Details** screens below shows a UniStim IP phone (extension 8000) and a SIP phone (extension 8021) used in the reference configuration. Note that the phones use Bandwith Zone 5, defined earlier in **Section 5.5.2**.

The screenshot displays the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation menu with categories like UCM Network Services, System, Customers, Routes and Trunks, Dialing and Numbering Plans, Phones, Tools, and Security. The main content area is titled "Phone Details" and shows a UniStim IP phone icon. The system information includes "System: EM on cs1k", "Phone Type: 1165", and "Sync Status: TRN". Below this, the "General Properties" section is visible, showing fields for "Customer Number" (0), "Terminal Number" (008 0 00 00), "Designation" (8000), and "Zone" (5). The "Designation" field has a note "(1-6 characters)".

The screenshot displays the AVAYA CS1000 Element Manager interface for a SIP phone. The left sidebar is identical to the previous screenshot. The main content area is titled "Phone Details" and shows a SIP phone icon. The system information includes "System: EM on cs1k", "Phone Type: UEXT-SIPL", and "Sync Status: TRN". Below this, the "General Properties" section is visible, showing fields for "Customer Number" (0), "Terminal Number" (008 0 00 07), "Designation" (SIPD), "Zone" (5), "SIP User Name" (8021), and "Node Id" (1006). The "Designation" field has a note "(1-6 characters)" and the "SIP User Name" field has a note "(1-16 characters)".

On the **Phone Details** screen, scroll down to the **Features** section to verify/assign the features on the phone.

### 5.9.1.1 Privacy

Outbound Calling Party Privacy was tested on CS1000E stations by setting **CLBA Calling Party Privacy** to *Allowed* in the Features section as shown below. By doing this, the outbound SIP INVITE will contain a “Privacy: id” header, while the From header will be set to “anonymous”



The screenshot shows a table titled "Features" with columns for Feature, Description, and Value. The CLBA feature is highlighted with a red border and set to "Allowed".

Feature	Description	Value
CFXA	Call Forward External	Allowed
CLBA	Calling Party Privacy	Allowed
CLRO	Calling Number Restriction Override	Denied
CLS	Trunk/Call Type Access Restriction	Unrestricted

### 5.9.1.2 Call Forward no Answer

Inbound unanswered PSTN calls were redirected to voicemail (Call Pilot) or to other endpoints by setting the following parameters in the Features section (not shown):

- **CFTA (Call Forward by Call Type):** Set to *Allowed*.
- **EFD (CFNA DN for External Calls with CFTA):** Set to the Call Pilot access number (8056 in the reference configuration) or the desired endpoint.

### 5.9.1.3 Call Forward Busy

Inbound PSTN calls to busy CS1000E extensions were redirected to voicemail (Call Pilot) or to other endpoints by setting the following parameters in the Features section (not shown):

- **CFTA (Call Forward by Call Type):** Set to *Allowed*.
- **EHT (Hunt DN for External Calls with CFTA):** Set to the Call Pilot access number (8056 in the reference configuration) or the desired endpoint.
- **HTA (Hunting):** Set to *Allowed*.
- **HUNT (Hunt DN – All Calls or Internal Calls for CFTA):** Set to the Call Pilot access number (8056 in the reference configuration) or desired endpoint.



### 5.9.1.4 Call Forward All Calls

Scroll down to the **Keys** section of the **Phone Details** screen. Define a key for **CFW- Forward All Calls** and enter the **Redirection DN Length** and **Redirection DN** values. The feature is activated by pressing the corresponding softkey on the telephone pad.

Key No.	Key Type	Key Value
16	NUL - Unassigned	
17	TRN - Call Transfer	
18	A06 - 6-Party Conference	
19	CFW - Forward All Calls	Redirection DN Length: 12 Redirection DN: 915853211235
20	RGA - Ring Again	

### 5.9.2. Example Digital Phone with Call Waiting

The screen below shows the Phone Details screen for a M3904 digital station.

The screenshot shows the AVAYA CS1000 Element Manager interface. The main content area is titled "Phone Details" and shows a phone icon and the following information: System: EM on cs1k, Phone Type: M3904, and Sync Status: TRN. Below this, there are tabs for "General Properties", "Features", "Keys", and "User Fields". The "General Properties" tab is active, showing fields for Customer Number (0), Terminal Number (004 0 04 00), Designation (M3904), KBA (0), and DBA (0). A left-hand navigation menu includes sections like UCM Network Services, Home, Links, System, Customers, Routes and Trunks, Dialing and Numbering Plans, Phones, Tools, and Security.

### 5.9.2.1 Call Waiting

To enable Call Waiting with tone on the phone, scroll down to the **Features** section and set **WTA Warning Tone** to *Allowed* (not shown). Scroll down further to the **Keys** section and define a key for **CWT - Call Waiting** as shown on the screen below.

Key No.	Key Type	Key Value
0	SCR - Single Call Ringing	
1	CWT - Call Waiting	
2	NUL - Unassigned	

Directory Number: 8011

Multiple Appearance Redirection Prime(MARP)

CPND Name: Avaya | Display Format: First, Last | Language: Roman

CLID Entry (Numeric or D): 4

ANIE Entry:

### 5.9.3. Analog Fax Line

The screen below shows the **Phone Details** screen for an analog station used during testing for a Ventafax fax machine emulator.

System: EM on cs1k

Phone Type: 500

Sync Status: TRN

General Properties | Features | Single Line Features | User Fields

Custom View: All

General Properties

Customer Number: 0 \*

Terminal Number: 004 0 03 01

Designation: 500 \* (1-6 characters)

Directory Number: 8017

CLID entry: 3

On the **Features** section of the analog station, **FAXA Fax Class of Service** was set to *Allowed*, and **MPT Modem Pass Through** was set to *MPTD* (not shown), to enable the use of Fax T.38 upon detection of fax V.21 preamble.

## 6. Configure Avaya Aura® Session Manager

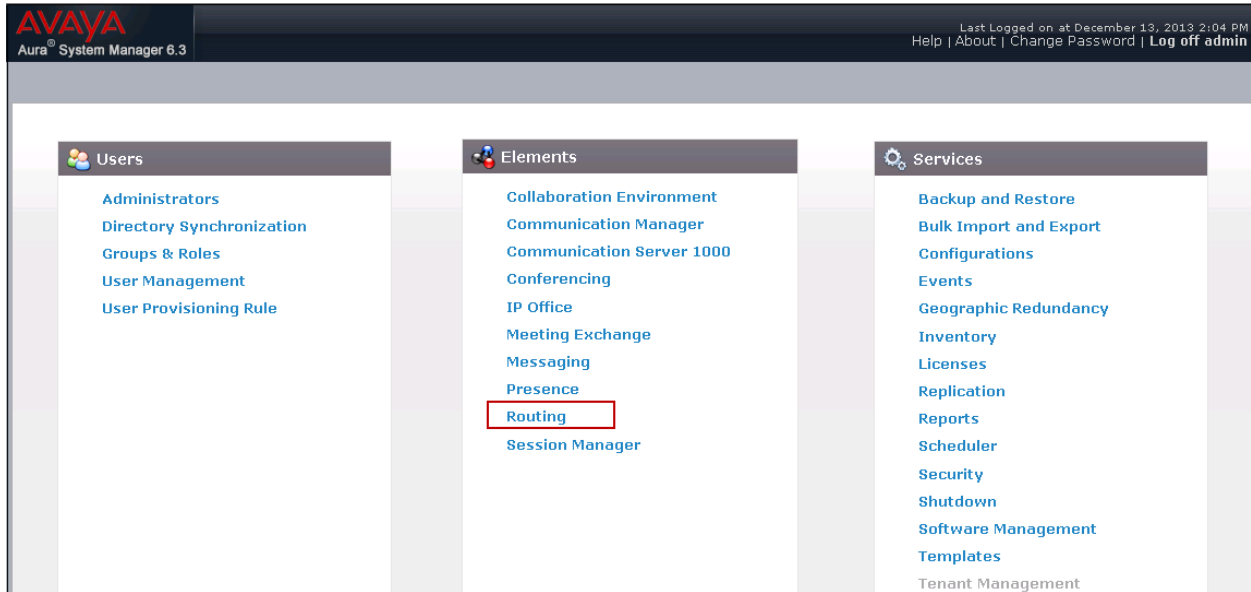
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain.
- Logical/physical locations that can be occupied by SIP Entities.
- Adaptation modules
- 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.

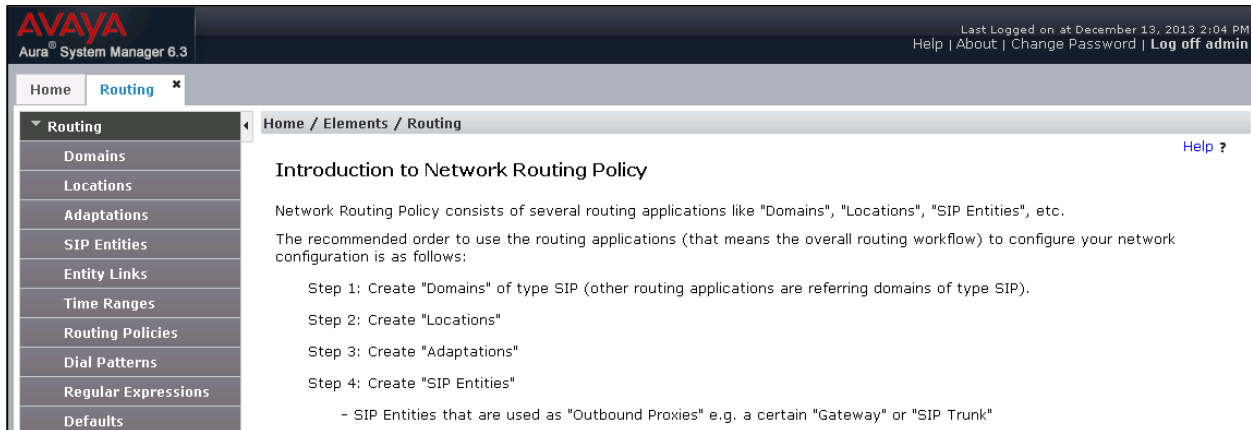
The following sections assume that network connectivity exists between System Manager and Session Manager, and that the initial configuration of Session Manager and System Manager has already been completed.

## 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. Log in with the appropriate credentials and click on **Log On** (not shown). The screen shown below is then displayed; click on **Routing**.



The navigation tree displayed in the left pane below will be referenced in subsequent sections to navigate to items requiring configuration. Most items discussed in this section will be located under the **Routing** link shown below.



## 6.2. SIP Domain

Create a SIP domain for each domain for which Session Manager will need to be aware in order to route calls. For the compliance test, this will be the enterprise lab domain, *avaya.lab.com*. Navigate to **Routing → Domains** in the left-hand navigation pane (**Section 6.1**) and click the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Name:** Enter the domain name.
- **Type:** Select **sip** from the drop-down menu.
- **Notes:** Add a brief description (optional).

Click **Commit**. The screen below shows the entry for the enterprise domain

The screenshot shows the Avaya Session Manager interface. The left navigation pane is expanded to 'Routing' and 'Domains'. The main area shows the 'Domain Management' screen. The breadcrumb is 'Home / Elements / Routing / Domains'. There are 'Commit' and 'Cancel' buttons at the top right. Below the breadcrumb is a table with one item:

Name	Type	Notes
*avaya.lab.com	sip	Lab Domain

There are 'Commit' and 'Cancel' buttons at the bottom right.

## 6.3. Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management, call admission control and location-based routing. 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).

Defaults can be used for all other parameters.

The following screen shows the location details for the location named “MA Session Manager”. Later, this location will be assigned to the SIP Entity corresponding to Session Manager.

Home / Elements / Routing / Locations Help ?

Location Details Commit Cancel

**General**

\* Name:   
 Notes:

**Dial Plan Transparency in Survivable Mode**

Enabled:

Listed Directory Number:

Associated CM SIP Entity:

**Overall Managed Bandwidth**

Managed Bandwidth Units:

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth:

**Per-Call Bandwidth Parameters**

Maximum Multimedia Bandwidth (Intra-Location):  Kbit/Sec  
 Maximum Multimedia Bandwidth (Inter-Location):  Kbit/Sec  
 \* Minimum Multimedia Bandwidth:  Kbit/Sec  
 \* Default Audio Bandwidth:

**Alarm Threshold**

Overall Alarm Threshold:  %  
 Multimedia Alarm Threshold:  %  
 \* Latency before Overall Alarm Trigger:  Minutes  
 \* Latency before Multimedia Alarm Trigger:  Minutes

**Location Pattern**

0 Items Refresh Filter: Enable

IP Address Pattern	Notes

Commit Cancel

The following screen shows the location details for the location named “**CS1K Node**”. Later, this location will be assigned to the SIP Entity corresponding to the CS1000. Other location parameters (not shown) retained the default values.

The screenshot shows a web interface with a breadcrumb trail 'Home / Elements / Routing / Locations' at the top. Below this, the title 'Location Details' is displayed on the left, and 'Commit' and 'Cancel' buttons are on the right. Under the 'General' section, there are two input fields: '\* Name:' with the value 'CS1k Node' and 'Notes:' with the value 'CS1K7.6'.

The following screen shows the location details for the location named “**MA SBCE**”. Later, this location will be assigned to the SIP Entity corresponding to the Avaya SBCE. Other location parameters (not shown) retained the default values.

The screenshot shows a web interface with a breadcrumb trail 'Home / Elements / Routing / Locations' at the top. Below this, the title 'Location Details' is displayed on the left, and 'Commit' and 'Cancel' buttons are on the right. Under the 'General' section, there are two input fields: '\* Name:' with the value 'MA SBCE' and 'Notes:' with the value 'Avaya SBCE 6.2'.

## 6.4. Adaptations

Session Manager can be configured with adaptation modules to modify SIP messages before or after routing decisions have been made. A generic adaptation module **DigitConversionAdapter** supports digit conversion of telephone numbers in specific headers of SIP messages. Other adaptation modules are built on this generic module, and can modify other headers to permit interoperability with third party SIP products.

