



Avaya Solution & Interoperability Test Lab

Application Notes for Telenor SIP Trunk Service with Avaya Communication Server 1000 Release 7.6 SP8, Avaya Aura® Session Manager Release 7.0.1 SP1 and Avaya Session Border Controller for Enterprise Release 7.1 SP1 - Issue 1.0

Abstract

These Application Notes illustrate a sample configuration of Avaya Communication Server 1000 Release 7.6 SP8 and Avaya Aura® Session Manager Release 7.0.1 SP1 with SIP Trunks to Avaya Session Border Controller for Enterprise (Avaya SBCE) Release 7.1 SP1 when used to connect Telenor SIP Trunk service.

Telenor SIP Trunk service provides PSTN access via a SIP trunk between the enterprise and Telenor network as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as any observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

Telenor is a member of the Avaya DevConnect Service Provider program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing was conducted via the DevConnect Program at Avaya lab.

Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1	Interoperability Compliance Testing.....	4
2.2	Test Results	5
2.3	Support	6
3.	Reference Configuration	6
4.	Equipment and Software Validated	8
5.	Configure Avaya CS1000	9
5.1	Access to Avaya CS1000 System	9
5.1.1	Access to Avaya CS1000 Element Manager	9
5.1.2	Access Avaya CS1000 Call Server by using CLI.....	10
5.2	Administer IP Telephony Node	11
5.2.1	Obtain Node IP address	11
5.2.2	Administer Terminal Proxy Server (TPS)	13
5.2.3	Administer Voice Codecs	14
5.2.4	Synchronize New Configuration.....	15
5.2.5	Enable Voice Codec on Media Gateways.....	16
5.3	Zones and Bandwidth Management.....	17
5.4	Administer SIP Trunk	18
5.4.1	Integrated Services Digital Network (ISDN).....	18
5.4.2	Administer SIP Trunk Gateway.....	19
5.4.3	Administer Virtual D-Channel.....	22
5.4.4	Administer Virtual Super-Loop	23
5.4.5	Administer Virtual SIP Routes	23
5.4.6	Administer Virtual Trunks.....	27
5.4.7	Administer Calling Line Identification Entries.....	29
5.4.8	Enable External Trunk to Trunk Transfer.....	30
5.5	Administer Dialing Plans	31
5.5.1	Define ESN Access Codes and Parameters (ESN).....	31
5.5.2	Digit Manipulation Block Index (DMI).....	32
5.5.3	Route List Block Index	33
5.5.4	Incoming Digit Translation Configuration	34
5.5.5	Outbound Call – Trunk Steering Code Configuration.....	35
5.6	Enable Plug-ins on CS1000.....	35
5.7	Save the configuration.....	35
6.	Configure Avaya Aura® Session Manager	36
6.1	Configure SIP Domain	37
6.2	Configure Locations	38
6.3	Configure Adaptations	39
6.4	Configure SIP Entities.....	42
6.4.1	Configure Session Manager SIP Entity	42

6.4.2	Configure Avaya CS1000 SIP Entity	43
6.4.3	Configure Avaya SBCE SIP Entity	44
6.5	Configure Entity Links	44
6.5.1	Configure Entity Link to Avaya CS1000.....	45
6.5.2	Configure Entity Link for Avaya SBCE.....	46
6.6	Configure Routing Policies	46
6.6.1	Configure Routing Policy for Avaya CS1000	47
6.6.2	Configure Routing Policy for Avaya SBCE	48
6.7	Configure Dial Patterns.....	49
7.	Configure Avaya Session Border Controller for Enterprise	51
7.1	System Management – Status	53
7.2	Global Profiles.....	53
7.2.1	Uniform Resource Identifier (URI) Groups.....	53
7.2.2	Server Interworking – Session Manager.....	54
7.2.3	Server Interworking – Telenor.....	57
7.2.4	Signaling Manipulation.....	59
7.2.5	Server Configuration – Session Manager	60
7.2.6	Server Configuration – Telenor	62
7.2.7	Routing – To Session Manager.....	64
7.2.8	Routing – To Telenor.....	65
7.2.9	Topology Hiding – Session Manager	66
7.2.10	Topology Hiding – Telenor	66
7.2.11	Domain Policies.....	67
7.2.12	Application Rules.....	67
7.2.13	Border Rules	67
7.2.14	Media Rules	67
7.2.15	Security Rules	67
7.2.16	Signaling Rules	67
7.2.17	Endpoint Policy Groups.....	72
7.2.18	Session Policies.....	74
7.3	Device Specific Settings.....	75
7.3.1	Network Management.....	75
7.3.2	Media Interfaces.....	75
7.3.3	Signaling Interface	76
7.3.4	Endpoint Flows – For Session Manager	77
7.3.5	Endpoint Flows – For Telenor	79
7.3.6	Session Flows.....	80
8.	Verification Steps.....	81
8.1	Avaya Session Border Controller for Enterprise.....	81
8.2	Avaya CS1000.....	83
8.3	Avaya Aura® Session Manager Status	84
8.4	Telephony Services	84
9.	Conclusion	85
10.	Additional References.....	85

1. Introduction

These Application Notes illustrate a sample configuration for Avaya Communication Server 1000 Release 7.6 SP8 (Avaya CS1000) and Avaya Aura® Session Manager Release 7.0.1 SP1 with SIP Trunks to Avaya Session Border Controller for Enterprise (Avaya SBCE) Release 7.1 SP1 when used to connect to the Telenor SIP Trunk service.

Avaya Aura® Session Manager is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya CS1000 is a telephony application server and is the point of connection between the enterprise endpoints and Avaya Aura® Session Manager. Avaya SBCE is the point of connection between Avaya Aura® Session Manager and Telenor SIP Trunk service and is used to not only secure the SIP trunk, but also to make adjustments to VoIP traffic for interoperability.

The SIP Trunk service available from Telenor is the SIP-based Voice over IP (VoIP) service offered to enterprises for a variety of voice communications needs. The Telenor SIP Trunk service allows enterprises to place outbound local and long distance calls, receive inbound Direct Inward Dialing (DID) calls from the PSTN, and place calls between an enterprise's sites.

2. General Test Approach and Test Results

The general test approach was to make calls from/to Avaya CS1000 through Avaya Aura® Session Manager and Avaya SBCE using Telenor SIP Trunk service. The configuration (shown in **Figure 1**) was used to exercise the features and functionality tests listed in **Section 2.1**.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising 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

The interoperability compliance testing focused on verifying inbound and outbound call flows between Avaya CS1000, Avaya Aura® Session Manager, Avaya SBCE, and the Telenor SIP Trunk service.

The compliance testing was based on the Avaya DevConnect CS1000 Generic SIP Trunk test plan and the Telenor-IPT-CPE test plan. The testing covered functionality required for compliance as a solution supported on the Telenor SIP Trunk network. Calls were made to and from the PSTN across the Telenor network. The following standard features were tested as part of this effort:

- Inbound PSTN calls to various phone types including Unistim, SIP, digital and analog telephones at the enterprise. All inbound calls from PSTN are routed to the enterprise across the SIP trunk from the service provider.
- Outbound PSTN calls from various phone types including Unistim, SIP, digital and analog telephones at the enterprise. All outbound calls to PSTN are routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya i2050 softphone.
- Inbound and outbound Avaya CS1000 calls from/to Telenor IP Telephony.
- Dialing plans including local, long distance, international, outbound toll-free calls, etc.
- Calling Party Name presentation and Calling Party Name restriction.
- Codecs G.711A and G.711MU.
- Inbound and outbound fax using T.38.
- DTMF tone transmissions as out-of-band RTP events as per RFC2833.
- Voicemail navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, forward and conference.
- Off-net call forward with History-info.
- Avaya CS1000 MobileX feature.
- Response to incomplete call attempts and trunk errors.

2.2 Test Results

Interoperability testing of Telenor SIP Trunk Service was completed with successful results for all test cases with the exception of the observations/limitations described below.

Please refer to the test case document for a complete list of solution issues found when tested.

- **Faxing** – T.38 Fax is not working on Avaya SBCE 7.1 SP1. Avaya has resolved this issue and the fix will be available on the upcoming Avaya SBCE Service Pack. G.711 pass through mode for Fax works and should be used with Avaya SBCE 7.1 SP1.
- **Off-net Call Transfer** - When a PSTN phone called to an Avaya phone, the phone answered the call and performed a blind transfer or consultative transfer to another PSTN endpoint. The expected behavior was that the Avaya phone should transfer the call successfully. But in this case, the Avaya phone could not complete the transfer. In order to overcome this issue, plug-in 201 and plug-in 501 must be enabled on Avaya CS1000. The CS1000 default configuration will not allow a blind transfer to be executed (incoming SIP Service Provider trunk to outgoing SIP Service Provider trunk) if the SIP Service Provider in question does not support the SIP UPDATE method. With the installation of plugin 501 on the CS1000, the blind transfer will be allowed and the call will be completed. In addition to plug-in 501, it is required that VTRK SU version “cs1000-vtrk-7.65.16.22.-4.i386.000.ntl” or higher be used on all SSG signaling servers to ensure proper operation of the blind transfer feature. The use of plug-in 501 does not restrict the use of the SIP UPDATE method of blind transfer to other parties that do happen to support the UPDATE method, but rather extends support to those parties that

do not. Note that plug-in 501 is independent of and does not require the Global Plugin Package 409.

- **If the Avaya CS1000 phone holds/resumes an outbound call, the dialed digits were no longer displayed** - This is a known limitation on Avaya CS1000.
- **Calling Line Identification Display (CLID) was not correctly displayed** - After call redirection, namely blind/consultative transfers, was completed with 2-way audio, the CLID on the transferee's phone was not updated accordingly. This is a known Avaya CS1000 limitation.
- **Media trombone**: As Telenor requires that PBX/clients must send at least one media-packet before Telenor can send back towards the PBX/client and call phase be preceded, **Media Anchoring** must be disabled on Avaya SBCE for **Media Tromboning Only** call type. Otherwise, the loss of speech path will occur in this type of call. Refer to **Section 7.2.18**.

2.3 Support

- **Avaya**: Avaya customers may obtain documentation and support for Avaya products by visiting <http://support.avaya.com>.
- **Telenor**: Customers should contact their Telenor Business representative or follow the support links available on <https://www.telenor.com/>.

3. Reference Configuration

The reference configuration used in these Application Notes is shown in the diagram below and consists of several components.

- Avaya Aura® Session Manager running on VMware ESXi 5.5.
- Avaya Aura® System Manager running on VMware ESXi 5.5.
- Avaya CS1000 CPPM co-resident.
- Avaya CallPilot 201i.
- Avaya IP phones are represented with Avaya 1100 Series IP Telephones running Unistim/SIP software.
- Avaya 3904 digital phone.
- Avaya i2050 softphone.
- The Avaya SBCE provided Session Border Controller functionality, including, SIP header manipulation, and Topology Hiding between the Telenor SIP Trunk service and the enterprise network.
- Telenor SIP Trunk service provided one trunk group for SIP trunks. DID range assigned by Telenor for this testing is +4722391xxx (10 digits). Telenor requires all numbering format for outbound call to be E.164 with Country Code included.