To view or change adaptations, select **Routing → Adaptations**. Click on the checkbox corresponding to the name of an adaptation and **Edit** to edit an existing adaptation, or the **New** button to add an adaptation. Click the **Commit** button after changes are completed.

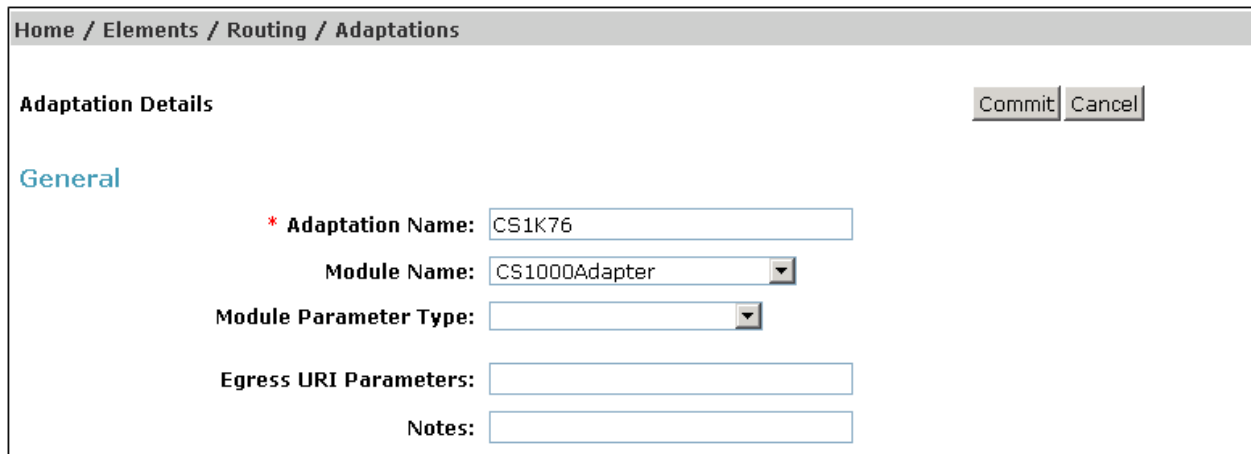
Two adaptations, named *CS1K76* and *History-Diversion*, were created and used during the compliance test.

The adaptation named *CS1K76* is shown on the screen below. It will later be assigned to the SIP Entity corresponding to the CS1000.

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

- **Adaptation Name:** Enter a descriptive name for the adaptation.
- **Module Name:** Select the *CS1000Adapter* from drop-down menu.

Click **Commit** to save.



The screenshot shows a web interface for configuring an adaptation. At the top, there is a breadcrumb trail: Home / Elements / Routing / Adaptations. Below this, the page is titled "Adaptation Details" and includes "Commit" and "Cancel" buttons. The "General" section contains the following fields:

- \* Adaptation Name:** Text input field containing "CS1K76".
- Module Name:** Drop-down menu with "CS1000Adapter" selected.
- Module Parameter Type:** Drop-down menu.
- Egress URI Parameters:** Text input field.
- Notes:** Text input field.



The adaptation named **History-Diversion** is shown on the screen below. This adaptation will later be assigned to the SIP Entity corresponding to the Avaya SBCE.

- **Adaptation Name:** Enter a descriptive name for the adaptation.
- **Module Name:** Enter **DiversionTypeAdapter**. The adapter is used to convert the History-Info headers coming from the CS1000 to Diversion headers supported by Frontier
- **Module Parameter Type:** Select **Name-Value Parameter** from the drop-down menu. Click the **Add** button and set the parameter **Name** to **MIME** and **Value** to **no**. This parameter will remove MIME types inserted by the CS1000 which are not used for call processing that should not be sent to the service provider.

Click **Commit** to save.

Home / Elements / Routing / Adaptations

**Adaptation Details** Commit Cancel

**General**

\* **Adaptation Name:**

**Module Name:**

**Module Parameter Type:**

<input type="checkbox"/>	Name	Value
<input type="checkbox"/>	MIME	no

Select : All, None

**Egress URI Parameters:**

**Notes:**

## 6.5. 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 the **New** button in the right pane (not shown). In the **General** section, enter the following values. Use default values for all remaining fields:

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Select *Session Manager* for Session Manager, *Other* for the CS1000 and *SIP Trunk* for the Avaya SBCE
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If applicable, select the **Adaptation Name** defined in **Section 6.4**
- **Location:** Select the location that applies to the SIP Entity being created, defined in **Section 6.3**.
- **Time Zone:** Select the time zone for the location above.

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

The screenshot shows a web interface for configuring SIP Entities. The breadcrumb path is "Home / Elements / Routing / SIP Entities". The page title is "SIP Entity Details" with "Commit" and "Cancel" buttons. The "General" section is active and contains the following fields:

- Name:** MA\_Session Manager
- FQDN or IP Address:** 192.168.10.32
- Type:** Session Manager (dropdown)
- Notes:** Security Module
- Location:** MA Session Manager (dropdown)
- Outbound Proxy:** (empty dropdown)
- Time Zone:** America/New\_York (dropdown)
- Credential name:** (empty text field)


The "SIP Link Monitoring" section is also visible, with the field "SIP Link Monitoring" set to "Use Session Manager Configuration" (dropdown).

To define the ports that Session Manager will use to listen for SIP requests, scroll down to the **Port** section of the **SIP Entity Details** screen. This section is only present for **Session Manager** SIP entities. The screen below shows the ports used by Session Manager in the shared lab environment. Only TCP port 5060 for the connection to the Avaya SBCE and UDP port 5087 for the CS1000 are directly relevant to these Application Notes.

**Port**

TCP Failover port:

TLS Failover port:

8 Items  Filter: Enable

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	<input type="text" value="5060"/>	TCP	avaya.lab.com	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5060"/>	UDP	avaya.lab.com	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5061"/>	TLS	avaya.lab.com	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5087"/>	UDP	avaya.lab.com	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5070"/>	TCP	avaya.lab.com	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5075"/>	TCP	avaya.lab.com	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="5080"/>	TCP	avaya.lab.com	<input type="text"/>
<input type="checkbox"/>	<input type="text" value="6060"/>	TCP	avaya.lab.com	<input type="text"/>

Select : All, None

The following screen shows the addition of this SIP Entity for the CS1000. The **FQDN or IP Address** field is set to the TLAN IP address of the CS1000 Signaling Gateway (Node IP address, **Section 5.2.1**). The **Adaptation** selected is *CS1K76*, defined in **Section 6.4**. The **Location** is set to *CS1K Node*, defined in **Section 6.3**.

Home / Elements / Routing / SIP Entities

**SIP Entity Details** Commit Cancel

**General**

\* **Name:** CS1K7.6

\* **FQDN or IP Address:** 172.16.20.60

**Type:** Other

**Notes:** CS1000 Rel. 7.6

**Adaptation:** CS1K76

**Location:** CS1k Node

**Time Zone:** America/New\_York

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

**Credential name:**

**Call Detail Recording:** none

**CommProfile Type Preference:**

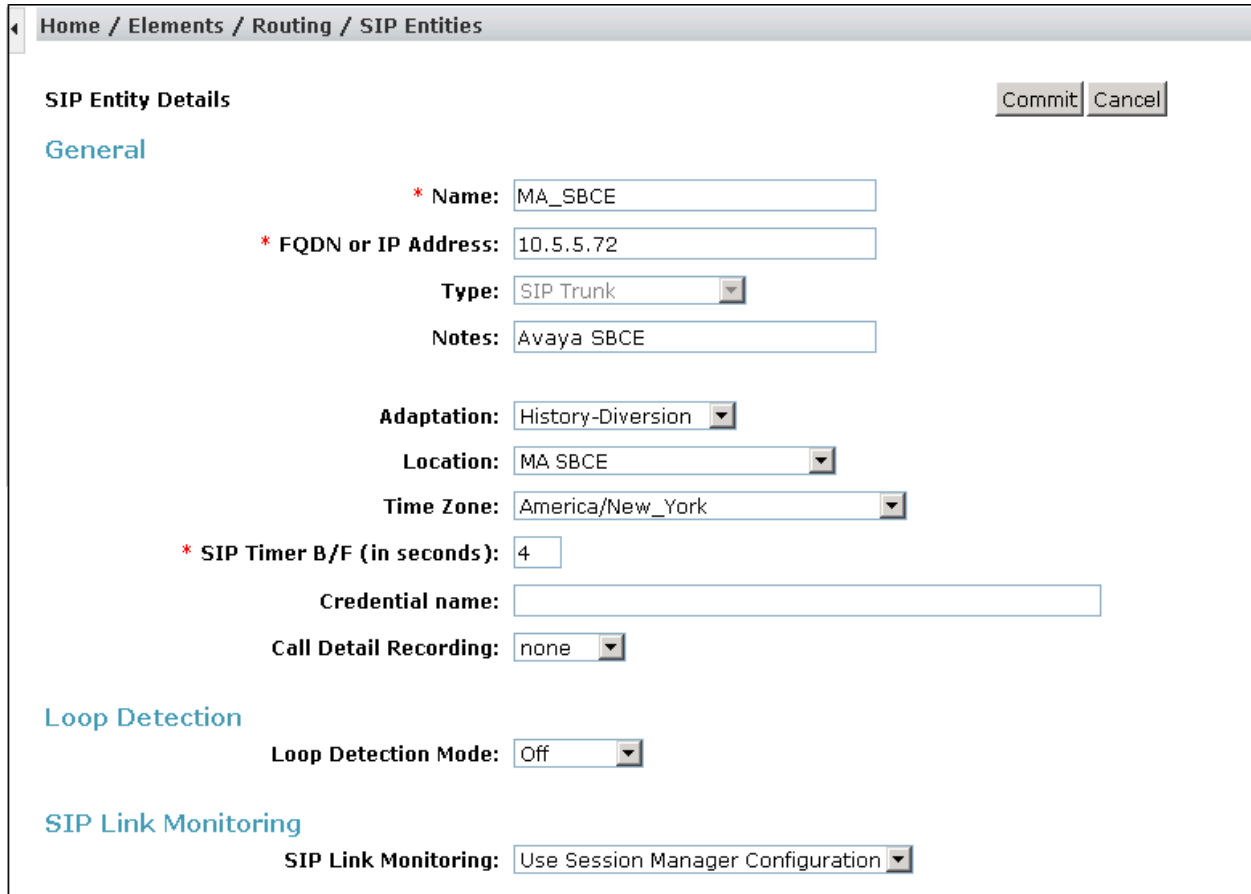
**Loop Detection**

**Loop Detection Mode:** Off

**SIP Link Monitoring**

**SIP Link Monitoring:** Use Session Manager Configuration

The following screen shows the addition of the Avaya SBCE Entity. The **FQDN or IP Address** field is set to the IP address of the SBC private network interface (see **Figure 1**). The **Adaptation** selected is *History-Diversion*, defined in **Section 6.4**, and the **Location** is set to *MA SBCE*, defined in **Section 6.3**.



Home / Elements / Routing / SIP Entities

SIP Entity Details Commit Cancel

General

\* Name: MA\_SBCE

\* FQDN or IP Address: 10.5.5.72

Type: SIP Trunk

Notes: Avaya SBCE

Adaptation: History-Diversion

Location: MA SBCE

Time Zone: America/New\_York

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

Credential name:

Call Detail Recording: none

Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

## 6.6. Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created; one to the CS1000 and the other to the Avaya SBCE. To add an Entity Link, navigate to **Routing** → **Entity Links** in the left-hand 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 from the drop-down menu.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end.
- **SIP Entity 2:** Select the name of the other system from the drop-down menu.
- **Port:** Port number on which the other system receives SIP requests from Session Manager.
- **Connection Policy:** Select *trusted* to allow calls from the associated SIP Entity.

Click **Commit** to save.

The screen below illustrates the Entity Link to the CS1000. Note that the protocol used is **UDP**, and the local and remote SIP listening ports are set to **5087**.

The screenshot shows the 'Entity Links' configuration page. The breadcrumb is 'Home / Elements / Routing / Entity Links'. There are 'Commit' and 'Cancel' buttons. A table lists one item with the following details:

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy
* MA-SM to CSIK7.6	* MA_Session Manager	UDP	* 5087	* CS1K7.6	<input type="checkbox"/>	* 5087	trusted

The following screen illustrates the Entity Link to the Avaya SBCE. Note that the protocol used is **TCP**, and the local and remote SIP listening ports are set to **5060**.

The screenshot shows the 'Entity Links' configuration page. The breadcrumb is 'Home / Elements / Routing / Entity Links'. There are 'Commit' and 'Cancel' buttons. A table lists one item with the following details:

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy
* MA_SM to ASBCE	* MA_Session Manager	TCP	* 5060	* MA_SBCE	<input type="checkbox"/>	* 5060	trusted

## 6.7. Routing Policies

Routing policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.4**.

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. In the **General** section, enter a descriptive **Name** and add a brief description under **Notes** (optional).

In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). Choose 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 to the CS1000 and the Avaya SBCE

Home / Elements / Routing / Routing Policies Help ?

Routing Policy Details Commit Cancel

**General**

\* Name:

Disabled:

\* Retries:

Notes:

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type	Notes
CS1K7.6	172.16.20.60	Other	CS1000 Rel. 7.6

Home / Elements / Routing / Routing Policies Help ?

Routing Policy Details Commit Cancel

**General**

\* Name:

Disabled:

\* Retries:

Notes:

**SIP Entity as Destination**

Select

Name	FQDN or IP Address	Type	Notes
MA_SBCE	10.5.5.72	SIP Trunk	Avaya SBCE

## 6.8. Dial Patterns

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

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, or select “**ALL**” to route incoming calls to all SIP domains.
- **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.



The example below shows dial pattern **1**, for outbound calls using the North American Numbering Plan area prefix. The SIP Domain is set to **ALL**, the Originating Location is the **CS1k Node (Section 6.3)**, and the Routing Policy is **Outbound to MA SBCE (Section 6.7)**.

Home / Elements / Routing / Dial Patterns Help ?

**Dial Pattern Details** Commit Cancel

**General**

\* Pattern:

\* Min:

\* Max:

Emergency Call:

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

**Originating Locations and Routing Policies**

Add Remove

6 Items Filter: Enable

<input type="checkbox"/>	Originating Location Name ▲	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	CS1k Node	CS1K7.6	Outbound to MA SBCE	0	<input type="checkbox"/>	MA_SBCE	Outbound to MA_SBCE

Repeat this procedure as needed, to define additional dial patterns for PSTN numbers to be routed to the Frontier network via the Avaya SBCE.

The following screen illustrates an example dial pattern used to verify inbound PSTN calls to the enterprise. In the example, calls to 10 digit numbers starting with **585321** which are on the DID range assigned by Frontier to the SIP trunk, arriving from location **MA SBCE** (under **Originating Location Name**), will use route policy **To CS1K76** to the CS1000.

Home / Elements / Routing / Dial Patterns Help ?

Dial Pattern Details Commit Cancel

**General**

\* Pattern:

\* Min:

\* Max:

Emergency Call:

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

**Originating Locations and Routing Policies**

Add Remove

2 Items Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	MA SBCE	Avaya SBCE 6.2	To CS1K76	0	<input type="checkbox"/>	CS1K7.6	Inbound Calls to CS1K76

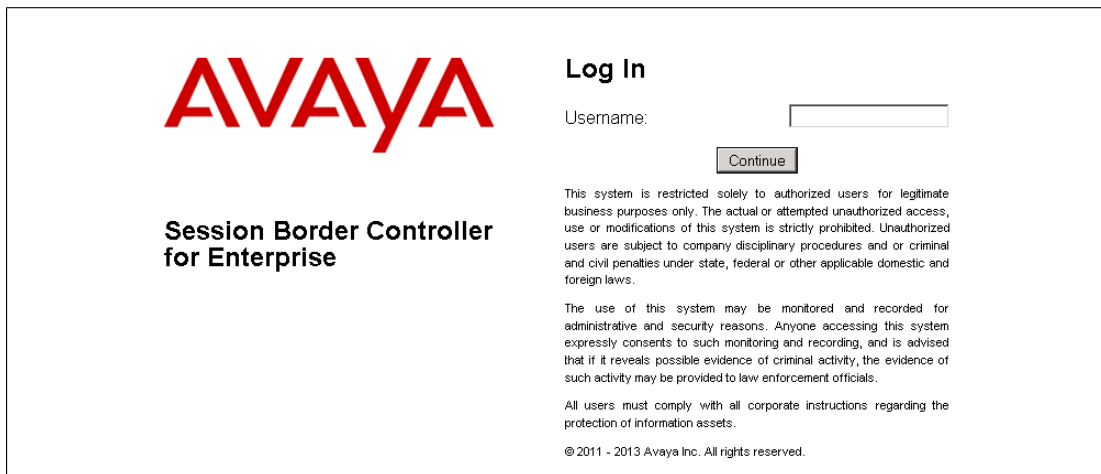
Repeat this procedure as needed to define additional dial patterns for other numbers assigned to the enterprise by the service provider, to be routed to the CS1000.

## 7. Configure Avaya Session Border Controller for Enterprise

In the sample configuration, the Avaya SBCE is used as the edge device between the Avaya CPE and the Frontier SIP Trunking service. It is assumed that the initial installation of the Avaya SBCE and the assignment of the management interface IP Address have already been completed; hence these tasks are not covered in these Application Notes. For more information on the SBC installation and initial provisioning, consult the Avaya SBCE documentation listed in the **References in Section 11**.

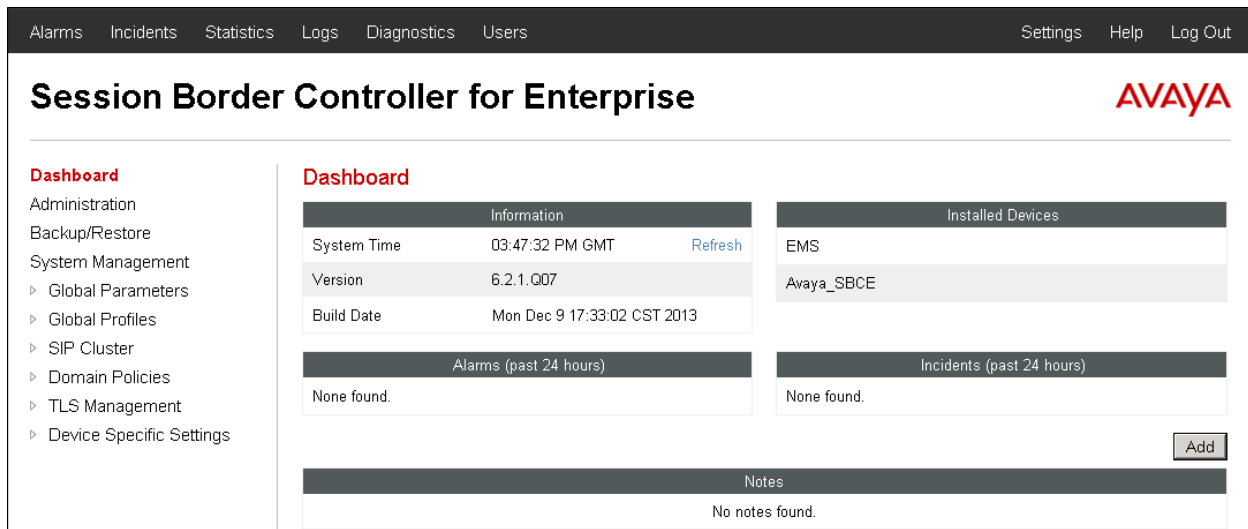
### 7.1. System Access

Access the Session Border Controller web management interface by using a web browser and entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation. Log in using the appropriate credentials.



The screenshot shows the login page for the Avaya Session Border Controller for Enterprise. On the left is the Avaya logo and the product name. On the right, there is a 'Log In' section with a 'Username:' label and an input field. Below the input field is a 'Continue' button. Underneath the button is a disclaimer: 'This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws.' Below the disclaimer is another paragraph: '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.' At the bottom, it says 'All users must comply with all corporate instructions regarding the protection of information assets.' and '© 2011 - 2013 Avaya Inc. All rights reserved.'

Once logged in, the Dashboard screen is presented. The left navigation pane contains the different available menu items used for the configuration of the Avaya SBCE.



The screenshot shows the dashboard of the Avaya Session Border Controller for Enterprise. At the top, there is a navigation bar with links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. Below the navigation bar is the title 'Session Border Controller for Enterprise' and the Avaya logo. The main content area is divided into several sections. On the left is a navigation pane with the following items: Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, SIP Cluster, Domain Policies, TLS Management, and Device Specific Settings. The main content area has a 'Dashboard' title and contains several widgets: 'Information' (System Time: 03:47:32 PM GMT, Version: 6.2.1.Q07, Build Date: Mon Dec 9 17:33:02 CST 2013), 'Installed Devices' (EMS, Avaya\_SBCE), 'Alarms (past 24 hours)' (None found), 'Incidents (past 24 hours)' (None found), and 'Notes' (No notes found). There is an 'Add' button next to the Notes section.

## 7.2. System Management

To view current system information, select **System Management** on the left navigation pane. A list of installed devices is shown in the **Devices** tab on the right pane. In the reference configuration, a single device named **Avaya\_SBCE** is shown. The management IP address that was configured during installation and the current software version are shown here. Note that the management IP address needs to be on a subnet separate from the ones used in all other interfaces of the Avaya SBCE, segmented from all VoIP traffic. Verify that the **Status** is **Commissioned**, indicating that the initial installation process of the device has been previously completed, as shown on the screen 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

**System Management**

Devices Updates SSL VPN Licensing

Device Name (Serial Number)	Management IP	Version	Status				
Avaya_SBCE (9PC63700132)	192.168.10.70	6.2.1.Q07	Commissioned	Reboot	Shutdown	Restart Application	View Edit Delete

To view the network configuration assigned to the Avaya SBCE, click **View** on the screen above. The **System Information** window is displayed, containing the current device and the network settings. Note that the **A1** and **B1** interfaces correspond to the inside and outside interfaces for the Avaya SBCE. The highlighted **A1** and **B1** IP addresses are the ones relevant to these Application Notes, for the configuration of the SIP trunk to Frontier.

**System Information: Avaya\_SBCE**

**General Configuration**

Appliance Name Avaya\_SBCE  
Box Type SIP  
Deployment Mode Proxy

**Device Configuration**

HA Mode No  
Two Bypass Mode No

**Network Configuration**

IP	Public IP	Netmask	Gateway	Interface
10.5.5.72	10.5.5.72	255.255.255.0	10.5.5.254	A1
172.16.157.148	172.16.157.148	255.255.255.0	172.16.157.129	B1
10.5.5.73	10.5.5.73	255.255.255.0	10.5.5.254	A1
172.16.157.146	172.16.157.146	255.255.255.0	172.16.157.129	B1
172.16.157.145	172.16.157.145	255.255.255.0	172.16.157.129	B1

**DNS Configuration**

Primary DNS 172.16.216.122  
Secondary DNS 10.10.153.242  
DNS Location DMZ  
DNS Client IP 172.16.157.148

**Management IP(s)**

IP 192.168.10.70

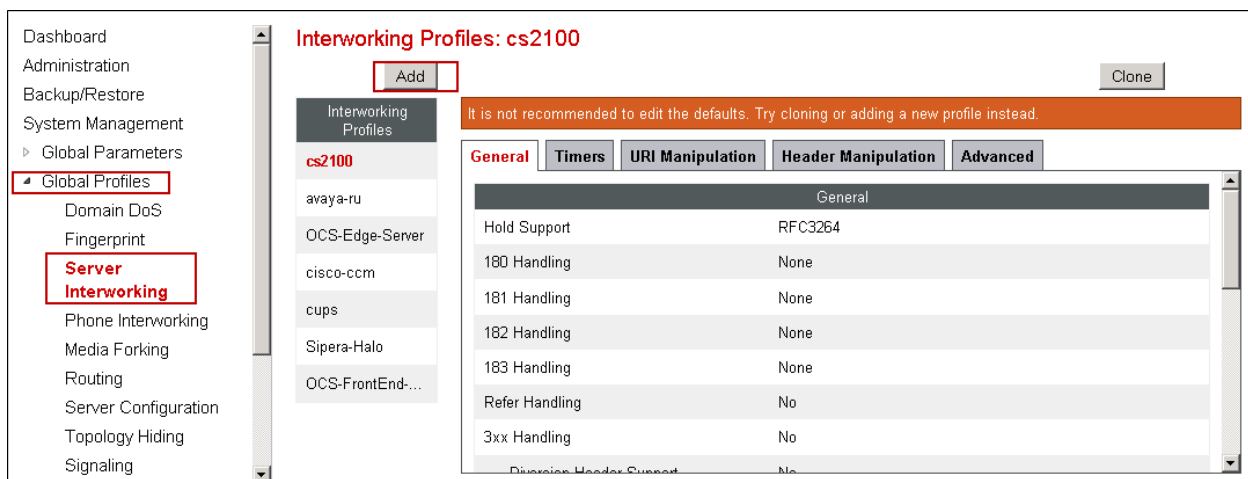
### 7.3. Global Profiles

The Global Profiles Menu, on the left navigation pane, allows the configuration of parameters across all Avaya SBCE appliances.

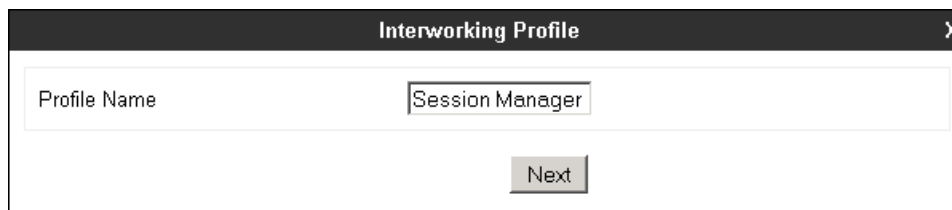
#### 7.3.1. Server Interworking

Interworking Profile features are configured to facilitate the interoperability between the enterprise SIP-enabled solution (Call Server) and the SIP trunk service provider (Trunk Server). In the reference configuration, Session Manager functions as the Call Server and the Frontier SIP Proxy as the Trunk Server.

To configure the interworking profile in the enterprise direction, select **Global Profiles** → **Server Interworking** on the left navigation pane. Click **Add**.



Enter a descriptive name for the new profile. Click **Next**.



On the **General** screen, check the **T.38 Support** box. All other parameters retain their default values. Click **Next**.

The screenshot shows a configuration window titled "Interworking Profile" with a close button (X) in the top right corner. The window is divided into a "General" tab and a list of settings. The "T.38 Support" checkbox is checked and highlighted with a red border. The other settings are as follows:

Setting	Value
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"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
<b>T.38 Support</b>	<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

At the bottom of the window, there are two buttons: "Back" and "Next".

Click **Next** on the **Privacy/DTMF** and **SIP Timers/Transport Timers** tabs (not shown). On the **Advanced Settings** tab, uncheck the **Topology Hiding: Change Call-ID** box and check the **AVAYA Extensions** box. Click **Finish** to save and exit.