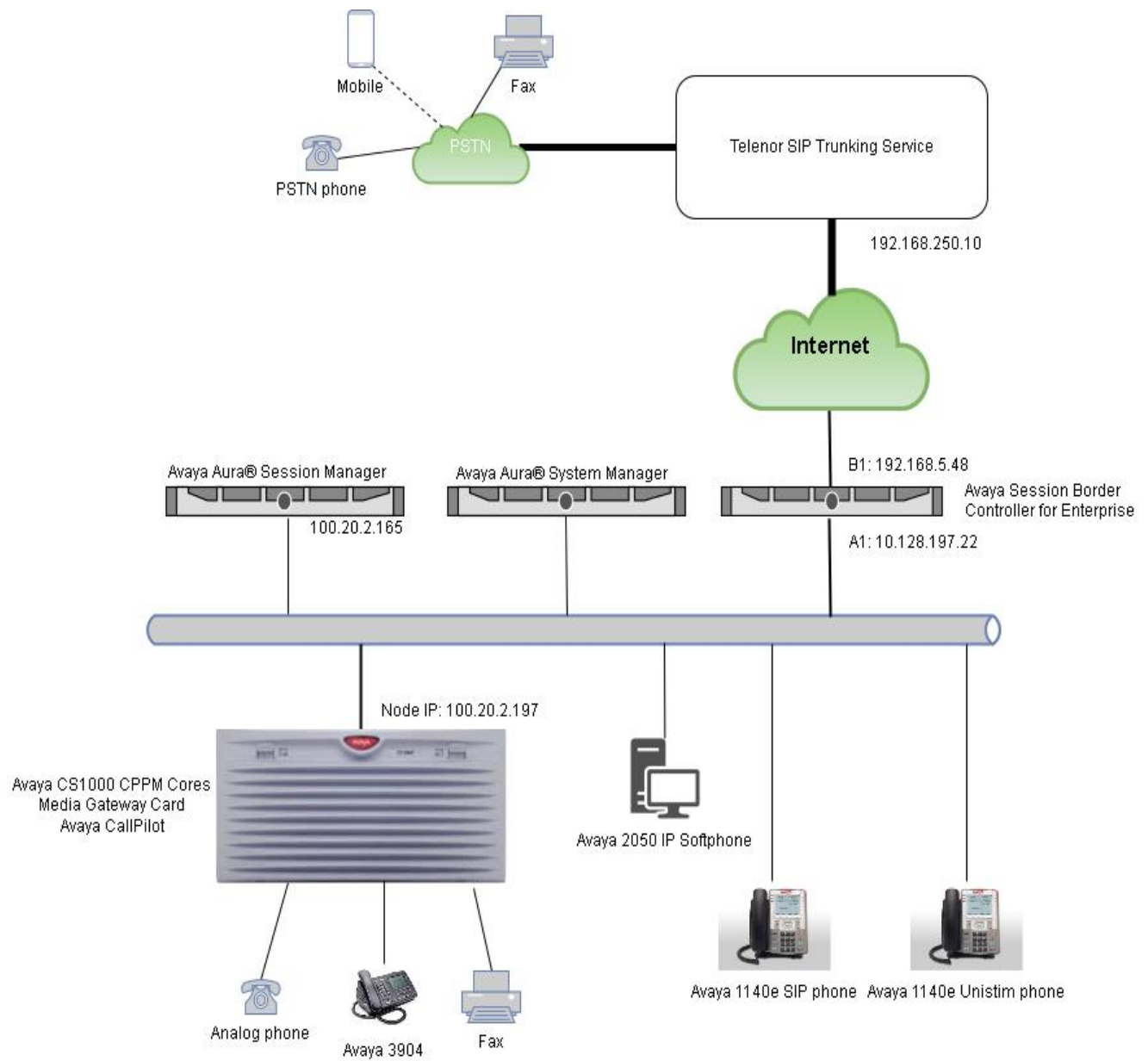


Figure 1: Network Components as Tested

4. Equipment and Software Validated

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

Component	Version
Avaya	
Avaya Aura® System Manager 7.0.1 SP1	7.0.1.1.065378
Avaya Aura® Session Manager 7.0.1 SP1	7.0.1.1.701114
Avaya Session Border Controller for Enterprise 7.1 SP1	7.1.0.1-07-12368
Avaya Communication Server 1000 7.6 SP8	Call Server 7.65 Service Pack 8 Signaling Server 7.65 Service Pack 8
Avaya CallPilot	5.1 SU4
Avaya 1100 Series Unistim phone	5.5.6
Avaya 1100 Series SIP phone	4.4.5
Avaya 3904 Digital phone	9.3
Avaya 2050 Softphone	4.4.6
Analog phone	N/A
Service Provider	
Telenor	IPT 11.0.181

Table 1: Software version

5. Configure Avaya CS1000

The configuration of the Avaya CS1000 outlined in these Application Notes uses the Incoming Digit Translation feature to receive calls, and the Trunk Steering Code (TSC) feature to route calls from the Avaya CS1000 to the PSTN via SIP trunks to the Telenor SIP Trunk service.

These Application Notes assume that the basic Avaya CS1000 configuration has already been administered. For further information on Avaya CS1000, please consult the references in **Section 10**. The procedures below describe the configuration details for configuring the Avaya CS1000.

5.1 Access to Avaya CS1000 System

Changes to Avaya CS1000 can be made using Element Manager, which is accessible from Unified Communications Management (UCM) and offers the user a Web GUI for making changes. Changes to Avaya CS1000 can also be made using the Command Line Interface (CLI) offered using PuTTY to make a SSH connection.

5.1.1 Access to Avaya CS1000 Element Manager

Open an instance of a web browser and connect to UCM using the following address: <https://<UCM IP address>/network-login/>. Log in using an appropriate User ID and Password (not shown). The UCM screen is displayed.

AVAYA Avaya Unified Communications Management

Host Name: 100.20.2.196 Software Version: 02.30.0099.00(6718) 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.

Search Reset

Element Name	Element Type	Release	Address	Description
1 <input type="checkbox"/> EM on cs1k	CS1000	7.6	100.20.2.136	New element
2 <input type="checkbox"/> cs1k.sipinterop.com (primary)	Linux Base	7.6	100.20.2.196	Base OS element
3 <input type="checkbox"/> CaliPilot	Non CS1000 Manual Device	7.6	100.20.2.137	
4 <input type="checkbox"/> 100.20.2.135	Media Gateway Controller	7.6	100.20.2.135	New element

Click on the **Element Name** of the Avaya CS1000 Element: “**EM on cs1k**”. The Avaya CS1000 Element Manager **System Overview** page is displayed as shown below:

AVAYA CS1000 Element Manager

Managing: 100.20.2.136 Username: admin

System Overview

IP Address: 100.20.2.136
Type: Avaya Communication Server 1000E CPPM Linux
Version: 4121
Release: 765 P +

5.1.2 Access Avaya CS1000 Call Server by using CLI

Using Putty to open a SSH session to the IP address of Avaya CS1000 Signaling Server then log in with administrator credentials. Run the command **cslogin** and log in with the appropriate user account and password. Sample output is shown below.

```
login as: admin
```

```
Avaya Inc. Linux Base 7.65
```

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

```
admin@100.20.2.196's password:
```

```
Last login: Tue Sep 20 16:57:20 2016 from 100.20.2.189
```

```
[admin@cs1k ~]$
```

```
[admin@cs1k ~]$
```

```
[admin@cs1k ~]$
```

```
[admin@cs1k ~]$ cslogin
```

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

```
TTY 07 SCH MTC BUG OSN 10:46
```

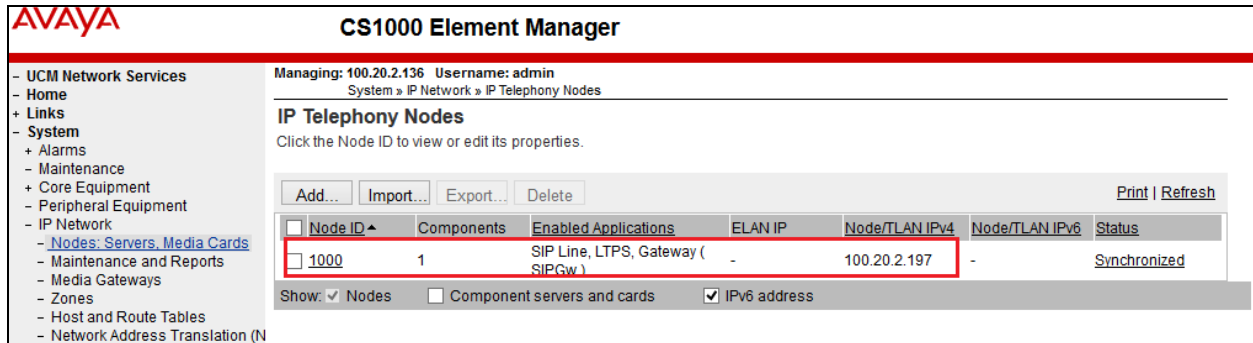
```
OVL111 IDLE 0
```

```
>
```

5.2 Administer IP Telephony Node

5.2.1 Obtain Node IP address

These Application Notes assume that the basic Avaya CS1000 configuration has already been administered and that a Node has already been created. This section describes the steps for configuring a Node (**Node ID 1000**) in Avaya CS1000 IP network to work with Telenor SIP Trunk service. Access Element Manager as per **Section 5.1.1**. Select **System > IP Network > Nodes: Servers, Media Cards** and then click on the **Node ID** as shown below:



AVAYA CS1000 Element Manager

Managing: 100.20.2.136 Username: admin
System » IP Network » IP Telephony Nodes

IP Telephony Nodes

Click the Node ID to view or edit its properties.

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

<input type="checkbox"/> Node ID	Components	Enabled Applications	ELAN IP	Node/TLAN IPv4	Node/TLAN IPv6	Status
<input type="checkbox"/> 1000	1	SIP Line, LTPS, Gateway (SIPGw)	-	100.20.2.197	-	Synchronized

Show: ☒ Nodes ☐ Component servers and cards ☒ IPv6 address

The **Node Details** screen is displayed with the IP address of the Avaya CS1000 node: **Call server IP address: 100.20.2.136**. The **Node IPv4 address 100.20.2.197** for **Telephony LAN (TLAN)** is a virtual address which corresponds to the **TLAN IPv4 address 100.20.2.196** of the Signaling Server/SIP Signaling Gateway. The SIP Signaling Gateway uses this Node IP address to communicate with other components to process SIP calls.