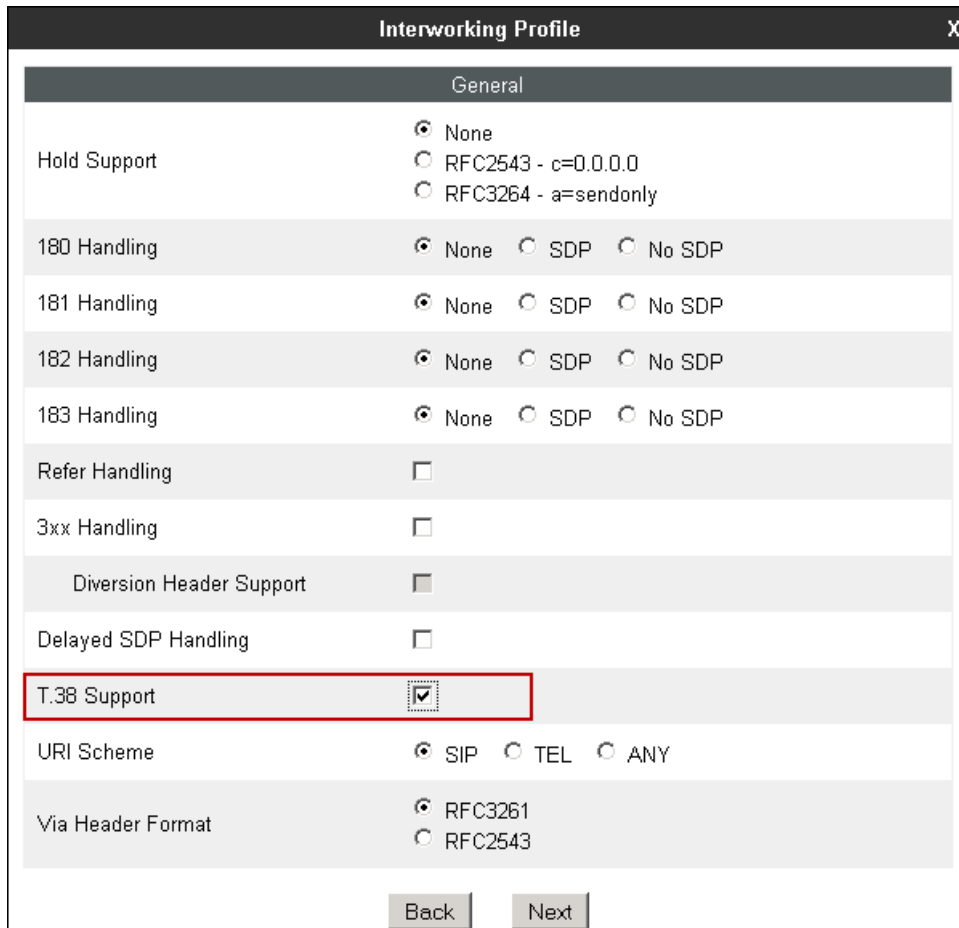
Interworking Profile	
Record Routes	<input type="radio"/> None <input type="radio"/> Single Side <input checked="" type="radio"/> Both Sides
Topology Hiding: Change Call-ID	<input type="checkbox"/>
Call-Info NAT	<input type="checkbox"/>
Change Max Forwards	<input checked="" type="checkbox"/>
Include End Point IP for Context Lookup	<input type="checkbox"/>
OCS Extensions	<input type="checkbox"/>
AVAYA Extensions	<input checked="" 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"/>
<input type="button" value="Back"/> <input type="button" value="Finish"/>	

A second interworking profile named *Service Provider* in the direction of the SIP trunk to Frontier was similarly created. For this profile default values were used for all parameters except for **T.38 Support**, which was checked.



The screenshot shows a window titled "Interworking Profile" with a close button (X) in the top right corner. Below the title bar, there is a text input field labeled "Profile Name" containing the text "Service Provider". Below the input field is a "Next" button.

**General tab:**



The screenshot shows the "Interworking Profile" window with the "General" tab selected. The settings are as follows:

Setting	Value
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"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
<b>T.38 Support</b>	<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

At the bottom of the window are "Back" and "Next" buttons.



**Advanced Settings** tab:

**Interworking Profile** X

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"/>

### 7.3.2. Signaling Manipulation

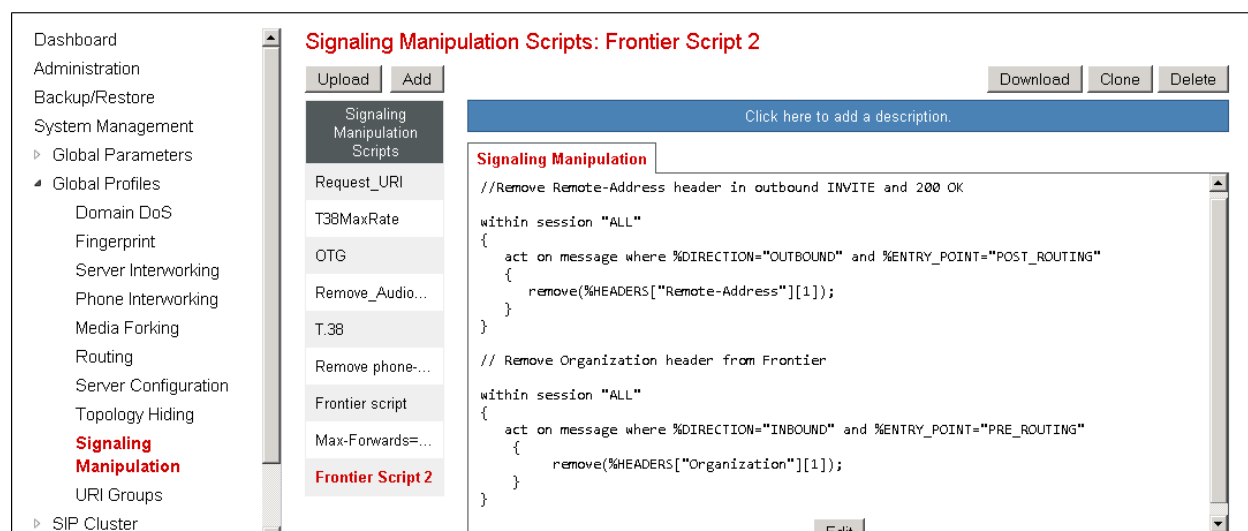
The Signaling Manipulation feature of the Avaya SBCE allows an administrator to perform a granular header manipulation on the headers of the SIP messages, which sometimes is not possible by direct configuration on the web interface. This ability to configure header manipulation in such a highly flexible manner is achieved by the use of a proprietary scripting language called SigMa.

The script can be created externally as a regular text file and imported in the Signaling Manipulation screen, or they can be written directly in the page using the embedded Sigma Editor. In the reference configuration, the Editor was used. A detailed description of the structure of the SigMa scripting language and details on its use is beyond the scope of these Application Notes. Consult [13] on the **References** section for more information on this topic.

With the purpose of blocking private enterprise information from being propagated to the public network, and to reduce the size of outbound SIP messages sent to Frontier, Signaling Rules are used, later in **Section 7.4.1**, to remove unnecessary headers. In addition, a Sigma script was created to remove the “Remote-Address” parameter, used by the Avaya SBCE, from all outbound messages. This parameter contains private enterprise IP addresses that have no significance to the service provider. The script will additionally remove the “Organization” header on inbound messages from Frontier.

From the **Global Profiles** menu on the left panel, select **Signaling Manipulation**. Click **Add** to open the SigMa Editor screen, where the text of the script can be entered.

The screen below shows the finished Signaling Manipulation script named *Frontier Script 2*. The details of the script can be found in **Appendix A** in this document.



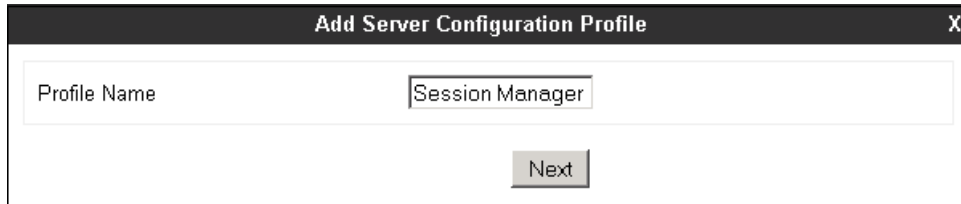
The screenshot displays the 'Signaling Manipulation Scripts: Frontier Script 2' configuration page. On the left is a navigation menu with 'Signaling Manipulation' selected. The main area shows a list of scripts with 'Frontier Script 2' highlighted. The script content is as follows:

```
//Remove Remote-Address header in outbound INVITE and 200 OK
within session "ALL"
{
  act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    remove(%HEADERS["Remote-Address"][1]);
  }
}

// Remove Organization header from Frontier
within session "ALL"
{
  act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
  {
    remove(%HEADERS["Organization"][1]);
  }
}
```

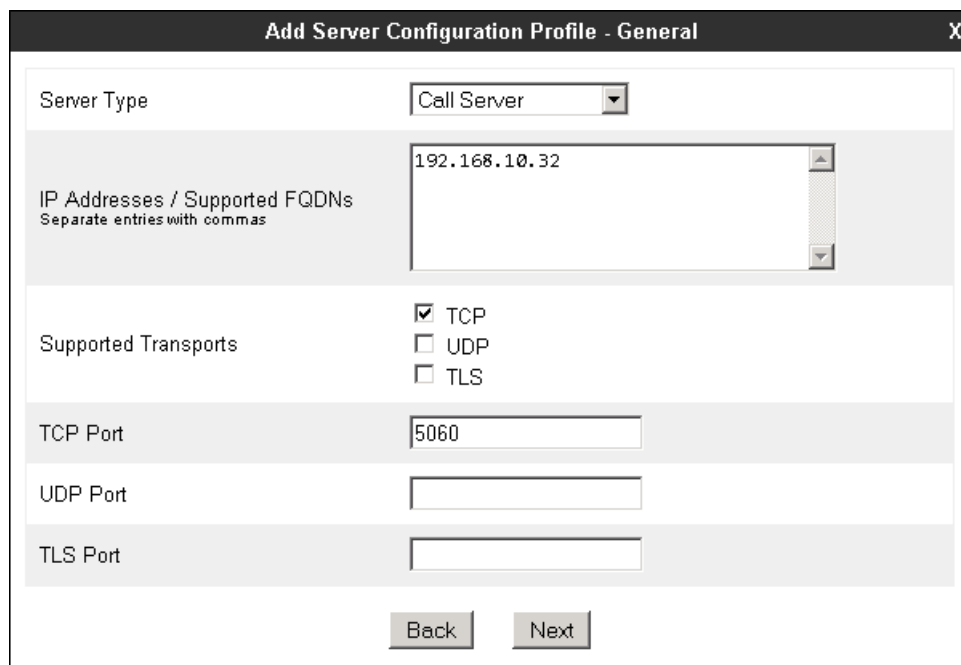
### 7.3.3. Server Configuration

Server Profiles are created to define the parameters for the Avaya SBCE two peers, i.e., Session Manager (Call Server) and the SIP Proxy at the service provider's network (Trunk Server). From the **Global Profiles** menu on the left-hand navigation pane, select **Server Configuration** and click the **Add** button (not shown) to add a new profile for the Call Server. Enter an appropriate **Profile Name** similar to the screen below. Click **Next**.



The screenshot shows a dialog box titled "Add Server Configuration Profile" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" containing the text "Session Manager". Below the input field is a "Next" button.

On the **Add Server Configuration Profile - General** Tab select **Call Server** from the drop-down menu for the **Server Type**. On the **IP Addresses / Supported FQDNs** field, enter the IP address of the Session Manager Security Module. Select **TCP** for **Supported Transports**, and enter **5060** under **TCP Port**. The transport protocol and port selected here must match the values defined for the Session Manager SIP entity in **Section 6.4**. Click **Next**.

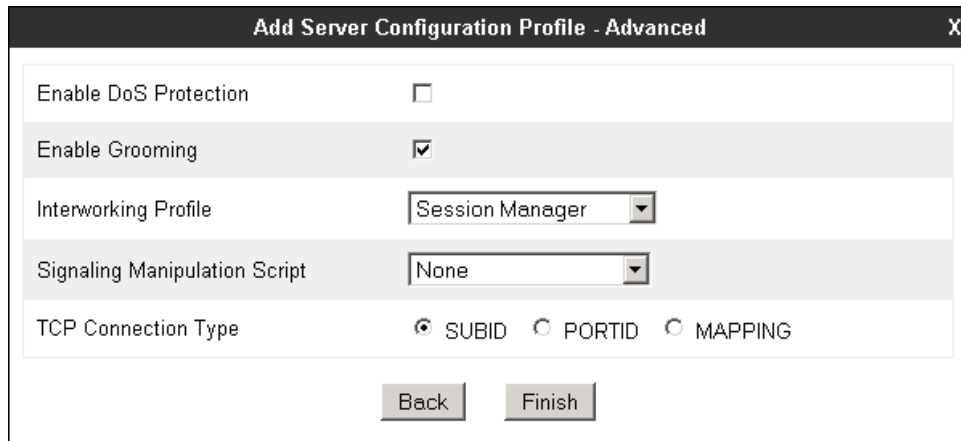


The screenshot shows a dialog box titled "Add Server Configuration Profile - General" with a close button (X) in the top right corner. The dialog contains several fields and options:

- Server Type:** A dropdown menu set to "Call Server".
- IP Addresses / Supported FQDNs:** A text area containing "192.168.10.32". Below the text area is the instruction "Separate entries with commas".
- Supported Transports:** Three radio button options: "TCP" (checked), "UDP", and "TLS".
- TCP Port:** A text input field containing "5060".
- UDP Port:** An empty text input field.
- TLS Port:** An empty text input field.

At the bottom of the dialog are "Back" and "Next" buttons.

Click **Next** on the **Authentication** and **Heartbeat** tabs (not shown). On the **Advanced** tab, since TCP is used, check the **Enable Grooming** box. Select **Session Manager** from the **Interworking Profile** drop-down menu. Click **Finish**.

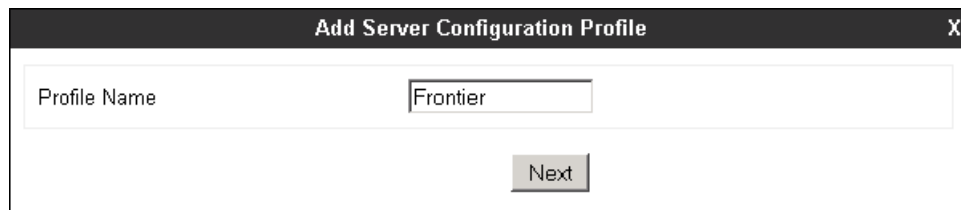


The screenshot shows a dialog box titled "Add Server Configuration Profile - Advanced". It contains the following settings:

- Enable DoS Protection:
- Enable Grooming:
- Interworking Profile: Session Manager (selected in a dropdown menu)
- Signaling Manipulation Script: None (selected in a dropdown menu)
- TCP Connection Type:  SUBID,  PORTID,  MAPPING

At the bottom, there are two buttons: "Back" and "Finish".

Similarly, to add the profile for the Trunk Server, click the **Add** button on the **Server Configuration** screen (not shown). Enter an appropriate **Profile Name** similar to the screen below. Click **Next**.



The screenshot shows a dialog box titled "Add Server Configuration Profile". It contains the following settings:

- Profile Name: Frontier (entered in a text field)

At the bottom, there is a "Next" button.

On the **Add Server Configuration Profile-General** Tab select *Trunk Server* from the drop-down menu for the **Server Type**. On the **IP Addresses / Supported FQDNs** field, enter the IP address of the Frontier SIP proxy server. Select **UDP** for **Supported Transports**, and enter *5060* under **UDP Port**, as specified by Frontier. Click **Next**.

**Add Server Configuration Profile - General**

Server Type: Trunk Server

IP Addresses / Supported FQDNs: 192.168.24.12  
Separate entries with commas

Supported Transports:  
 TCP  
 UDP  
 TLS

TCP Port: [ ]

UDP Port: 5060

TLS Port: [ ]

Back Next

Click **Next** on the **Authentication** and **Heartbeat** tabs (not shown). On the **Advanced** tab, select *Service Provider* from the **Interworking Profile** drop-down menu. Under **Signaling Manipulation Script**, select the *Frontier Script 2* created on the previous section. Click **Finish**.

**Add Server Configuration Profile - Advanced**

Enable DoS Protection:

Enable Grooming:

Interworking Profile: Service Provider

Signaling Manipulation Script: Frontier Script 2

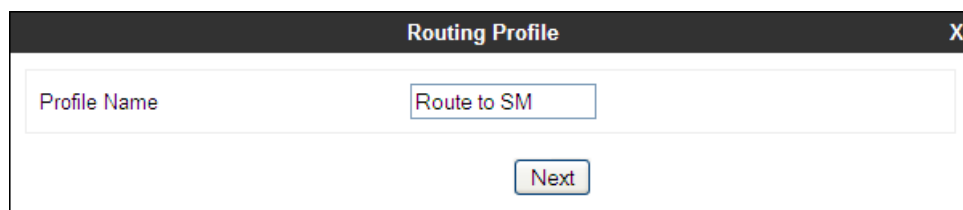
UDP Connection Type:  SUBID  PORTID  MAPPING

Back Finish

### 7.3.4. Routing Profiles

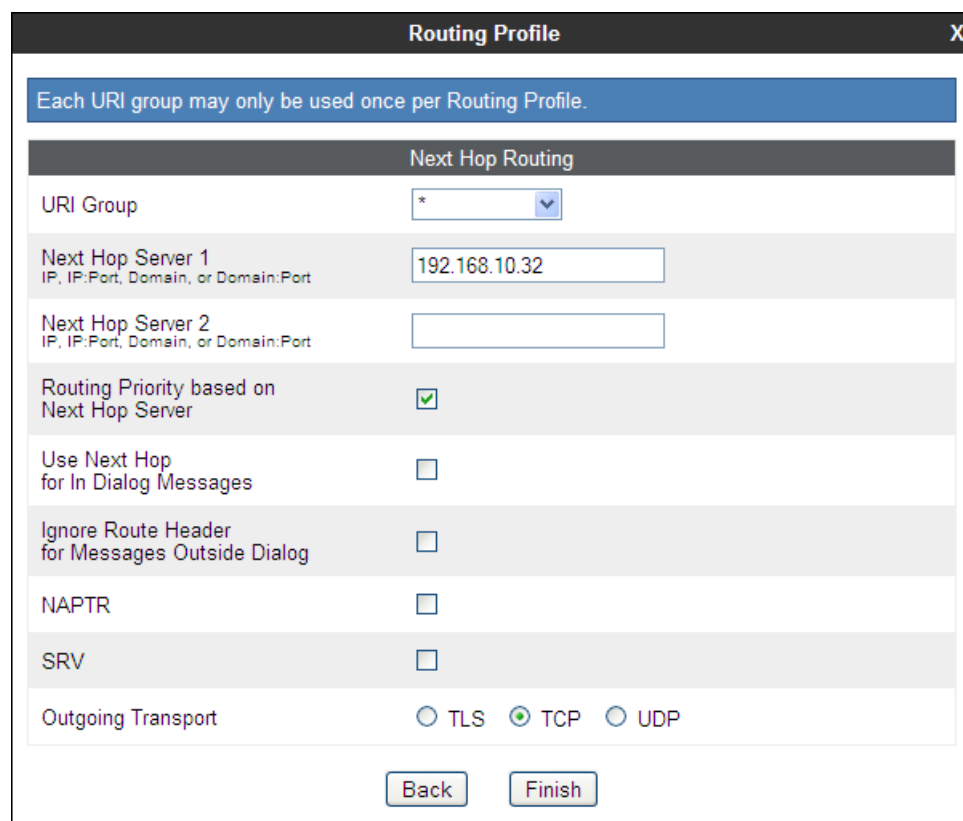
Routing profiles define a specific set of routing criteria that is used, in addition to other types of domain policies, to determine the path that the SIP traffic will follow as it flows through the Avaya SBCE interfaces.

Two Routing Profiles were created in the test configuration, one for inbound calls, with Session Manager as the destination, and the second one for outbound calls, which are routed to the Frontier SIP trunk. To create the inbound route, select the **Routing** tab from the **Global Profiles** menu on the left-hand side and select **Add** (not shown). Enter an appropriate **Profile Name** similar to the example below. Click **Next**.



The screenshot shows a window titled "Routing Profile" with a close button (X) in the top right corner. Below the title bar is a text input field labeled "Profile Name" containing the text "Route to SM". Below the input field is a button labeled "Next".

On the **Next Hop Routing** tab, enter the IP Address of Session Manager as **Next Hop Server 1**. Since the default well-known port value of 5060 for TCP was used, it is not necessary to enter the port number here. Check **Routing Priority based on Next Hop Server**. Choose **TCP** for **Outgoing Transport**. Click **Finish**.

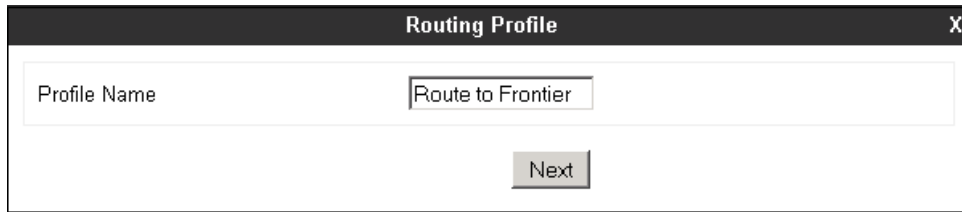


The screenshot shows a window titled "Routing Profile" with a close button (X) in the top right corner. Below the title bar is a blue banner with the text "Each URI group may only be used once per Routing Profile." Below the banner is a section titled "Next Hop Routing". The "Next Hop Routing" section contains the following fields and options:

- URI Group: A dropdown menu with the value "\*" selected.
- Next Hop Server 1: A text input field containing "192.168.10.32". Below the field is the text "IP, IP:Port, Domain, or Domain:Port".
- Next Hop Server 2: An empty text input field. Below the field is the text "IP, IP:Port, Domain, or Domain:Port".
- Routing Priority based on Next Hop Server: A checkbox that is checked.
- Use Next Hop for In Dialog Messages: An unchecked checkbox.
- Ignore Route Header for Messages Outside Dialog: An unchecked checkbox.
- NAPTR: An unchecked checkbox.
- SRV: An unchecked checkbox.
- Outgoing Transport: Three radio buttons labeled "TLS", "TCP", and "UDP". The "TCP" radio button is selected.

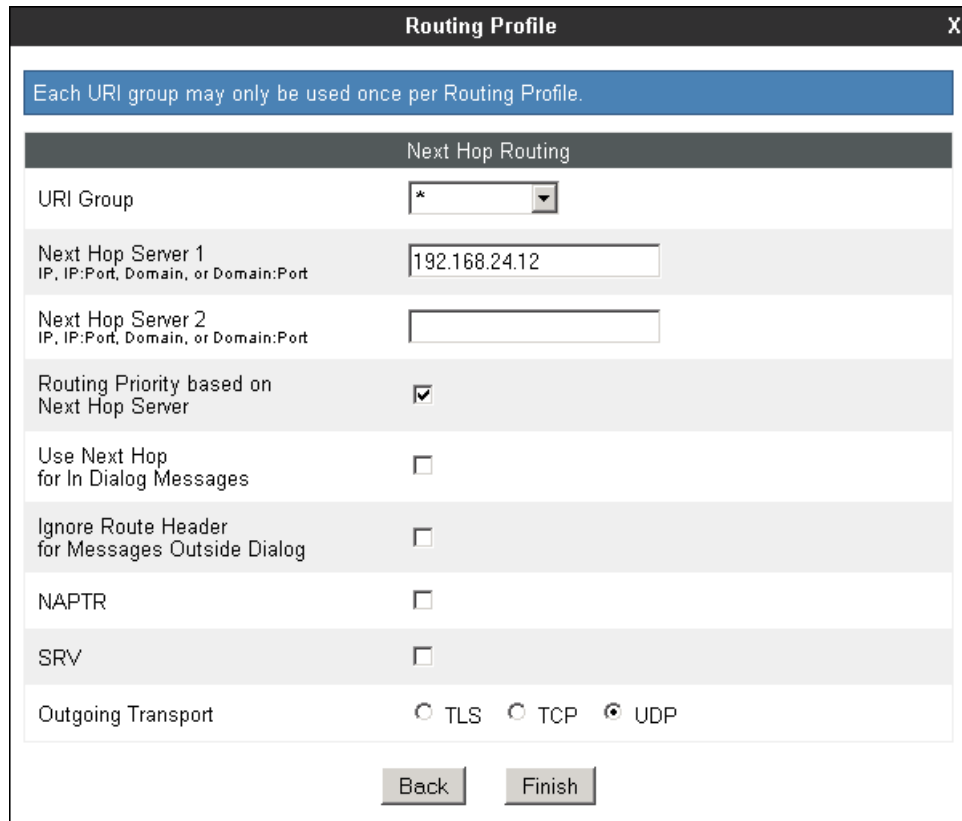
At the bottom of the window are two buttons: "Back" and "Finish".

Back at the **Routing** tab, select **Add** (not shown) to repeat the process in order to create the outbound route. Enter an appropriate **Profile Name**. Click **Next**.



The screenshot shows a dialog box titled "Routing Profile" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Profile Name" containing the text "Route to Frontier". Below the input field is a button labeled "Next".

On the Next Hop Routing tab, enter the IP address of the service provider SIP proxy server as **Next Hop Server 1**. Since the default well-known port value of 5060 for UDP was used, it is not necessary to enter the port number here. Check the **Routing Priority based on Next Hop Server**. Choose **UDP** for **Outgoing Transport**. Click **Finish**.



The screenshot shows the "Routing Profile" dialog box with the "Next Hop Routing" tab selected. At the top, a blue banner reads "Each URI group may only be used once per Routing Profile." Below this, the "Next Hop Routing" section contains the following fields and options:

- URI Group: A dropdown menu with an asterisk (\*) selected.
- Next Hop Server 1: A text input field containing "192.168.24.12". Below the field is the label "IP, IP:Port, Domain, or Domain:Port".
- Next Hop Server 2: An empty text input field. Below the field is the label "IP, IP:Port, Domain, or Domain:Port".
- Routing Priority based on Next Hop Server: A checkbox that is checked.
- Use Next Hop for In Dialog Messages: An unchecked checkbox.
- Ignore Route Header for Messages Outside Dialog: An unchecked checkbox.
- NAPTR: An unchecked checkbox.
- SRV: An unchecked checkbox.
- Outgoing Transport: Radio buttons for TLS, TCP, and UDP. The UDP option is selected.

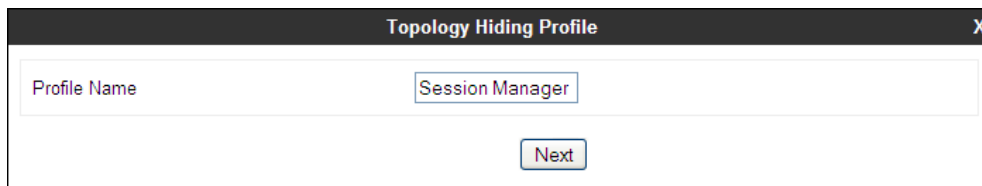
At the bottom of the dialog, there are two buttons: "Back" and "Finish".

### 7.3.5. Topology Hiding

Topology Hiding is a security feature that allows the modification of several SIP headers, preventing private enterprise network information from being propagated to the untrusted public network.

Topology Hiding can also be used as an interoperability tool to adapt the host portion in the SIP headers to the IP addresses or domains expected on the service provider and the enterprise networks. For the compliance test, only the minimum configuration required to achieve interoperability on the SIP trunk was performed. Additional steps can be taken in this section to further mask the information that is sent from the enterprise to the public network.

To add the **Topology Hiding Profile** in the enterprise direction, select **Topology Hiding** from the **Global Profiles** menu on the left-hand side and click the **Add** button (not shown). Enter a **Profile Name** such as the one shown below. Click **Next**.



Topology Hiding Profile

Profile Name: Session Manager

Next

On the **Topology Hiding Profile** screen, click the **Add Header** button repeatedly to show the rest of the headers in the profile.



Topology Hiding Profile

Add Header

Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP/Domain	Auto	

Delete

Back Finish



For the **Request-Line**, **From** and **To** headers, select **Overwrite** in the **Replace Action** column and enter the enterprise SIP domain known by the Session Manager, **avaya.lab.com**, in the **Overwrite Value** column of these headers, as shown below. Default values were used for all other fields. Click **Finish**.