AVAYA

CS1000 Element Manager

Managing: 100.20.2.136 Username: admin
System » IP Network » IP Telephony Nodes » Node Details

Node Details (ID: 1000 - SIP Line, LTPS, Gateway (SIPGw))

Node ID: 1000 * (0-9999)

Call server IP address: 100.20.2.136 *

TLAN address type: ☒ IPv4 only
☐ IPv4 and IPv6

Embedded LAN (ELAN)

Gateway IP address: 100.20.2.129 *

Telephony LAN (TLAN)

Node IPv4 address: 100.20.2.197 *

Subnet mask: 255.255.255.224 *

Subnet mask: 255.255.255.224 *

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

Associated Signaling Servers & Cards

Select to add Add Remove Make Leader Print Refresh

Hostname	Type	Deployed Applications	ELAN IP	TLAN IPv4	Role
cs1k	Signaling_Server	SIP Line, LTPS, Gateway (SIP/H323), PD, Presence Publisher, IP Media Services	100.20.2.136	100.20.2.196	Leader

Show: IPv6 address

5.2.2 Administer Terminal Proxy Server (TPS)

Continuing from **Section 5.2.1**, on the **Node Details** page, select the **Terminal Proxy Server (TPS)** link then check the **UNISlim Line Terminal Proxy Server** box to enable proxy service on this node and click on **Save** button:

AVAYA **CS1000 Element Manager**

Managing: 100.20.2.136 Username: admin
System » IP Network » IP Telephony Nodes » Node Details » UNISlim Line Terminal Proxy Server (LTPS) Configuration

Node ID: 1000 - 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: admin
Password:

DTLS

DTLS policy: Off

Options: ☐ Client authentication
☐ Periodic re-keying

Network Connect Server

Primary network connect server (T1 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 Voice Codecs

On the **Node Details** page shown in **Section 5.2.1**, click on **Voice Gateway (VGW) and Codecs**. Make sure FAX and only G.711 are configured as shown below then click on **Save** button:

AVAYA CS1000 Element Manager

Managing: 100.20.2.136 Username: admin
System » IP Network » IP Telephony Nodes » Node Details » VGW and Codecs

Node ID: 1000 - Voice Gateway (VGW) and Codecs

General | Voice Codescs | 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 Codescs

Codec G711: ☒ Enabled (required)
Voice payload size: 20 (milliseconds per frame)
Voice playout (jitter buffer) delay: 40 80 (milliseconds)
Nominal Maximum

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

AVAYA CS1000 Element Manager

Managing: 100.20.2.136 Username: admin
System » IP Network » IP Telephony Nodes » Node Details » VGW and Codecs

Node ID: 1000 - Voice Gateway (VGW) and Codecs

General | Voice Codescs | Fax

General

Codec G723.1: ☐ Enabled
Voice payload size: 30 (milliseconds per frame)
Voice playout (jitter buffer) delay: 60 120 (milliseconds)
Nominal Maximum
Maximum delay may be automatically adjusted based on nominal settings.
Coding rate: 5.3 (kbps)

Fax

Codec name: T.38 FAX
Maximum rate: 14400 (bps)
Fax TCF method: 2
Fax playout nominal delay: 100 (0 - 300 milliseconds)
FAX no activity timeout: 20 (10 - 32000 milliseconds)
Packet size: 30 (bps)

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

5.2.4 Synchronize New Configuration

On **Node Details** page shown in **Section 5.2.1**, click on **Save** button. The **Node Saved** screen is displayed. Click on **Transfer Now** (not shown).

The **Synchronize Configuration Files (Node ID <1000>)** screen is displayed (not shown). Check the **cs1k** box and click on **Start Sync**. When the synchronization completes, check the **cs1k** box and click on the **Restart Applications** (not shown).

5.2.5 Enable Voice Codec on Media Gateways

From the left menu of the **Element Manager** page, navigate to **System > IP Network > Media Gateways**. The Media Gateways page will appear (not shown). Click on the **MGC** which is located on the right of the page. In the following screen, uncheck **Enable modem/fax pass through mode** box then scroll down to make sure only Codec **G.711** and **T38 FAX** are selected. Scroll down to the bottom of the page and click on the **Save** button (not shown).

AVAYA

CS1000 Element Manager

- UCM Network Services
 - Home
 - Links
 - Virtual Terminals
 - System
 - + Alarms
 - Maintenance
 - + Core Equipment
 - Peripheral Equipment
 - IP Network
 - Nodes: Servers, Media Cards
 - Maintenance and Reports
 - Media Gateways
 - Zones
 - Host and Route Tables
 - Network Address Translation (N
 - QoS Thresholds
 - Personal Directories
 - Unicode Name Directory
 - + Interfaces
 - Engineered Values
 - + Emergency Services
 - + Geographic Redundancy
 - + Software
 - Customers
 - Routes and Trunks
 - Routes and Trunks
 - D-Channels
 - Digital Trunk Interface
 - Dialing and Numbering Plans
 - Electronic Switched Network
 - Flexible Code Restriction
 - Incoming Digit Translation
 - Phones
 - Templates
 - Reports
 - Views
 - Lists
 - Properties
 - Migration
 - Tools
 - + Backup and Restore
 - Date and Time
 - + Logs and reports
 - Security
 - + Passwords
 - + Policies
 - + Login Options

Managing: **100.20.2.136** Username: admin
System » IP Network » Media Gateways » IPMG 4 0 Media Gateway Controller (MGC) Configuration

IPMG 4 0 Media Gateway Controller (MGC) Configuration

+ Media Gateway Controller

+ DSP Daughterboard 1

+ DSP Daughterboard 2

- VGW and IP phone codec profile

Enable echo canceller ☒

Echo canceller tail delay (milliseconds)

Enable dynamic attenuation ☒

Voice activity detection threshold (0 - 4 DBM)

Idle noise level (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

FAX maximum rate (bps)

FAX playout nominal delay (0 - 300 milliseconds)

FAX no activity timeout (10 - 32000 milliseconds)

FAX packet size

+ Codec G711 ☒

+ Codec G729A ☐

+ Codec G723.1 ☐

+ Codec T38 FAX ☒

+ QoS

+ Media Based CLID

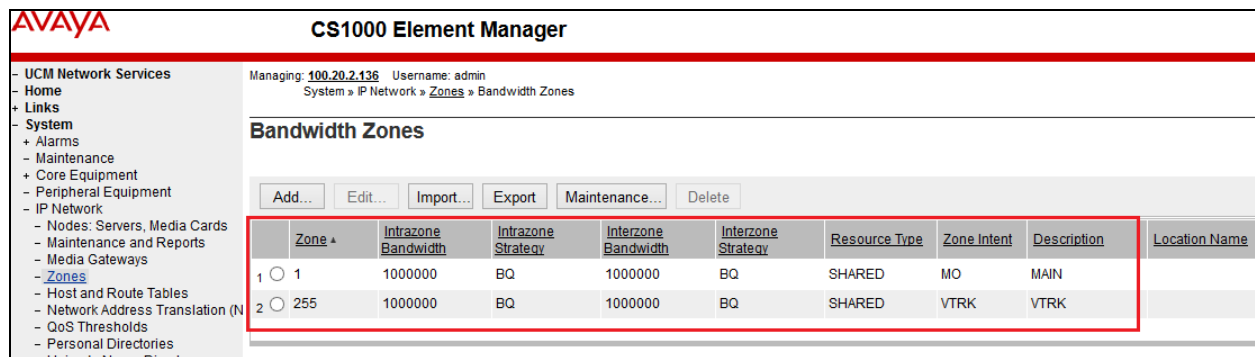
5.3 Zones and Bandwidth Management

Navigate to **System > IP Network > Zones** from the left pane (not shown), click on **Bandwidth Zones** (not shown). Click on **Add** to create new zones for IP Phones and Virtual Trunk.

Input these values for **Zone 1** which is used for IP Phones and Voice Gateway:

- **Intrazone Bandwidth (INTRA_BW): 1000000.**
- **Intrazone Strategy (INTRA_STGY):** Set codec for local calls. Select **Best Bandwidth (BB)** to use **G.729** as the first priority codec for negotiation or select **Best Quality (BQ)** to use **G.711** as the first priority codec for negotiation. In this example, **BQ** was chosen.
- **Interzone Bandwidth (INTER_BW): 1000000.**
- **Interzone Strategy (INTER_STGY):** Set codec for the calls over trunk. Select **Best Bandwidth (BB)** to use **G.729** as the first priority codec for negotiation or select **Best Quality (BQ)** to use **G.711** as the first priority codec for negotiation. In this example, **BQ** was chosen.
- **Zone Intent (ZBRN):** Select **MO** for IP phones, and Voice Gateway.

Use the same above values for **Zone 255** which is used for virtual trunk except for **Zone Intent (ZBRN)** field. Select **VTRK** for this field.



AVAYA CS1000 Element Manager

Managing: 100.20.2.136 Username: admin
System > IP Network > Zones > Bandwidth Zones

Bandwidth Zones

Add... Edit... Import... Export Maintenance... Delete

Zone	Intrazone Bandwidth	Intrazone Strategy	Interzone Bandwidth	Interzone Strategy	Resource Type	Zone Intent	Description	Location Name
1	1000000	BQ	1000000	BQ	SHARED	MO	MAIN	
255	1000000	BQ	1000000	BQ	SHARED	VTRK	VTRK	

5.4 Administer SIP Trunk

This section describes the steps for establishing a SIP connection between the SIP Signaling Gateway and Avaya Aura® Session Manager (Session Manager).

5.4.1 Integrated Services Digital Network (ISDN)

Select **Customers** in the left pane. The **Customers** screen is displayed. Click on the link associated with the appropriate customer, in this case **00**.

AVAYA CS1000 Element Manager

Managing: 100.20.2.136 Username: admin
Customers

Customers

Add... Delete

Customer Number	Total Routes	Total Trunks
1 00	2	20

The **Customer Details** page will appear. Select the **Feature Packages** option from **Customer Details** page (not shown).

The screen is updated with a list of available **Feature Packages**. Select **Integrated Services Digital Network** to edit the parameters shown below. Check the **Integrated Services Digital Network** option, enter **1** into **Virtual private network identifier** and **Private network identifier**, then click on the **Save** button (not shown).

AVAYA CS1000 Element Manager

Managing: 100.20.2.136 Username: admin
Customers

Feature Packages

- + Flexible Tones and Cadences Package: 125
- + Multifrequency Compelled Signaling Package: 128
- + International Supplementary Features Package: 131
- + Enhanced Night Service Package: 133
- Integrated Services Digital Network Package: 145
- + Dial Access Prefix on CLID table entry option

Integrated Services Digital Network: ☒

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

- Private network identifier: 1 (1 - 16383)

- Node DN: 1000

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

5.4.2 Administer SIP Trunk Gateway

Navigate to **System > IP Network > Nodes: Servers, Media Cards** from the left pane. In the **IP Telephony Nodes** screen displayed (not shown), select the **Node ID** of the CS1000 system. The **Node Details** screen is displayed as shown in **Section 5.2.1**.

On the **Node Details** screen, select **Enable gateway service on this node** for the **Vtrk gateway application** field. Under the **General** tab of the **Virtual Trunk Gateway Configuration Details** screen, enter the following values (highlighted in red boxes) for the specified fields, and retain the default values for the remaining fields as shown below. The **SIP domain name** and **Local SIP port** should be matched with the configuration of Session Manager in **Section 6.2**, and **6.5**.

AVAYA CS1000 Element Manager

Managing: 100.20.2.136 Username: admin
System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration

Node ID: 1000 - 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: sipinterop.com *
Local SIP port: 5060 * (1 - 65535)
Gateway endpoint name: cs1k *
Gateway password: *
Application node ID: 1000 * (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

SIP ANAT: ☒ IPv4

Click on the **SIP Gateway Settings** tab. Under **Proxy or Redirect Server**, enter the following values (highlighted in red boxes) for the specified fields and retain the default values for the remaining fields, as shown below. Enter the IP address of Session Manager in the **Primary TLAN IP address** field. Enter **5060** for **Port** and select **TCP** for **Transport protocol**. This should be matched with the configuration of Avaya Aura® Session Manager (see in **Section 6.5.1**). Uncheck the **Support registration** checkbox.