Header	Criteria	Replace Action	Overwrite Value	
Request-Line	IP/Domain	Overwrite	avaya.lab.com	Delete
From	IP/Domain	Overwrite	avaya.lab.com	Delete
To	IP/Domain	Overwrite	avaya.lab.com	Delete
Record-Route	IP/Domain	Auto		Delete
Via	IP/Domain	Auto		Delete
SDP	IP/Domain	Auto		Delete
Refer-To	IP/Domain	Auto		Delete
Referred-By	IP/Domain	Auto		Delete

A **Topology Hiding Profiles** named **Service Provider** was similarly configured in the direction of the SIP trunk to Frontier. During the compliance test, IP addresses instead of domains were used in all SIP messages between the Frontier SIP proxy server and the Avaya SBCE. Note that since the default action of **Auto** implies the insertion of IP addresses in the host portion of these headers, it was not necessary to modify any of the headers sent to the service provider.

**Topology Hiding Profiles: Service Provider**

Click here to add a description.

**Topology Hiding**

Header	Criteria	Replace Action	Overwrite Value
Via	IP/Domain	Auto	---
To	IP/Domain	Auto	---
From	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---
Request-Line	IP/Domain	Auto	---

## 7.4. Domain Policies

Domain Policies allow the configuration of sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise. Domain Policies include rules for Application, Media, Signaling, Security, etc.

In the reference configuration, two new Signaling Rules were created. All other rules under Domain Policies, linked together on the End Point Policy Groups later in this section, used one of the default sets already pre-defined in the configuration. Please note that changes should not be made to any of the defaults. If changes are needed, it is recommended to create a new rule by cloning one of the defaults and then make the necessary changes to the new rule.

### 7.4.1. Signaling Rules


A Signaling Rule named *Frontier SM Side* was created to remove (block) unnecessary headers from outbound SIP messages.

The following headers were blocked:

- Alert-Info
- AV-Global-Session-ID
- Endpoint-View
- History-Info
- P-AV-Message-ID
- P-Charging-Vector
- P-Location
- User Agent

These headers are sent in messages from the Session Manager to the Avaya SBCE. They contain private IP addresses and SIP Domains from the enterprise, which should not be propagated outside of the enterprise boundaries. This signaling rule had the additional purpose of reducing the size of the messages sent to Frontier.

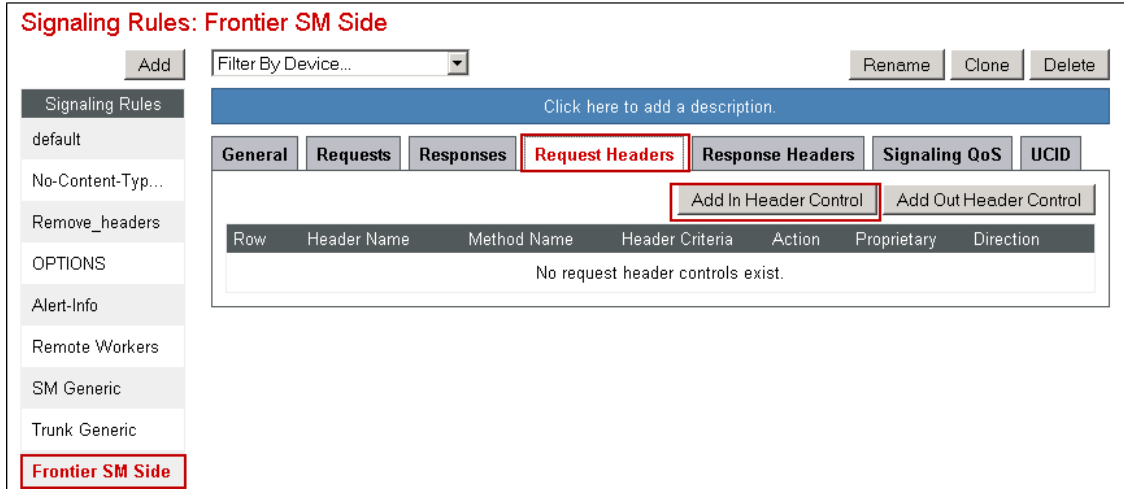
In the **Domain Policies** menu on the left-hand side, select **Signaling Rules**, then **Add Rule** (not shown). Enter an appropriate name like in the example below. Click **Next**.



The image shows a dialog box titled "Signaling Rule" with a close button (X) in the top right corner. Inside the dialog, there is a text input field labeled "Rule Name" containing the text "Frontier SM Side". Below the input field is a "Next" button.

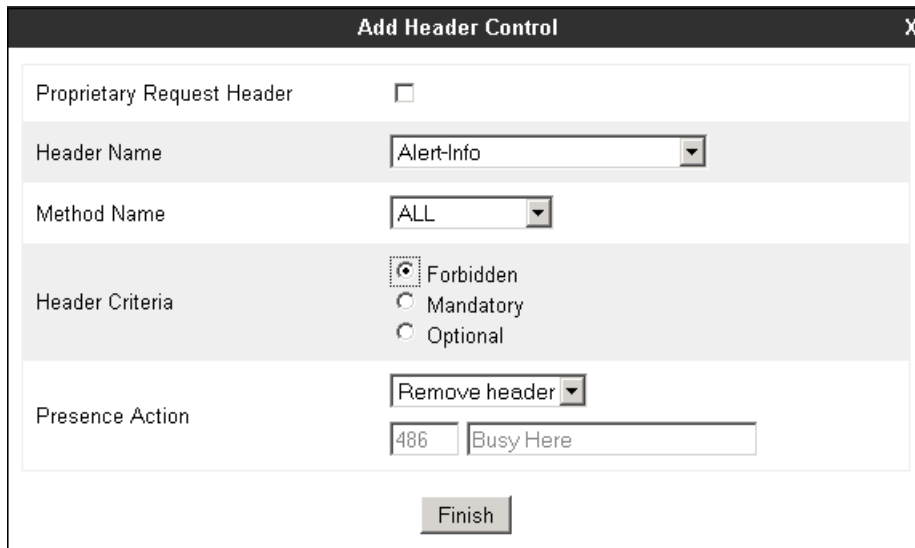
On the next three pages (not shown), leave sections **Inbound**, **Outbound** and **Content-Type Policies** with their default values. Default values were also used on the **Signaling QoS** and **UCID** tabs. Click **Finish**.

On the newly created **Signaling Rule**, select the **Request Headers** tab to create the manipulations to be performed on request messages. Select **Add In Header Control**.



In the **Add Header Control** screen select the following:

- **Header Name:** *Alert-Info*
- **Method Name:** *ALL*
- **Header Criteria:** Check **Forbidden**
- **Presence Action:** *Remove Header*
- Click **Finish**



Select **Add In Header Control** as needed to configure the remaining header control rules. Make sure to check the **Proprietary Request Header** box as appropriate in the **Add Header Control** tab, to be allowed to type the name of proprietary headers on the **Header Name** box. Once completed, the **Request Headers** tab should look like the following screen.

Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction		
1	AV-Global-Session-ID	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	Alert-Info	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
3	Endpoint-View	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
4	History-Info	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
5	P-AV-Message-ID	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
6	P-Charging-Vector	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
7	P-Location	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
8	User-Agent	ALL	Forbidden	Remove Header	No	IN	Edit	Delete

Select the **Response Headers** tab to similarly create the manipulations performed on response messages. Select **Add In Header Control** (not shown).

The screen below shows the settings for the Alert-Info header on response messages.

**Add Header Control** X

---

Proprietary Response Header

Header Name

Response Code

Method Name

Header Criteria  Forbidden  
 Mandatory  
 Optional

Presence Action

Select **Add In Header Control** as needed to configure the remaining header control rules. Make sure to check the **Proprietary Request Header** box as appropriate in the **Add Header Control** tab to be allowed to type the name of proprietary headers on the **Header Name** box. Once completed, the **Response Headers** tab should look like the following screen.

Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction		
1	AV-Global-Session-ID	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
2	AV-Global-Session-ID	200	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
3	Alert-Info	200	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
4	Endpoint-View	200	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
5	History-Info	1XX	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
6	History-Info	2XX	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
7	P-AV-Message-ID	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
8	P-AV-Message-ID	200	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
9	P-Charging-Vector	200	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
10	P-Location	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
11	P-Location	200	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete

A second **Signaling Rule** named *Frontier Trunk Side* was created in order to block OPTIONS messages sent by Frontier from passing through the Avaya SBCE to Session Manager, and return a 200 OK as the response. In this case, on the **Requests** tab, click on **Add In Request Control** to add the new Request Control. Once completed, the **Request tab** of the newly created Signaling Rule should look like the screen below.

Row	Method Name	In Dialog Action	Out of Dialog Action	Proprietary	Direction		
1	OPTIONS	Block with "200 OK"	Block with "200 OK"	No	In	Edit	Delete

## 7.4.2. End Point Policy Groups

End Point Policy Groups associate the different sets of rules (Media, Signaling, Security, etc) to be applied to specific SIP messages traversing through the Avaya SBCE.

To create an End Point Policy Group for the enterprise, select **End Point Policy Groups** under the **Domain Policies** menu. Select **Add** (not shown).

Enter an appropriate name in the **Group Name** field. *Enterprise* was used. Click **Next**.

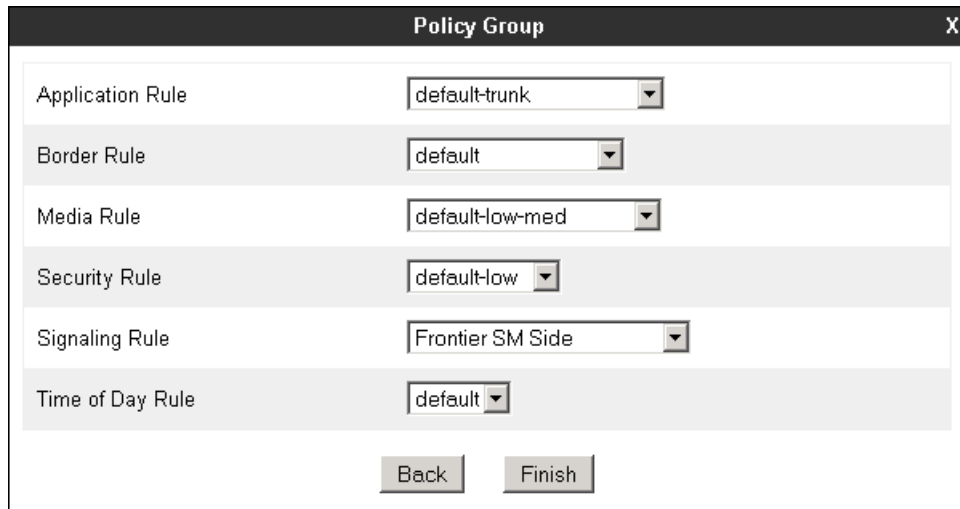


Policy Group

Group Name: Enterprise

Next

In the Policy Group tab, all fields used one of the default sets already pre-defined in the configuration, with the exception of the **Signaling Rule**, where the *Frontier SM Side* rule created in **Section 7.4.1** was selected. Click **Finish**.



Policy Group

Application Rule: default-trunk

Border Rule: default

Media Rule: default-low-med

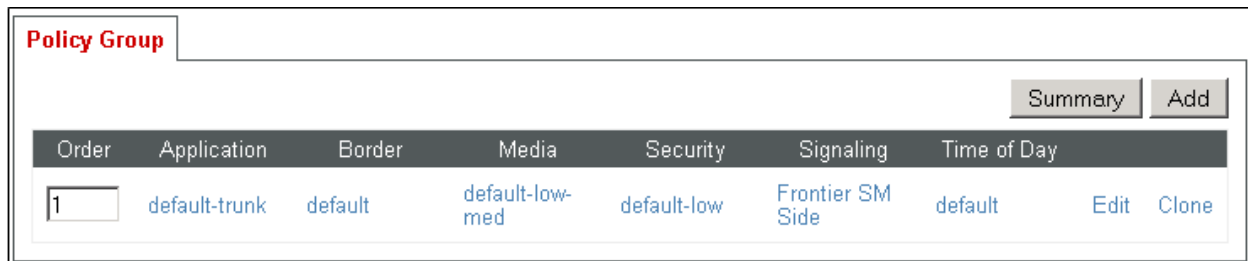
Security Rule: default-low

Signaling Rule: Frontier SM Side

Time of Day Rule: default

Back Finish

The screen below shows the *Enterprise* End Point Policy Group after the configuration was completed.



Policy Group

Summary Add

Order	Application	Border	Media	Security	Signaling	Time of Day		
1	default-trunk	default	default-low-med	default-low	Frontier SM Side	default	Edit	Clone

A second End Point Policy Group was similarly created for the service provider, repeating the steps described previously. All fields used one of the default sets already pre-defined in the configuration, with the exception of the **Signaling Rule**, where the *Frontier Trunk Side* rule created in **Section 7.4.1** was selected.

The screen below shows the *Service Provider* End Point Policy Group after the configuration was completed.

Policy Group								Summary	Add
Order	Application	Border	Media	Security	Signaling	Time of Day			
1	default-trunk	default	default-low-med	default-low	Frontier Trunk Side	default	Edit	Clone	

## 7.5. Device Specific Settings

The **Device Specific Settings** determine server specific parameters that determine how the device will work when deployed on the network. Among the parameters defined here are IP addresses, media and signaling interfaces, call flows, etc.

### 7.5.1. Network Management

The network configuration parameters should have been previously specified during installation of the Avaya SBCE. In the event that changes need to be made to the network configuration, they can be entered here.

Select **Network Management** from **Device Specific Settings** on the left-side menu (not shown). Under **Devices** in the centre pane, select the device being managed, **Avaya\_SBCE** in the sample configuration. On the **Network Configuration** tab, verify or enter the network information as needed. Note that the **A1** interface is used for the internal side and **B1** is used for the external side of the Avaya SBCE.

**Network Management: Avaya\_SBCE**

Devices

Avaya\_SBCE

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](#).

A1 Netmask

A2 Netmask

B1 Netmask

B2 Netmask

IP Address	Public IP	Gateway	Interface	
<input type="text" value="10.5.5.72"/>	<input type="text"/>	<input type="text" value="10.5.5.254"/>	A1	Delete
<input type="text" value="172.16.157.148"/>	<input type="text"/>	<input type="text" value="172.16.157.129"/>	B1	Delete

On the **Interface Configuration** tab, verify the **Administrative Status** is **Enabled** for both the **A1** and **B1** interfaces. Click the **Toggle** buttons if necessary to enable the interfaces.

Network Configuration		Interface Configuration	
Devices			
Avaya_SBCE			
Name	Administrative Status		
A1	Enabled	Toggle	
A2	Disabled	Toggle	
B1	Enabled	Toggle	
B2	Disabled	Toggle	

## 7.5.2. Media Interface

Media Interfaces were created to specify the IP address and port range in which the Avaya SBCE will accept media streams on each interface. Packets leaving the interfaces of the Avaya SBCE will advertise this IP address and one of the ports in this range as the listening IP address and port in which it will accept media from the Call or Trunk Server.

To add the Media Interface in the enterprise direction, select **Media Interface** from the **Device Specific Settings** menu on the left-hand side, select the **Avaya\_SBCE** device and click the **Add** button (not shown). On the **Add Media Interface** screen, enter an appropriate **Name** for the Media Interface. Select the private IP Address for the Avaya SBCE from the **IP Address** drop-down menu. The **Port Range** was left at the default values of **35000-40000**. Click **Finish**.

**Add Media Interface** X

---

Name

IP Address

Port Range  -

A second Media Interface facing the public network side was similarly created with the name **Public\_med**, as shown below. The outside IP Address of the Avaya SBCE was selected from the drop-down menu. The **Port Range** was left at the default values.

**Add Media Interface** X

---

Name

IP Address

Port Range  -



Once the configuration is complete, the **Media Interface** screen will appear as follows.

**Media Interface: Avaya\_SBCE**

Devices  
Avaya\_SBCE

**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	Edit	Delete
Private_med	10.5.5.72	35000 - 40000	Edit	Delete
Public_med	172.16.157.148	35000 - 40000	Edit	Delete

### 7.5.3. Signaling Interface

Signaling Interfaces are created to specify the IP addresses and ports in which the Avaya SBCE will listen for signaling traffic in both the inside and outside networks.

To add the Signaling Interface in the enterprise direction, select **Signaling Interface** from the **Device Specific Settings** menu on the left-hand side, select the **Avaya\_SBCE** device and click the **Add** button (not shown). On the **Add Signaling Interface** screen, enter an appropriate **Name** for the interface. Select the private IP Address for the Avaya SBCE from the **IP Address** drop-down menu. Enter **5060** for **TCP Port**, since TCP port 5060 is used to listen to signaling traffic from Session Manager in the sample configuration. Click **Finish**.

**Add Signaling Interface** X

Name: Private\_sig

IP Address: 10.5.5.72

TCP Port: 5060  
Leave blank to disable

UDP Port:   
Leave blank to disable

Enable Stun:

TLS Port:   
Leave blank to disable

TLS Profile: AvayaSBCServer

Enable Shared Control:

Shared Control Port:   
Leave blank to disable

Finish

A second Signaling Interface with the name **Public\_sig** was similarly created in the network direction. The outside **IP Address** of the Avaya SBCE was selected from the drop-down menu. Under **UDP Port**, enter **5060** since this is the protocol and port used by the Avaya SBCE to listen to the service provider's SIP traffic.

Once the configuration is complete, the **Signaling Interface** screen will appear as follows:

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
Private_sig	10.5.5.72	5060	---	---	None	<a href="#">Edit</a> <a href="#">Delete</a>
Public_sig	172.16.157.148	---	5060	---	None	<a href="#">Edit</a> <a href="#">Delete</a>

### 7.5.4. End Point Flows

End Point Flows determine the path to be followed by the packets traversing through the Avaya SBCE. They also combine the different sets of rules and profiles previously configured, to be applied to the SIP traffic traveling in each direction.

To create the call flow toward the enterprise, from the **Device Specific** menu, select **End Point Flows**, then select the **Server Flows** tab. Click **Add** (not shown). The screen below shows the flow named **Session Manager Flow** created in the sample configuration. The flow uses the interfaces, policies, and profiles defined in previous sections. Note the **Routing Profile** selection, which is the reverse route of the flow. Click **Finish**.

Edit Flow: Session Manager Flow	
Flow Name	Session Manager Flow
Server Configuration	Session Manager
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Public_sig
Signaling Interface	Private_sig
Media Interface	Private_med
End Point Policy Group	Enterprise
Routing Profile	Route to Frontier
Topology Hiding Profile	Session Manager
File Transfer Profile	None
<b>Finish</b>	

A second Server Flow with the name **SIP Trunk Flow** was similarly created in the network direction. The flow uses the interfaces, policies, and profiles defined in previous sections. Note the **Routing Profile** selection, which is the reverse route of the flow. Click **Finish**.

**Edit Flow: SIP Trunk Flow** X

---

Flow Name:

Server Configuration:

URI Group:

Transport:

Remote Subnet:

Received Interface:

Signaling Interface:

Media Interface:

End Point Policy Group:

Routing Profile:

Topology Hiding Profile:

File Transfer Profile:

The two Server Flows created in the sample configuration are summarized on the screen below:

**End Point Flows: Avaya\_SBCE**

Devices

Subscriber Flows

Server Flows

Avaya\_SBCE

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	SIP Trunk Flow	*	Private_sig	Public_sig	Service Provider	Route to SM	<a href="#">View</a>	<a href="#">Clone</a>	<a href="#">Edit</a>	<a href="#">Delete</a>

**Server Configuration: Session Manager**

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	Session Manager Flow	*	Public_sig	Private_sig	Enterprise	Route to Frontier	<a href="#">View</a>	<a href="#">Clone</a>	<a href="#">Edit</a>	<a href="#">Delete</a>

## 8. Frontier Communications SIP Trunking Service Configuration

Frontier is responsible for the configuration of the SIP Trunking service on its network. The customer will need to provide to Frontier the IP address used to reach the Avaya SBCE at the enterprise. Frontier will provide the customer the necessary information to configure the SIP connection from the enterprise site to the Frontier network, including:

- IP address of the Frontier SIP Proxy server.
- Supported codecs and order of preference.
- DID numbers.
- All IP addresses and port numbers used for signaling or media that will need access to the enterprise network through any security devices.

This information is used to complete the configuration of the CS1000, Session Manager and the Avaya SBCE discussed in the previous sections.

## 9. Verification Steps

The following steps may be used to verify the configuration of the Avaya solution with the Frontier SIP Trunking service.

### 9.1. Avaya Communication Server 1000E Verification

This section illustrates sample verifications that may be performed on the CS1000, using the Avaya Unified Communication Management GUI.

#### 9.1.1. IP Network Maintenance and Reports Commands

From the CS1000 Element Manager screen, navigate to **System** → **IP Network** → **Maintenance and Reports**. Click the **Gen CMD** button as shown below.

The screenshot shows the Avaya CS1000 Element Manager interface. The main content area is titled "Node Maintenance and Reports" and displays a table for Node ID: 1006. The table has columns for Hostname, ELAN IP, Type, and TN. The data row shows Hostname: cs1k, ELAN IP: 172.16.21.61, Type: Signaling Server-Avaya CPMG, and TN: NO TN. To the right of the table are several buttons: GEN CMD (highlighted with a red box), SYS LOG, OM RPT, Reset, Status, and Virtual Terminal. The left sidebar contains a navigation menu with options like Home, Links, System, Alarms, Maintenance, Core Equipment, Peripheral Equipment, IP Network, and Nodes: Servers, Media Cards, Maintenance and Reports, Media Gateways, and Zones.

The **General Commands** screen is displayed.

The screenshot shows the "General Commands" screen. At the top, it displays "Element IP : 172.16.21.61" and "Element Type : Signaling Server-Avaya CPMG". Below this, there are two rows of input fields and buttons. The first row has a "Group" dropdown menu, a "Command" dropdown menu (set to "-- Select A Group --"), and a "RUN" button. The second row has an "IP address" field (set to 172.16.21.61), a "Number of pings" field (set to 3), and a "PING" button.

A variety of commands are available by making the appropriate selections on the **Group** and **Command** drop-down menus. For example, to check the status of the SIP Gateway to Session Manager, select *Sip* from the **Group** menu and *SIPGwShow* from the **Command** menu. Click **Run**. The example output below shows the Session Manager (192.168.10.32, port 5087, UDP) with a **SIPNPM Status** “Active”.

**General Commands**

Element IP : 172.16.21.61 Element Type : Signaling Server-Awaya CPMG

Group: Sip Command: SIPGwShow SIP PING RUN

IP address: 172.16.21.61 Number of pings: 3 PING

```

SIPNPM Status      : Active
Primary Proxy IP address : 192.168.10.32
Primary Proxy port      : 5087
Primary Proxy Transport : UDP
Secondary Proxy IP address : 0.0.0.0
Secondary Proxy port      : 5060
Secondary Proxy Transport : UDP
Primary Proxy2 IP address : 192.168.10.32
Primary Proxy2 port      : 5087
Primary Proxy2 Transport : UDP
Active Proxy          : Primary :Register Not Supported
Time To Next Registration : 0 Seconds
Channels Busy / Idle / Total : 0 / 11 / 11
Stack version          : 5.5.0.13
TLS Security Policy     : Security Disabled
  
```

### 9.1.2. System Maintenance Commands

A variety of system maintenance commands are available by navigating to **System** → **Maintenance** on the left pane. Maintenance commands can be used by either choosing the **Select by Overlay** or the **Select by Functionality** approaches.

**AVAYA CS1000 Element Manager** Help | Logout

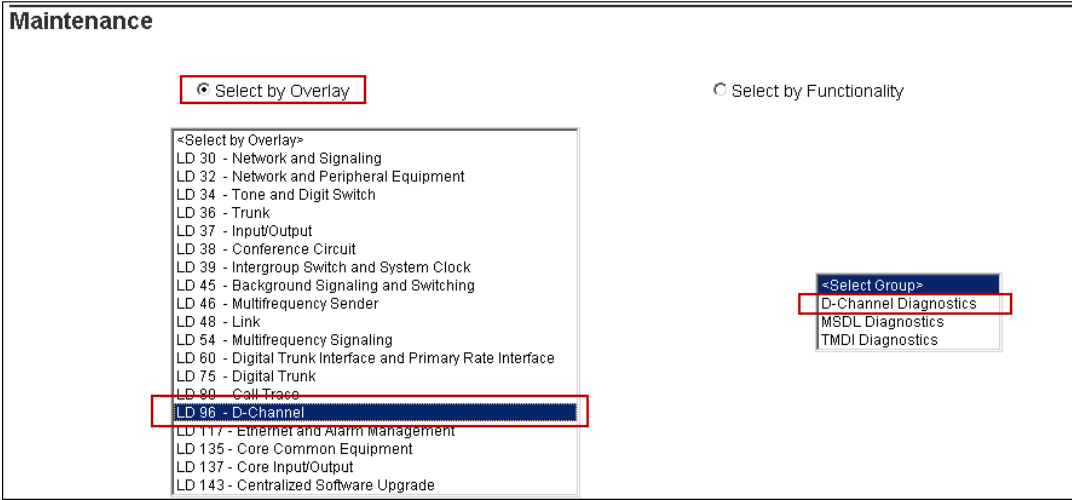
Managing: 172.16.21.61 Username: admin System > Maintenance

**Maintenance**

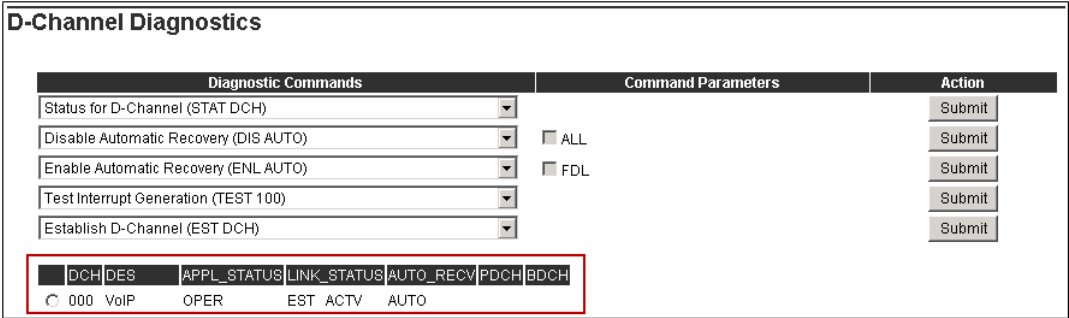
Select by Overlay  Select by Functionality

- <Select by Overlay>
- LD 30 - Network and Signaling
- LD 32 - Network and Peripheral Equipment
- LD 34 - Tone and Digit Switch
- LD 36 - Trunk
- LD 37 - Input/Output
- LD 38 - Conference Circuit
- LD 39 - Intergroup Switch and System Clock
- LD 45 - Background Signaling and Switching
- LD 46 - Multifrequency Sender
- LD 48 - Link
- LD 54 - Multifrequency Signaling

The following screen shows an example using the **Select by Overlay** approach, where the **LD 96 – D-Channel** overlay is chosen.



On the previous screen, selecting **D-Channel Diagnostic** under the **Select Group** menu will produce a screen such as the one shown below. D-Channel number **0**, which is used in the sample configuration, shows that the application status is operational (**OPER**), and the link status is established (**EST**) and active (**ACTV**).



## 9.2. Avaya Aura® Session Manager Verification

Log in to System Manager. Under the **Elements** section, navigate to **Session Manager** → **System Status** → **SIP Entity Monitoring** (not shown). Verify that the state of the Session Manager links under the **Conn. Status** and **Link Status** columns to the CS1000 and the Avaya SBCE is **UP**, like shown on the screen below.

Home / Elements / Session Manager / System Status / SIP Entity Monitoring Help ?