AVAYA CS1000 Element Manager

Managing: 100.20.2.136 Username: admin
System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration

Node ID: 1000 - Virtual Trunk Gateway Configuration Details

General | **SIP Gateway Settings** | SIP Gateway Services

☐ Enable Shared Bandwidth Management

Proxy Or Redirect Server:

Proxy Server Route 1:

Primary TLAN IP address: 100.20.2.165
The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"

Port: 5060 (1 - 65535)

Transport protocol: TCP

Options: ☐ Support registration
☐ Primary CDS proxy

Secondary TLAN IP address: 0.0.0.0
The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"

Port: 5060 (1 - 65535)

Transport protocol: TCP

Options: ☐ Support registration

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

AVAYA CS1000 Element Manager

Managing: 100.20.2.136 Username: admin
System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration

Node ID: 1000 - Virtual Trunk Gateway Configuration Details

General | **SIP Gateway Settings** | SIP Gateway Services

☐ Tertiary CDS proxy

Proxy Server Route 2:

Primary TLAN IP address: 100.20.2.165
The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"

Port: 5060 (1 - 65535)

Transport protocol: TCP

Options: ☒ Registration not supported
☐ Primary CDS proxy

CLID Presentation:

Country code (CCC):
Area code: NPA in North America

Number translation: Strip: Prefix: CLID display format:
Subscriber (SN): 0 <CCC> <Area code> <SN>

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

Scroll down to the **SIP URI Map** section. Under **Public E.164 domain names**, leave blank for: **National, Subscriber, Special Number, Unknown**.

Under **Private domain names**, leave blank for: **UDP, CDP, Special Number, Vacant number, Unknown**.

The screenshot displays the AVAYA CS1000 Element Manager web interface. The left sidebar contains a navigation tree with categories like UCM Network Services, System, Interfaces, Customers, Routes and Trunks, and Dialing and Numbering Plans. The main content area is titled 'Node ID: 1000 - Virtual Trunk Gateway Configuration Details' and includes tabs for General, SIP Gateway Settings, and SIP Gateway Services. The 'SIP URI Map' section is highlighted with a red rectangle and is divided into two columns: 'Public E.164 domain names' and 'Private domain names'. Each column contains five input fields for National, Subscriber, Special number, and Unknown, with an additional field for UDP in the Private column. Below this, the 'SIP Gateway Services' section includes a checkbox for 'SIP Converged Desktop', a 'Service DN' field, and several other configuration fields with their respective units and descriptions. At the bottom, there are 'Save' and 'Cancel' buttons, along with a note about saving changes.

Managing: 100.20.2.136 Username: admin
System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration

Node ID: 1000 - Virtual Trunk Gateway Configuration Details

General | SIP Gateway Settings | SIP Gateway Services

SIP URI Map:

Public E.164 domain names		Private domain names	
National:	<input type="text"/>	UDP:	<input type="text"/>
Subscriber:	<input type="text"/>	CDP:	<input type="text"/>
Special number:	<input type="text"/>	Special number:	<input type="text"/>
Unknown:	<input type="text"/>	Vacant number:	<input type="text"/>
		Unknown:	<input type="text"/>

SIP Gateway Services

SIP Converged Desktop: ☐ Enable CD service

Service DN: Used for making VTRK call from agent.

Converged telephone call forward DN:

RAN route for announce: (route number 0 - 511)

Wait time before RAN queue: (-1 - 32767 msec)

Timeout for ringing indication: (5 - 60 seconds)

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

Synchronize the new configuration (please refer to **Section 5.2.4**).

5.4.3 Administer Virtual D-Channel

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

The **D-Channels 10 Property Configuration** screen is displayed next, as shown below. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **D-channel Card Type: D-Channel is over IP (DCIP).**
- **Designator: A descriptive name.**
- **User: Integrated Services Signaling Link Dedicated (ISLD).**
- **Interface type for D-channel: Meridian Meridian1 (SL1).**
- **Meridian 1 node type: Slave to the controller (USR).**
- **Release ID of the switch at the far end: 25.**

AVAYA CS1000 Element Manager

Managing: 100.20.2.136 Username: admin
Routes and Trunks » D-Channels » D-Channels 10 Property Configuration

D-Channels 10 Property Configuration

- Basic Configuration

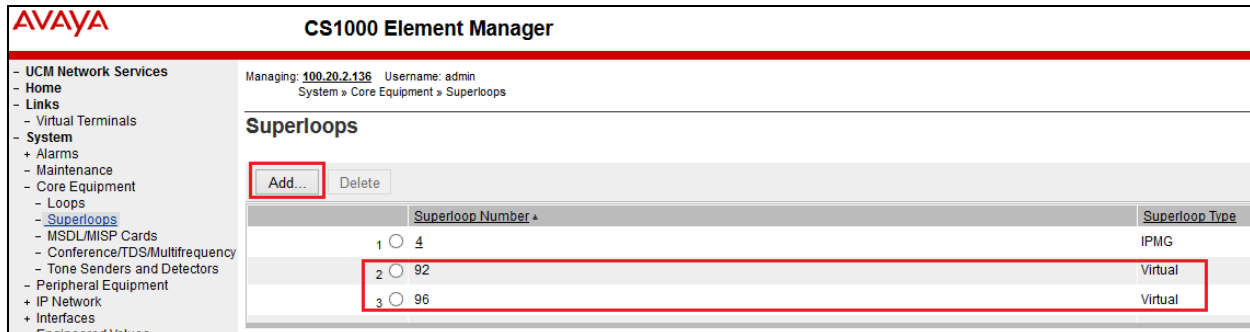
Input Description	Input Value
Action Device And Number (ADAN):	DCH
D channel Card Type :	DCIP
Designator:	vtrk
Recovery to Primary:	<input type="checkbox"/>
PRI loop number for Backup D-channel:	
User :	Integrated Services Signaling Link Dedicated (ISLD) ▼ *
Interface type for D-channel:	Meridian Meridian1 (SL1) ▼
Country:	ETS 300 =102 basic protocol (ETSI) ▼
D-Channel PRI loop number:	
Primary Rate Interface:	<input type="text"/> more PRI
Secondary PRI2 loops:	<input type="text"/>
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

+ Basic options (BSCOPT)
+ Advanced options (ADVOPT)
+ Feature Packages

Submit Refresh Delete Cancel

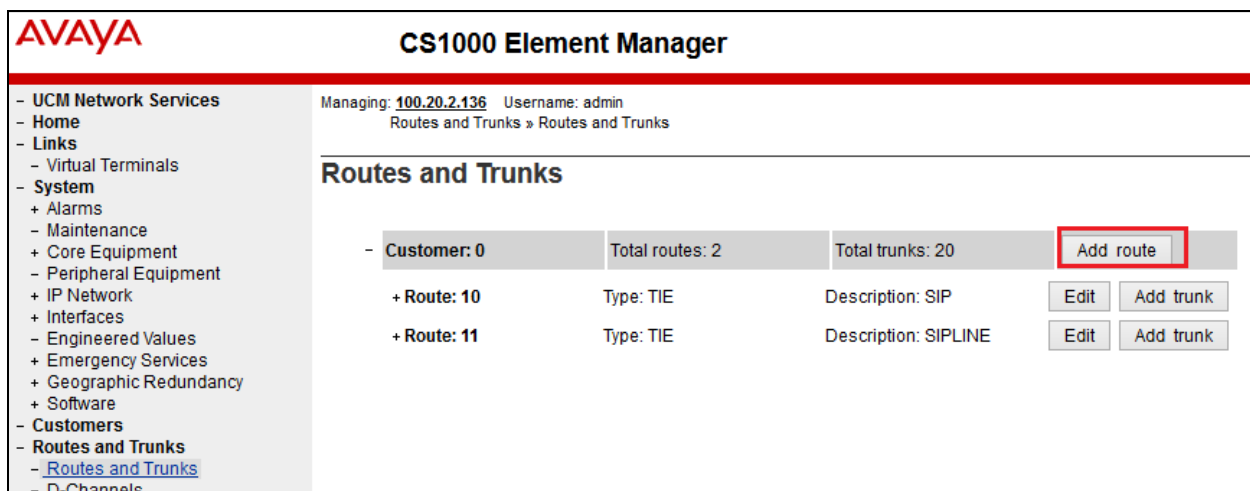
5.4.4 Administer Virtual Super-Loop

Navigate to **System > Core Equipment > Superloops** from the left pane to display the **Superloops** screen. If the Superloop does not exist, click the **Add** button to create a new one as shown below. In this example, **Virtual Superloops 92, 96** have been added and were being used.



5.4.5 Administer Virtual SIP Routes

Navigate to **Routes and Trunks > Routes and Trunks** (not shown) from the left pane to display the **Routes and Trunks** screen. In this example, **Customer 0** was being used. Click on the **Add route** button as shown below.



The **Customer 0, New Route Configuration** screen is displayed next (not shown). The **Basic Configuration** section is displayed. Enter the following values for the specific fields, and retain the default values for the remaining fields. The screenshot of **Basic Configuration** section of existing **route 10** is displayed to edit as shown below.

- **Route data block (RDB) (TYPE):** RDB as default.
- **Customer number (CUST):** 0 as customer 0 is used.
- **Route number (ROUT):** Enter an available route number (example: route 10).
- **Designator field for trunk (DES):** A descriptive text (SIP).
- **Trunk type (TKTP):** TIE trunk data block (TIE).
- **Incoming and outgoing trunk (ICOG):** Incoming and Outgoing (IAO).

- **Access code for the trunk route (ACOD):** An available access code (example: **8753**)
- Check **The route is for a virtual trunk route (VTRK)** field, to enable four additional fields to appear.
- For **Zone for codec selection and bandwidth management (ZONE)** field, enter **255** (created in **Section 5.3**). Note: the Zone value is filled out as 255, but after it is added, the screen is displayed with prefix 00.
- For **Node ID of signaling server of this route (NODE)** field, enter the node number 1000 (created in **Section 5.2.1**).
- Select **SIP (SIP)** from the drop-down list for **Protocol ID for the route (PCID)** field.
- Check **Integrated Services Digital Network option (ISDN)** box to enable additional fields to appear. Scrolling down to the bottom of the screen, enter the following values for the specified fields, and retain the default values for the remaining fields.
 - **Mode of operation (MODE):** Select **Route uses ISDN Signalling Link (ISLD)**.
 - **D channel number (DCH):** Enter **10** (created in **Section 5.4.3**).
 - **Interface type for route (IFC):** Select **Meridian M1 (SL1)**.
 - **Private network identifier (PNI):** Enter **1**. Note: the value is filled out as 1, but after it is added, the screen is displayed with prefix 0000.
 - **Network calling name allowed (NCNA):** Check this option to allow calling name display.
 - **Network call redirection (NCRD):** Check this option to allow call redirection.
 - **Call type for outgoing direct dialed TIE route (CTYP):** select **Unknown Call type (UKWN)**.
 - **Insert ESN access code (INAC):** Check this option to insert ESN access code.
- Click on **Basic Route Options**, check **Incoming DID digit conversion on this route (IDC)** boxes. Enter **0** for both **Day IDC tree number** and **Night IDC tree number**.

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

Customer 0, Route 10 Property Configuration

- Basic Configuration

Route data block (RDB) (TYPE):	RDB
Customer number (CUST):	00
Route number (ROUT):	10
Designator field for trunk (DES):	SIP
Trunk type (TKTP):	TIE
Incoming and outgoing trunk (ICOG):	Incoming and Outgoing (IAO) ▼
Access code for the trunk route (ACOD):	8753

Trunk type M911P (M911P):	
The route is for a virtual trunk route (VTRK):	<input checked="" type="checkbox"/>
- Zone for codec selection and bandwidth management (ZONE):	00255 (0 - 8000)
- Node ID of signaling server of this route (NODE):	1000 (0 - 9999)
- Protocol ID for the route (PCID):	SIP (SIP) ▼

- Print correlation ID in CDR for the route (CRID): ☐
- Enable Shared Bandwidth Management for the route (SBWM): ☐

Integrated services digital network option (ISDN):	<input checked="" type="checkbox"/>
- Mode of operation (MODE):	Route uses ISDN Signaling Link (ISLD) ▼
- D channel number (DCH):	10 (0 - 254)
- Interface type for route (IFC):	Meridian M1 (SL1) ▼
- Private network identifier (PNI):	00001 (0 - 32700)
- Network calling name allowed (NCNA):	<input checked="" type="checkbox"/>
- Network call redirection (NCRD):	<input checked="" type="checkbox"/>

- 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):	<input checked="" type="checkbox"/>

- Integrated service access route (ISAR): ☐
- Display of access prefix on CLID (DAPC): ☐

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

Managing: **100.20.2.136** Username: admin
 Routes and Trunks » [Routes and Trunks](#) » Customer 0, Route 10 Property Configuration

Customer 0, Route 10 Property Configuration

+ Basic Configuration

- Basic Route Options

Attendant announcement (ATAN) :

Billing number required (BILN) : ☐

Call detail recording (CDR) : ☐

North American toll scheme (NATL) : ☒

Controls or timers (CNTL) : ☐

Conventional (Tie trunk only) (CNVT) : ☐

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

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

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

- Display external dialed digits (DEXT) : ☐

Multifrequency compelled or MFC signaling (MFC) :

Process notification networked calls (PNNC) : ☐

+ Network Options

+ General Options

+ Advanced Configurations

5.4.6 Administer Virtual Trunks

Navigate to **Routes and Trunks > Route and Trunks** (not shown). The Route list is now updated with the newly added routes in **Section 5.4.5**. In the example, **Route 10** was added. Click on the **Add** trunk button (not shown).

The **Customer 0, Route 10, Trunk type TIE trunk data block** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields. Media Security (sRTP) needs to be disabled at the trunk level by editing the **Class of Service (CLS)** at the bottom of the **Basic Configuration** page. Click on the **Edit** button as shown below.

In the sample configuration, 10 trunks were created.

- **Multiple trunk input number:** Enter the number of channels (in this example, there are 10 channels).
- Select **Auto increment member number**.
- **Trunk data block:** **TIE trunk data block (TIE)**.
- **Terminal Number:** Available terminal number (**Superloop 92** created in **Section 5.4.4**).
- **Designator field for trunk:** A descriptive text (**sip**).
- **Member number:** Current route number and starting member.
- **Start arrangement Incoming:** Select **Immediate (IMM)**.
- **Start arrangement Outgoing:** Select **Immediate (IMM)**.
- **Channel ID for this trunk:** An available starting channel ID.

For **Media Security**, select **Media Security Never (MSNV)**. Enter the values for the specified fields as shown below. Scroll down to the bottom of the screen and click **Return Class of Service** and then click on the **Save** button (not shown).

- Class of Service	
Input Description	Input Value
- ACD Priority :	<input type="text"/>
- Analog Semi-Permanent Connections :	<input type="text"/>
- ARF Supervised COT:	<input type="text"/>
- Barring:	<input type="text"/>
- Battery Supervised COT :	<input type="text"/>
- Busy Tone Supervised COT:	<input type="text"/>
- Calling Line Identification:	<input type="text"/>
- Calling party:	<input type="text"/>
- Central Office Ringback:	<input type="text"/>
- Centrex Switchhook Flash:	<input type="text"/>
- Dial Pulse:	<input type="text"/>
- DTR PAD value:	<input type="text"/>
- Echo Canceling:	<input type="text"/>
- Hong Kong DTI :	<input type="text"/>
- Loop Break Supervised COT:	<input type="text"/>
- Make-break ratio for dial pulse:	<input type="text"/>
- Manual Incoming:	<input type="text"/>
-Media Security:	Media Security Never (MSNV)
-Network Hook Flash Over M911P:	<input type="text"/>
- Polarity:	<input type="text"/>
- Priority:	<input type="text"/>
- Restriction level:	<input type="text"/>
- Reversed Ear Piece:	<input type="text"/>
- Short or long line:	<input type="text"/>
- Transmission Class of Service:	<input type="text"/>
- Warning Tone:	<input type="text"/>
- Reversed Ear Piece:	<input type="text"/>
- ARF Supervised COT:	<input type="text"/>

5.4.7 Administer Calling Line Identification Entries

Navigate to **Customers** on the left pane, and then select **00 > ISDN and ESN Networking** (not shown). Click on **Calling Line Identification Entries**:

Integrated services digital network: ☒

Microsoft converged office dialing plan: Private dialing plan

Private dialing plan for non-DID users: ☐ Coordinated dialing plan ☐ Uniform dialing plan

Extended Local Calls: ☐

Extended Local Calls Route list index: (0 - 1999)

Information for incoming/outgoing calls: No manipulation is done

Size: 256 (0 - 4000)

Country code: 0 (0 - 9999)

Code displayed as part of calling number

Calling Line Identification Entries

Click on **Add**. The add **entry 0** screen will display. Enter or select the following values for the specified fields and retain the default values for the remaining fields.

- **National Code:** Enter **004722**.
- **Local Code:** Enter **39**.
- **Home Location Code:** Leave blank
- **Local Steering Code:** Leave blank.
- **Use DN as DID:** YES.

Managing: 100.20.2.136 Username: admin

Customers > Customer 00 > Customer Details > ISDN and ESN Networking > Calling Line Identification Entries

Calling Line Identification Entries

Search for CLID

Start range:

End range:

'End range' should not exceed the CLID size specified

Search

Calling Line Identification Entries

Add... Delete

<input type="checkbox"/>	Entry id	National Code	Local Code	Home location code	Local steering code	Use DN as DID
1	<input type="checkbox"/> 0	004722	39			YES

5.4.8 Enable External Trunk to Trunk Transfer

External Trunk to Trunk Transfer feature is a mandatory configuration to make call transfer and conference work properly over a SIP trunk.

Access the Call Server Overlay CLI (please refer to **Section 5.1.2** for more details). Allow External Trunk to Trunk Transfer for **Customer Data Block** by using **ld 15**.

```
>ld 15
CDB000
MEM AVAIL: (U/P): 33600126 USED U P: 8345621 954062 TOT: 45579868
DISK SPACE NEEDED: 1722 KBYTES
REQ: chg
TYPE: net
TYPE NET_DATA
CUST 0
OPT
...
TRNX YES → Enable transfer feature
EXTT YES → Enable external trunk to trunk transfer
...
```

5.5 Administer Dialing Plans

This section describes the steps to configure dialing plans for outbound and inbound calls.

5.5.1 Define ESN Access Codes and Parameters (ESN)

Access the CS1000 Element Manager then navigate to **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** to define **NARS/BARS Access Code 1**, **NARS Access Code 2** and **Number of digits in CDP DN (DSC+DN or LSC+DN)** as shown below.

AVAYA CS1000 Element Manager

Managing: 100.20.2.136 Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control 8

ESN Access Codes and Basic Parameters

General Properties

NARS/BARS Access Code 1: 9
NARS Access Code 2: 6

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

Expensive Route Warning Tone: ☒

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

Coordinated Dialing Plan feature for this customer: ☒

- Maximum number of Steering Codes: 100 (1 - 64000)

- Number of digits in CDP DN (DSC + DN or LSC + DN): 4 (3 - 10)

Routing Controls: ☐

Check for Trunk Group Access Restrictions: ☐

Limits

Maximum number of Digit Manipulation tables: 100 (0 - 2000)

Maximum number of Route Lists: 100 (0 - 2000)

5.5.2 Digit Manipulation Block Index (DMI)

In this sample configuration, **Digit Manipulation Block Index 1** was added as shown below.

The screenshot displays the AVAYA CS1000 Element Manager web interface. On the left is a navigation menu with options like UCM Network Services, Home, Links, System, Customers, Routes and Trunks, and Dialing and Numbering Plans. The main content area shows the 'Digit Manipulation Block List' page. At the top, it indicates the user is managing IP 100.20.2.136 as 'admin'. Below this, a breadcrumb trail shows the path: Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Network Control & Services » Digit Manipulation Block List. The title 'Digit Manipulation Block List' is prominently displayed. Below the title, there is a prompt 'Please choose the' followed by a dropdown menu currently set to 'Digit Manipulation Block Index 2' and a 'to Add' button. A table below contains one entry, 'Digit Manipulation Block Index -- 1', which is highlighted with a red border. To the right of this entry is an 'Edit' button. Below the entry, two configuration details are listed: 'Number of leading digits to be deleted: 0' and 'Call Type to be used by the manipulated digits : NPA'.

AVAYA **CS1000 Element Manager**

Managing: [100.20.2.136](#) 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 2 to Add

Digit Manipulation Block Index -- 1	Edit
Number of leading digits to be deleted: 0	
Call Type to be used by the manipulated digits : NPA	

5.5.3 Route List Block Index

Navigate to **Dialing and Numbering Plans > Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen. Select **Route List Block**. Enter an available value in the textbox for the **Please enter a route list index** (in this example **10**) and click on **Add** (not shown).

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

- **Digit Manipulation Index: 1.**
- **Incoming CLID Table: 0** (created in **Section 5.4.7**).
- **Route number: 10** (created in **Section 5.4.5**).

AVAYA CS1000 Element Manager

Managing: 100.20.2.136 Username: admin
Dialing and Numbering Plans > **Electronic Switched Network (ESN)** > Customer 00 > Network Control & Services > Route List Blocks > Route List Block > Data Entry of a Route List Block

Data Entry of a Route List Block

Route List Block Index: 10

General Properties

Entry Number for the Route List: 0

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 - 100)

Options

Local Termination entry: ☐
Route Number: 10
Skip Conventional Signaling: ☐
Use Tone Detector: ☐
Conversion to LDN: ☐
Expensive Route: ☐
Strategy on Congestion: No Reroute (NRR)

5.5.4 Incoming Digit Translation Configuration

Navigate to **Dialing and Numbering Plans > Incoming Digit Translation** from the left pane to display the **Incoming Digit Translation** screen. Click on the **Edit IDC** button (not shown). Click on the **New DCNO** to create the digit translation mapping. In this example, **Digit Conversion Tree 0** has been previously created (not shown).

Detailed configuration of the **Digit Conversion Tree 0 Configuration** is shown below. The **Incoming Digits** can be added to map to the **Converted Digits** which would be the associated Avaya CS1000 system phone DN. This **DCNO** has been configured on **route 10** as shown in **Section 5.4.5**.

In the following configuration, the incoming call from the PSTN to DID with prefix 00472239xxxx will be translated to the associated DN with 4 digits.

Note: For confidentiality and privacy purposes, the actual 4 remaining digits used for DID numbers in this testing have been masked.