### Session Manager Entity Link Connection Status

This page displays detailed connection status for all entity links from a Session Manager.

All Entity Links for Session Manager: MA\_Session Manager

Status Details for the selected Session Manager:

Summary View

13 Items | Refresh Filter: Enable

	SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	<a href="#">CS1K7.6</a>	172.16.20.60	5087	UDP	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">MA_CM Trunk 2</a>	192.168.10.12	5070	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">MA C.M. Trunk 1</a>	192.168.10.12	5061	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">MA_SBCE</a>	10.5.5.72	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">MA_AA-SBC</a>	192.168.10.42	5060	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">MA C.M.Trunk 10</a>	192.168.10.12	5080	TCP	FALSE	UP	200 OK	UP
<input type="radio"/>	<a href="#">MA CM Trunk 98</a>	192.168.10.12	5062	TLS	FALSE	UP	200 OK	UP

Other Session Manager useful verification and troubleshooting tools include:

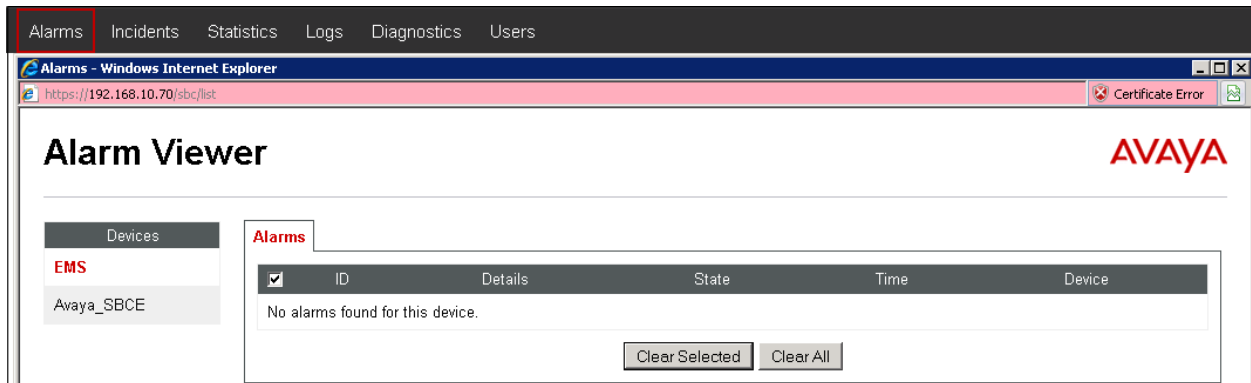
- **traceSM** – Session Manager command line tool for traffic analysis. Login to the Session Manager management interface to run this command.
- **Call Routing Test** - The Call Routing Test verifies the routing for a particular source and destination. To run the routing test, from the System Manager Home screen navigate to **Elements** → **Session Manager** → **System Tools** → **Call Routing Test**. Enter the requested data to run the test



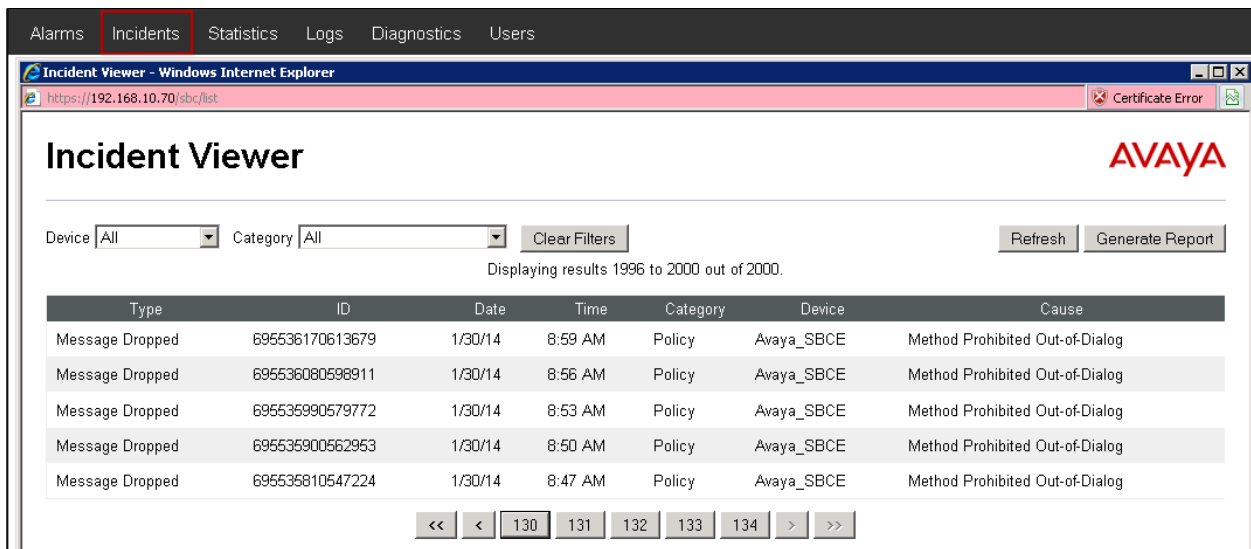
### 9.3. Avaya SBCE Verification

There are several links and menus located on the taskbar at the top of the screen of the web interface that can provide useful diagnostic or troubleshooting information.

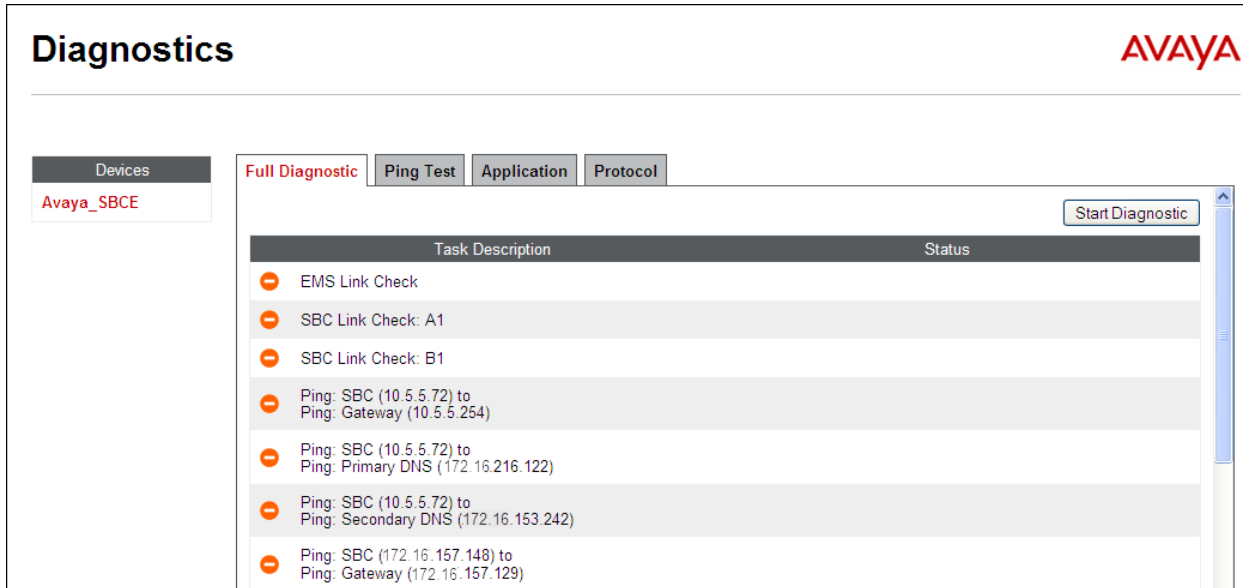
**Alarms:** Provides information about the health of the SBC.



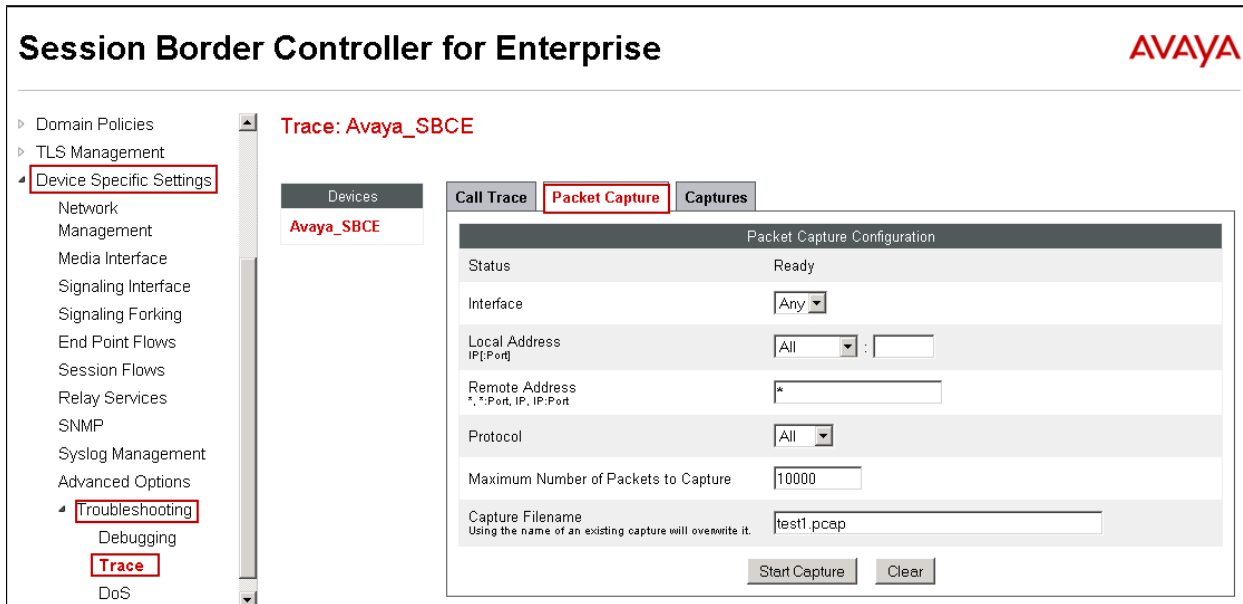
**Incidents :** Provides detailed reports of anomalies, errors, policies violations, etc.



**Diagnostics:** This screen provides a variety of tools to test and troubleshoot the SBC network connectivity.



Additionally, the Avaya SBCE contains an internal packet capture tool that allows the capture of packets on any of its interfaces, saving them as *pcap* files. Navigate to **Device Specific Settings** → **Troubleshooting** → **Trace**. Select the **Packet Capture** tab, set the desired configuration for the trace and click **Start Capture**.



Once the capture is stopped, click the **Captures** tab and select the proper *pcap* file. Note that the date and time is appended to the filename specified previously. The file can now be saved to the local PC, where it can be opened with an application such as Wireshark.

File Name	File Size (bytes)	Last Modified
<a href="#">test1_20140205185331.pcap</a>	118,784	February 5, 2014 6:53:51 PM GMT

## 10. Conclusion

These Application Notes describe the procedures necessary to configure Session Initiation Protocol (SIP) trunking between the Frontier Communications SIP Trunking service and a SIP-enabled enterprise solution consisting of Avaya Communication Server 1000E Release 7.6, Avaya Aura® Session Manager Release 6.3, and Avaya Session Border Controller for Enterprise 6.2.1.

Interoperability testing of the sample configuration was completed with successful results for all test cases with the exception of the observations/limitations described in **Section 2.2**.

## 11. References

This section references the documentation relevant to these Application Notes.

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

- [1] *Network Routing Service Fundamentals, Avaya Communication Server 1000*, Release 7.6, Document Number NN43001-130, Issue 04.04, November 2013.
- [2] *IP Peer Networking Installation and Commissioning, Avaya Communication Server 1000*, Document Number NN43001-313, Issue 06.02, November 2013
- [3] *Communication Server 1000E Overview, Avaya Communication Server 1000*, Release 7.6, Document Number NN43041-110, Issue 06.01, March 2013
- [4] [4] *Unified Communications Management Common Services Fundamentals, Avaya Communication Server 1000*, Release 7.6, Document Number NN43001-116, Issue 06.02, November 2013
- [5] *SIP Line Fundamentals Avaya Communication Server 1000*, Release 7.6, Document Number NN43001-508, Issue 04.01, March 2013
- [6] *Product Compatibility Reference, Avaya Communication Server 1000*, Release 7.6, Document Number NN43001-256, Issue 06.01 Standard, March 2013
- [7] *Configuring FAX over IP in CS 1000: An Overview*, Avaya Product Support Notice – PSN003460u
- [8] *Communication Server 1000 Release 7.6 Service Pack 4 Release Notes*, Issue 1.0, December 2013
- [9] *Implementing Avaya Aura® System Manager on System Platform*, Release 6.3, Issue 3, October 2013
- [10] *Administering Avaya Aura® System Manager*, Release 6.3, Issue 3, October 2013
- [11] *Administering Avaya Aura® Session Manager*, Release 6.3, Issue 3, October 2013
- [12] *Installing Avaya Session Border Controller for Enterprise*, Release 6.2, June 2013
- [13] *Administering Avaya Session Border Controller for Enterprise*, Release 6.2, Issue 2, January 2014
- [14] *Avaya Session Border Controller for Enterprise Release 6.2.1, Release Notes*, Release 6.2 FP1, Issue 5, December 2013
- [15] RFC 3261 SIP: Session Initiation Protocol, <http://www.ietf.org/>
- [16] *Recommendation ITU-T T.38, Procedures for real-time Group 3 facsimile communication over IP networks*. September 2010.

## 12. Appendix A

Signaling Manipulation script created in **Section 7.3.2** of the Avaya SBCE configuration, and included on the Trunk Server profile configuration, **Section 7.3.3**:

```
//Remove Remote-Address header in outbound INVITE and 200 OK
within session "ALL"
{
    act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
    {
        remove(%HEADERS["Remote-Address"][1]);
    }
}

// Remove Organization header from Frontier
within session "ALL"
{
    act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="PRE_ROUTING"
    {
        remove(%HEADERS["Organization"][1]);
    }
}
```

---

**©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](mailto:devconnect@avaya.com).