AVAYA

CS1000 Element Manager

UCM Network Services

Home

Links

Virtual Terminals

System

Customers

Routes and Trunks

Routes and Trunks

D-Channels

Digital Trunk Interface

Dialing and Numbering Plans

Electronic Switched Network

Flexible Code Restriction

Incoming Digit Translation

Phones

Templates

Reports

Views

Lists

Properties

Migration

Tools

Managing: 100.20.2.136 Username: admin

Dialing and Numbering Plans » Incoming Digit Translation » Customer 00 » Digit Conversion Tree 0 Configuration

Digit Conversion Tree 0 Configuration

Regular IDC tree

Send calling party DID disabled

Add...

Delete IDC

Delete IDC tree

	Incoming Digits ▲	Converted Digits	CPND Name
1 ○	00472239xxxx	1661	,
2 ○	00472239xxxx	1662	,
3 ○	00472239xxxx	1663	,
4 ○	00472239xxxx	1664	,

5.5.5 Outbound Call – Trunk Steering Code Configuration

The Trunk Steering Code 00 was added for making outbound call to Telenor. This number was associated to **Route list index 10** created in **Section 5.5.3**.

Navigate to **Dialing and Numbering Plans > Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen. Select **Trunk Steering Code (TSC)**. Enter a TSC number and then click on **Add** button. Below figure shows the TSC number used for this testing.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left navigation pane includes sections for UCM Network Services, System, Customers, Routes and Trunks, and Dialing and Numbering Plans. The 'Dialing and Numbering Plans' section is expanded, showing 'Electronic Switched Network' as the selected option. The main content area displays the 'Trunk Steering Code List' page. At the top, it shows 'Managing: 100.20.2.136' and 'Username: admin'. Below this, the breadcrumb path is 'Dialing and Numbering Plans > Electronic Switched Network (ESN) > Customer 00 > Coordinated Dialing Plan (CDP) > Trunk Steering Code List'. The page title is 'Trunk Steering Code List'. There is a 'Display' dropdown menu. Below that, there are input fields for 'Starting Trunk Steering Code' (set to 00) and 'Number of Steering Codes to display' (empty), with a 'View' button. A table below shows one entry: 'Trunk Steering Code -- 00'. To the right of this entry is an 'Edit' button. Below the table, there are two fields: 'Flexible Length number of digits: 0' and 'Route List to be accessed for trunk steering code: 10'. At the bottom, it says 'Collect Call Blocking: N'.

5.6 Enable Plug-ins on CS1000

In order for off-net call transfer to operate successfully, **plug-in 201** and **plug-in 501** must be enabled on CS1000. Please refer to **CS1000 Plug-in Feature** document which is available at <https://downloads.avaya.com/css/P8/documents/100166144> .

5.7 Save the configuration

Expand **Tools** → **Backup and Restore** on the left navigation panel and select **Call Server**. Select **Backup** and click **Submit** to save configuration changes as shown below.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left navigation pane includes sections for UCM Network Services, System, Customers, Routes and Trunks, and Dialing and Numbering Plans. The 'Tools' section is expanded, showing 'Backup and Restore' as the selected option. The main content area displays the 'Call Server Backup' page. At the top, it shows 'Managing: 100.20.2.136' and 'Username: admin'. Below this, the breadcrumb path is 'Tools > Backup and Restore > Call Server Backup and Restore > Call Server Backup'. The page title is 'Call Server Backup'. There is a red box around the 'Action' dropdown menu, which is set to 'Backup'. To the right of the dropdown are 'Submit' and 'Cancel' buttons.

The backup process will take several minutes to complete.

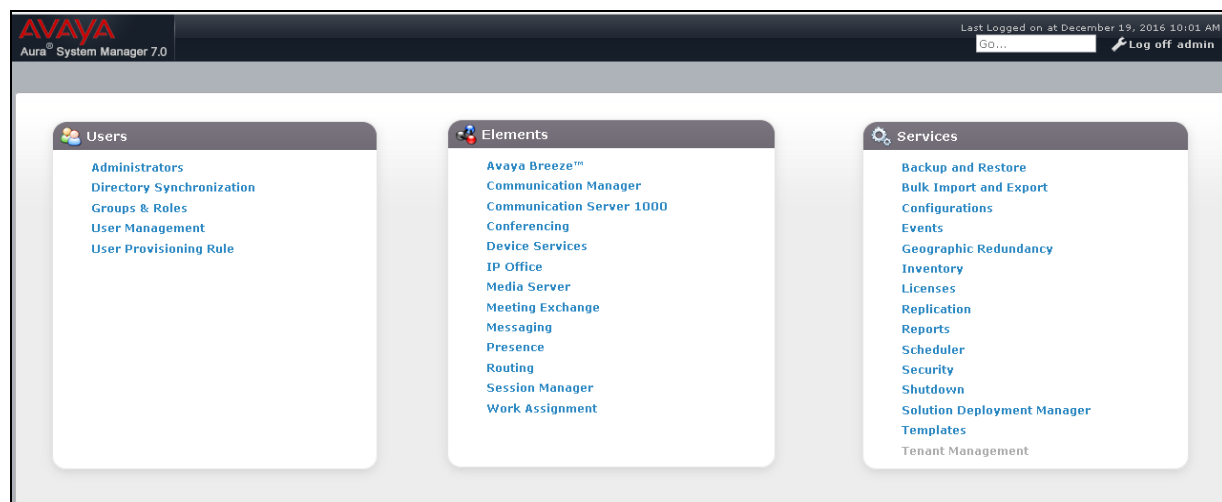
6. Configure Avaya Aura® Session Manager

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

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

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

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL **http://<ip-address>/SMGR**, where **<ip-address>** is the IP address of System Manager. In the **Log On** screen (not shown), enter appropriate **User ID** and **Password** and press the **Log On** button. Once logged in, the **Home** screen is displayed. From the **Home** screen, under the **Elements** heading in the center, select **Routing**.



6.1 Configure SIP Domain

Follow the steps shown below:

1. Select **Domains** from the left navigation menu. In the reference configuration, domain **sipinterop.com** was defined.
2. Click **New** (not shown). Enter the following values and use default values for remaining fields.
 - **Name:** Enter the enterprise SIP Domain Name. In the sample screen below, **sipinterop.com** is shown.
 - **Type:** Verify **sip** is selected.
 - **Notes:** Add a brief description.
3. Click **Commit** to save (not shown).

The screenshot shows the Avaya Aura System Manager 7.0 interface. The left navigation pane is expanded to 'Routing', and 'Domains' is selected. The main content area is titled 'Domain Management' and shows a table with one item. The table has columns for 'Name', 'Type', and 'Notes'. The item 'sipinterop.com' is listed with type 'sip' and note 'default sip domain'. The table is highlighted with a red border.

Name	Type	Notes
sipinterop.com	sip	default sip domain

6.2 Configure Locations

Locations are used to identify logical and/or physical locations where SIP Entities reside. In the reference configuration, location **siptrunking** was configured.

Follow the steps shown below:

1. Select **Locations** from the left navigational menu. Click on **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.
 - **Name:** Enter a descriptive name for the Location (e.g., **siptrunking**).
 - **Notes:** Add a brief description.
2. In the **Overall Managed Bandwidth** section:
 - **Total Bandwidth:** Enter a desired value (e.g., **2048**).
 - **Multimedia Bandwidth:** Enter a desired value (e.g., **1024**).
3. Click on **Commit** to save.

The screenshot displays the Avaya Aura System Manager 7.0 web interface. The left-hand navigation pane shows the 'Routing' menu expanded, with 'Locations' selected. The main content area is titled 'Location Details' and contains the following sections:

- General:** Includes fields for 'Name' (set to 'siptrunking') and 'Notes' (set to 'for SBCE sip trunking'). A red box highlights these two fields.
- Dial Plan Transparency in Survivable Mode:** Includes an 'Enabled' checkbox (unchecked), a 'Listed Directory Number' field, and an 'Associated CM SIP Entity' field.
- Overall Managed Bandwidth:** Includes a 'Managed Bandwidth Units' dropdown (set to 'Kbit/sec'), a 'Total Bandwidth' field (set to '2048'), and a 'Multimedia Bandwidth' field (set to '1024'). A red box highlights these three fields.

At the bottom of the form, there is a checkbox for 'Audio Calls Can Take Multimedia Bandwidth' which is checked. In the top right corner of the 'Location Details' section, there are 'Commit' and 'Cancel' buttons, with the 'Commit' button highlighted by a red box.

6.3 Configure Adaptations

An Adaptation was configured to format the History Info on Avaya CS1000 to be compatible with other Avaya products. To add a new Adaptation, navigate to **Routing > Adaptations**. Click the **New** button in the right pane (not shown). Enter an appropriate **Adaptation Name** to identify the Adaptation. Select **CS1000Adapter** from the **Module Name** drop-down menu. Select **Name-Value Parameter** from the **Module Parameter Type** drop-down menu. Click on **Add** button to add **Name** as **Fromto** and **Value** as **true**. Click on **Commit** button after changes are completed.

AVAYA
Aura® System Manager 7.0

Home Routing x

Home / Elements / Routing / Adaptations

Adaptation Details

Commit Cancel

General

* Adaptation Name: cs1k

* Module Name: CS1000Adapter

Module Parameter Type: Name-Value Parameter

Add Remove

<input type="checkbox"/>	Name	Value
<input type="checkbox"/>	fromto	true

Select : All, None

Egress URI Parameters:

Notes:

Another Adaptation was configured to convert the incoming numbers to Avaya CS1000 and to convert the outgoing numbers to Avaya SBCE. To add a new Adaptation, navigate to **Routing > Adaptations**. Click on **New** button in the right pane (not shown). Enter an appropriate **Adaptation Name** to identify the Adaptation. Select **DigitConversionAdapter** from the **Module Name** drop-down menu. Select **Name-Value Parameter** from the **Module Parameter Type** drop-down menu. Click on **Add** button two times to add **Name** as **MIME** and **Value** as **no**, and **Name** as **Fromto** and **Value** as **true**. Scroll down to **Digit Conversion for Incoming Calls to SM** to add a record so that the DID numbers sent from Telenor have “+” replaced by prefix 00 before sending to Avaya CS1000 as Avaya CS1000 does not recognize numbers started with “+”. Under **Digit Conversion for Outgoing Calls from SM** to add a record so that outgoing numbers to Avaya SBCE have prefix 00 replaced by “+” as Telenor requires international E.164 format with “+”. Click on **Commit** button after changes are completed.

AVAYA
Aura® System Manager 7.0

Home Routing

Home / Elements / Routing / Adaptations

Adaptation Details

Commit Cancel

General

* Adaptation Name: Telenor

* Module Name: DigitConversionAdapter


Module Parameter Type: Name-Value Parameter

Name	Value
fromto	true
MIME	no

Select : All, None

Digit Conversion for Incoming Calls to SM

Add Remove

1 Item  Filter: Enable


<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	*+47	*11	*11		*1	00	both		

< >

Select : All, None

Digit Conversion for Outgoing Calls from SM

Add Remove

1 Item  Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
<input type="checkbox"/>	*00	*10	*16		*2	+	both		

< >

Select : All, None

Commit Cancel

6.4 Configure SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it which includes Avaya CS1000 and Avaya SBCE.

6.4.1 Configure Session Manager SIP Entity

Follow the steps shown below:

1. In the left pane under **Routing**, click on **SIP Entities**. In the **SIP Entities** page, click on **New** (not shown).
2. In the **General** section of the **SIP Entity Details** page, provision the following:
 - **Name** – Enter a descriptive name (e.g., **sm01**).
 - **FQDN or IP Address** – Enter the IP address of Session Manager signaling interface, (*not* the management interface), provisioned during installation (e.g., **100.20.2.165**).
 - **Type** – Verify **Session Manager** is selected.
 - **Location** – Select location **siptrunking**.
 - **Outbound Proxy** – (Optional) Leave blank or select another SIP Entity. For calls to SIP domains for which Session Manager is not authoritative, Session Manager routes those calls to this **Outbound Proxy** or to another SIP proxy discovered through DNS if **Outbound Proxy** is not specified.
 - **Time Zone** – Select the time zone in which Session Manager resides.
3. In the **SIP Monitoring** section of the **SIP Entity Details** page, configure as follows:
 - Select **Use Session Manager Configuration** for **SIP Link Monitoring** field.
 - Use the default values for the remaining parameters. Click on **Commit**.

AVAYA
Aura® System Manager 7.0

Home Routing x

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit Cancel

General

* Name: sm01

* FQDN or IP Address: 100.20.2.165

Type: Session Manager

Notes:

Location: siptrunking

Outbound Proxy:

Time Zone: Asia/Ho_Chi_Minh

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

6.4.2 Configure Avaya CS1000 SIP Entity

Follow the steps shown below:

1. In the **SIP Entities** page, click on **New** (not shown).
2. In the **General** section of the **SIP Entity Details** page, provision the following:
 - **Name** – Enter a descriptive name (e.g., **cs1k**).
 - **FQDN or IP Address** – Enter the IP address of CS1000 Node IP as in **Section 5.2.1** (e.g., **100.20.2.197**).
 - **Type** – Select **SIP Trunk**.
 - **Adaptation** – Select **cs1k** created in **Section 6.3**.
 - **Location** – Select location **siptrunking** administered in **Section 6.2**.
 - **Time Zone** – Select the time zone in which CS1000 resides.
 - In the **SIP Link Monitoring** section of the **SIP Entity Details** page select:
 - Select **Use Session Manager Configuration** for **SIP Link Monitoring** field, and use the default values for the remaining parameters.
3. Click on **Commit**.

AVAYA
Aura® System Manager 7.0

Home Routing x

Home / Elements / Routing / SIP Entities

SIP Entity Details

General

Name: cs1k

FQDN or IP Address: 100.20.2.197

Type: SIP Trunk

Notes:

Adaptation: cs1k

Location: siptrunking

Time Zone: Asia/Ho_Chi_Minh

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

Credential name:

Securable: ☐

Call Detail Recording: egress

Loop Detection

Loop Detection Mode: On

Loop Count Threshold: 5

Loop Detection Interval (in msec): 200

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Commit **Cancel**

6.4.3 Configure Avaya SBCE SIP Entity

Repeat the steps in **Section 6.4.2** with the following changes:

- **Name** – Enter a descriptive name (e.g., **sbce-A1**).
- **FQDN or IP Address** – Enter the IP address of the A1 (private) interface of the Avaya SBCE (e.g., **10.128.197.22**).
- **Adaptation** – Select **Telenor** created in **Section 6.3**.

AVAYA
Aura® System Manager 7.0

Home Routing x

Home / Elements / Routing / SIP Entities

SIP Entity Details

Commit Cancel

General

* Name: sbce-A1

* FQDN or IP Address: 10.128.197.22

Type: SIP Trunk

Notes: sip trunk to sbce A1 interface

Adaptation: Telenor

Location: siptrunking

Time Zone: Asia/Ho_Chi_Minh

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

Credential name:

Securable: ☐

Call Detail Recording: egress

Loop Detection

Loop Detection Mode: On

Loop Count Threshold: 5

Loop Detection Interval (in msec): 200

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

6.5 Configure Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. During compliance testing, two Entity Links were created, one for Avaya CS1000 and another one for Avaya SBCE. To add an Entity Link, navigate to **Routing → Entity Links** in the left navigation pane and click on **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 defined in **Section 6.4.1**.
- **Protocol:** Select the transport protocol used for this link, **TLS** for the Entity Link to Avaya CS1000 and Avaya SBCE.

- **Port:** Port number on which Session Manager will receive SIP requests from the far-end.
- **SIP Entity 2:** Select the name of the other systems. For Avaya CS1000, select the Avaya CS1000 SIP Entity defined in **Section 6.4.2**. For Avaya SBCE, select the Avaya SBCE SIP Entity defined in **Section 6.4.3**.
- **Port:** Port number on which the other system receives SIP requests from Session Manager.
- **Connection Policy:** Select **Trusted**.
- Click **Commit** to save.

6.5.1 Configure Entity Link to Avaya CS1000

Follow the steps shown below:

1. In the left pane under **Routing**, click on **Entity Links**, then click on **New** button (not shown).
2. Continuing in the **Entity Links** page, provision the following:
 - **Name** – Enter a descriptive name (or have it created automatically) for this link to CS1000 (e.g., **sm01_cs1k_5061_TLS**).
 - **SIP Entity 1** – Select the SIP Entity administered in **Section 6.4.1** for Session Manager (e.g., **sm01**).
 - **SIP Entity 1 Port** – Enter **5061**.
 - **Protocol** – Select **TLS**.
 - **SIP Entity 2** – Select the SIP Entity administered in **Section 6.4.2** for the CS1000 entity (e.g., **cs1k**).
 - **SIP Entity 2 Port** – Enter **5061**.
 - **Connection Policy** – Select **Trusted**.
3. Click on **Commit**.

The screenshot shows the Avaya Aura System Manager 7.0 interface. The left navigation pane is expanded to 'Routing', and 'Entity Links' is selected. The main area shows the 'Entity Links' configuration page. At the top right, there are 'Commit' and 'Cancel' buttons, with 'Commit' highlighted by a red box. Below this is a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, DNS Override, Port, and Connection Policy. The row contains: sm01_cs1k_5060_TLS, sm01, TLS, 5061, cs1k, unchecked, 5061, and trusted. A red box highlights the entire row.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Conne Poli
* sm01_cs1k_5060_TLS	* Q sm01	TLS	* 5061	* Q cs1k	<input type="checkbox"/>	* 5061	trusted

6.5.2 Configure Entity Link for Avaya SBCE

To configure this Entity Link, repeat the steps in **Section 6.5.1**, with the following changes:

- **Name** – Enter a descriptive name (or have it created automatically) for this link to the Avaya SBCE (e.g., **sm01_sbce-A1_5061_TLS**).
- **SIP Entity 2** – Select the SIP Entity administered in **Section 6.4.3** for the Avaya SBCE entity (e.g., **sbce-A1**).

AVAYA
Aura® System Manager 7.0

Last Logged on at December 19, 2016 10:01 AM
Go... Log off admin

Home Routing

Home / Elements / Routing / Entity Links

Entity Links

Commit Cancel

1 Item Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Conne: Poli
sm01_sbce-A1_5061	* Q sm01	TLS	* 5061	* Q sbce-A1	<input type="checkbox"/>	* 5061	trusted

Select: All, None

6.6 Configure Routing Policies

Routing Policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two routing policies were added, one for Avaya CS1000 and another one for Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left navigation pane and click on **New** button in the right pane (not shown).

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

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

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

6.6.1 Configure Routing Policy for Avaya CS1000

This Routing Policy was used for inbound calls from Telenor.

1. In the left pane under **Routing**, click on **Routing Policies**. In the **Routing Policies** page click on **New** button (not shown).
2. In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** for routing calls from Telenor to Avaya CS1000 (e.g., **to cs1k**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
3. **Retries: 0**.
4. In the **SIP Entity as Destination** section of the **Routing Policy Details** page, click on **Select** and the SIP Entity list page will open.
5. In the **SIP Entity List** page, select the SIP Entity administered in **Section 6.4.2** for the CS1000 SIP Entity (**cs1k**), and click on **Select**.
6. Note that once the **Dial Patterns** are defined they will appear in the **Dial Pattern** section of this form.
7. No **Regular Expressions** were used in the reference configuration.
8. Click on **Commit**.

AVAYA
Aura® System Manager 7.0

Last Logged on a
Go...

Home Routing

Routing
Domains
Locations
Adaptations
SIP Entities
Entity Links
Time Ranges
Routing Policies
Dial Patterns
Regular Expressions
Defaults

Home / Elements / Routing / Routing Policies

Routing Policy Details

Commit Cancel

General

* Name: to cs1k

Disabled: ☐

* Retries: 0

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	No
cs1k	100.20.2.197	SIP Trunk	

6.6.2 Configure Routing Policy for Avaya SBCE

This Routing Policy is used for outbound calls to the service provider. Repeat the steps in **Section 6.6.1**, with the following changes:

- **Name** – Enter a descriptive name for this link to the Avaya SBCE (e.g., **to SBCE A1**).
- **SIP Entity List** –Select the SIP Entity administered in **Section 6.4.3** for the Avaya SBCE entity (e.g., **sbce-A1**).

The screenshot displays the Avaya Aura System Manager 7.0 interface. The left sidebar shows the navigation menu with 'Routing Policies' selected. The main content area is titled 'Routing Policy Details' and includes 'Commit' and 'Cancel' buttons. The 'General' tab is active, showing the following fields:

- * Name:** to SBCE A1
- Disabled:** ☐
- * Retries:** 0
- Notes:** outbound calls to SP

The 'SIP Entity as Destination' section is highlighted with a red box. It contains a 'Select' button and a table with the following data:

Name	FQDN or IP Address	Type	Notes
sbce-A1	10.128.197.22	SIP Trunk	sip trunk to sbce A1 interface

6.7 Configure Dial Patterns

Dial Patterns are needed to route specific calls through Session Manager. For the compliance testing, dial patterns were needed to route calls from Avaya CS1000 to Telenor and vice versa. Dial Patterns define which routing policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing** → **Dial Patterns** in the left navigation pane and click on **New** button in the right pane (not shown). In the **General** section, enter the following values:

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

In the **Originating Locations and Routing Policies** section, click on **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 on **Select**.

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

The first example shows that 5-digit to 16-digit dialed numbers that begin with 00 and have a destination domain of “**sipinterop.com**” uses route policy to Avaya SBCE as defined in **Section 6.6.2**.

The screenshot displays the Avaya Aura System Manager 7.0 interface. The left navigation pane shows the 'Routing' menu expanded, with 'Dial Patterns' selected. The main content area is titled 'Dial Pattern Details' and includes a 'Commit' button. The 'General' section contains the following fields:

- Pattern:** 00
- Min:** 5
- Max:** 16
- Emergency Call:** ☐
- Emergency Priority:** 1
- Emergency Type:**
- SIP Domain:** sipinterop.com
- Notes:** outbound call to Telenor

The 'Originating Locations and Routing Policies' section shows a table with one item:

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
-ALL-		to SBCE A1	0	<input type="checkbox"/>	sbce-A1	outbound calls to SP

The second example shows that 12-digit pattern that start with 00472239 is used for inbound calls from Telenor to DID numbers on Avaya CS1000.

AVAYA
Aura® System Manager 7.0

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

Commit Cancel

General

* Pattern: 00472239
* Min: 12
* Max: 12

Emergency Call: ☐
Emergency Priority: 1
Emergency Type:
SIP Domain: sipinterop.com
Notes: inbound DID call from Telenor to cs1k

Originating Locations and Routing Policies

Add Remove

1 Item

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination
<input type="checkbox"/>	-ALL-		to cs1k	0	<input type="checkbox"/>	cs1k

Select : All, None

7. Configure Avaya Session Border Controller for Enterprise

Note: The installation and initial provisioning of the Avaya SBCE is beyond the scope of this document.

IMPORTANT! – During the Avaya SBCE installation, the Management interface of the Avaya SBCE must be provisioned on a different subnet than either of the Avaya SBCE private and public network interfaces (e.g., A1 and B1).

As described in **Section 3**, the reference configuration places the private interface (A1) of the Avaya SBCE in the enterprise site (100.20.2.173). The connection to Telenor uses the Avaya SBCE public interface B1 (192.168.5.48). The follow provisioning is performed via the Avaya SBCE GUI interface, using the “M1” management LAN connection on the chassis.

1. Access the web interface by typing “**https://x.x.x.x**” (where x.x.x.x is the management IP address of the Avaya SBCE).
2. Enter the **Username** and click on **Continue**.

3. Enter the password and click on **Log In**.

The main menu window will open. Note that the installed software version is displayed. Verify that the **License State** is **OK**. The SBCE will only operate for a short time without a valid license. Contact your Avaya representative to obtain a license.

Session Border Controller for Enterprise AVAYA

Dashboard

- Administration
- Backup/Restore
- System Management
 - Global Parameters
 - Global Profiles
 - PPM Services
 - Domain Policies
 - TLS Management
 - Device Specific Settings

Information

System Time	10:06:31 AM ICT	Refresh
Version	7.1.0.1-07-12368	
Build Date	Fri Nov 11 09:21:54 EST 2016	
License State	OK	
Aggregate Licensing Overages	0	
Peak Licensing Overage Count	0	
Last Logged in at	12/27/2016 09:22:07 ICT	
Failed Login Attempts	0	

Installed Devices

- EMS
- sbce

Alarms (past 24 hours)

None found.

Incidents (past 24 hours)

- sbce : No Subscriber Flow Matched
- sbce : Method Prohibited Out-of-Dialog
- sbce : No Subscriber Flow Matched

7.1 System Management – Status

1. Select **System Management** and verify that the **Status** column says **Commissioned**.

System Management

Devices | Updates | SSL VPN | Licensing | Key Bundles

Device Name	Management IP	Version	Status	
sbce	100.20.2.173	7.1.0.1-07-12368	Commissioned	Reboot Shutdown Restart Application View Edit Uninstall

2. Click on **View** (shown above) to display the **System Information** screen.

System Information: sbce X

General Configuration

Appliance Name	sbce
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

License Allocation

Standard Sessions Requested: 20	20
Advanced Sessions Requested: 20	20
Scopia Video Sessions Requested: 0	0
CES Sessions Requested: 0	0
Transcoding Sessions Requested: 0	0
Encryption	<input checked="" type="checkbox"/>

Network Configuration

IP	Public IP	Network Prefix or Subnet Mask	Gateway	Interface
10.128.197.22	10.128.197.22	255.255.255.192	10.128.197.1	A1
192.168.5.48	192.168.5.48	255.255.255.0	192.168.5.1	B1

DNS Configuration

Primary DNS	8.8.8.8
Secondary DNS	
DNS Location	DMZ
DNS Client IP	

Management IP(s)

IP #1 (IPv4)	100.20.2.173
--------------	--------------

7.2 Global Profiles

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

7.2.1 Uniform Resource Identifier (URI) Groups

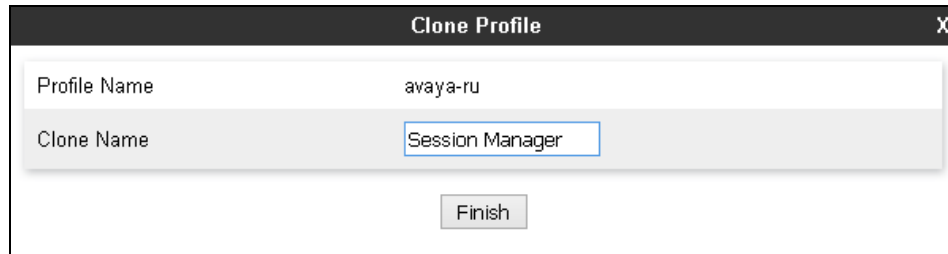
URI Group feature allows a user to create any number of logical URI Groups that are comprised of individual SIP subscribers located in that particular domain or group. These groups are used by the various domain policies to determine which actions (Allow, Block, or Apply Policy) should be used for a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

For this configuration testing, “*” is used for all incoming and outgoing traffic.

7.2.2 Server Interworking – Session Manager

Server Interworking allows users to configure and manage various SIP call server-specific capabilities such as call hold and T.38 faxing. This section defines the profile for the connection to Session Manager.

1. Navigate to **Global Profiles > Server Interworking** from the left-hand menu.
2. Select **avaya-ru** then click on **Clone** button.
3. Enter profile name: (e.g., **SessionManager**), and click on **Finish**.



Clone Profile	
Profile Name	avaya-ru
Clone Name	Session Manager
<div>Finish</div>	

4. Click on **Edit** in **General** tab (not shown).
- Check **T38 Support** box.
 - Click on **Finish**.

The screenshot shows a dialog box titled "Editing Profile: Session Manager" with a close button (X) in the top right corner. The "General" tab is selected. The dialog contains various settings for session management, each with a label and a control element (radio button, checkbox, or dropdown menu). The "T38 Support" checkbox is checked and highlighted with a red rectangular box. The "Finish" button at the bottom right is also highlighted with a red rectangular box.

Setting	Value/Option
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
URI Group	None (dropdown)
Send Hold	<input type="checkbox"/>
Delayed Offer	<input type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
Re-Invite Handling	<input type="checkbox"/>
Prack Handling	<input type="checkbox"/>
Allow 18X SDP	<input type="checkbox"/>
T38 Support	<input checked="" type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543

Finish

5. Click on **Edit** in the **Advanced** tab (not shown).
- **Record Routes:** Choose **None**.
 - Click on **Finish**.

Editing Profile: Session Manager

Record Routes

- ☒ None
- ☐ Single Side
- ☐ Both Sides
- ☐ Dialog-Initiate Only (Single Side)
- ☐ Dialog-Initiate Only (Both Sides)

Include End Point IP for Context Lookup ☒

Extensions Avaya

Diversion Manipulation ☐

Diversion Condition None

Diversion Header URI

Has Remote SBC ☒

Route Response on Via Port ☐

Relay INVITE Replace for SIPREC ☐

DTMF

DTMF Support

- ☒ None
- ☐ SIP Notify
- ☐ SIP Info
- ☐ Inband

Finish

7.2.3 Server Interworking – Telenor

Navigate to **Global Profiles > Server Interworking** from the left-hand menu to add an Interworking Profile for the connection to Telenor network.

1. Click on **Add** (not shown) then enter **Telenor** as the **profile name** and click on **Next** (not shown).
2. In **General** window: Check **T.38 Support** then click on **Next**.

The screenshot shows the 'Interworking Profile' configuration window with the 'General' tab selected. The window contains various settings for server interworking. The 'T.38 Support' checkbox is checked and highlighted with a red box. The 'Next' button at the bottom right is also highlighted with a red box.

Interworking Profile	
General	
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3264 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
URI Group	None
Send Hold	<input checked="" type="checkbox"/>
Delayed Offer	<input checked="" type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
Re-Invite Handling	<input type="checkbox"/>
Prack Handling	<input type="checkbox"/>
Allow 18X SDP	<input type="checkbox"/>
T.38 Support	<input checked="" type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3261 <input type="radio"/> RFC2543
<input type="button" value="Back"/> <input checked="" type="button" value="Next"/>	

3. Leave default values in **SIP Timers** window and **Privacy** window (not shown).
4. In **Advance** window: Select **None** for **Record Routes** then click on **Finish**.

The screenshot shows the 'Interworking Profile' configuration window. It contains several sections with various settings:

- Record Routes:** A radio button selection where 'None' is selected and highlighted with a red box. Other options are 'Single Side', 'Both Sides', 'Dialog-Initiate Only (Single Side)', and 'Dialog-Initiate Only (Both Sides)'.
- Include End Point IP for Context Lookup:** A checkbox that is currently unchecked.
- Extensions:** A dropdown menu showing 'None'.
- Diversion Manipulation:** A checkbox that is currently unchecked.
- Diversion Condition:** A dropdown menu showing 'None'.
- Diversion Header URI:** An empty text input field.
- Has Remote SBC:** A checkbox that is checked.
- Route Response on Via Port:** A checkbox that is currently unchecked.
- Relay INVITE Replace for SIPREC:** A checkbox that is currently unchecked.
- DTMF:** A section header followed by a radio button selection where 'None' is selected. Other options are 'SIP Notify', 'SIP Info', and 'Inband'.
- Buttons:** At the bottom, there are 'Back' and 'Finish' buttons. The 'Finish' button is highlighted with a red box.

7.2.4 Signaling Manipulation

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

On outbound international calls from the Avaya CS1000, it was observed that the numbering format in the Contact header contained “00” instead of “+”. Telenor requires all international numbering format to be E.164. A SigMa script was required on the Avaya SBCE to convert the “00” to “+” in the Contact header.

To define the signaling manipulation, navigate to **Global Profiles > Signaling Manipulation** in the main menu on the left hand side (not shown). Click on **Add** and enter **Telenor** for the **Title** in the script editor (not shown). The script text is displayed below.

```
within session "All"
{
    act on request where %DIRECTION="OUTBOUND" and
    %ENTRY_POINT="POST_ROUTING"
    {
        %HEADERS["Contact"][1].URI.USER.regex_replace("0047","+47");
    }
    act on response where %DIRECTION="OUTBOUND" and
    %ENTRY_POINT="POST_ROUTING"
    {
        %HEADERS["Contact"][1].URI.USER.regex_replace("0047","+47");
    }
}
```

7.2.5 Server Configuration – Session Manager

This section defines the Server Configuration for the Avaya SBCE connection to Session Manager.

1. Navigate to **Global Profiles > Server Configuration** from the left-hand menu.
2. Select **Add** and the **Profile Name** window will open. Enter a Profile Name (e.g., **Session Manager**) and click on **Next** (not shown).
3. The **Edit Server Configuration Profile - General** window will open.
 - Select **Server Type: Call Server**.
 - **IP Address / FQDN: 100.20.2.165** (Session Manager signaling IP Address as configured in **Section 6.4.1**).
 - **Transport: Select TLS**.
 - **Port: 5061**.
 - **TLS Client Profile: Select Avaya**.
 - Click on **Next**.

IP Address / FQDN	Port	Transport
100.20.2.165	5061	TLS

4. The **Add Server Configuration Profile - Authentication** window will open (not shown).
 - Click on **Next** to accept default values.

5. The **Add Server Configuration Profile - Heartbeat** window will open.
 - Check **Enable Heartbeat** box.
 - **Method**: Select **OPTIONS**.
 - **Frequency**: Enter **300** (or more).
 - **From URI** and **To URI**: Enter ping@sipinterop.com
 - Click on **Next** button.

Add Server Configuration Profile - Heartbeat

Enable Heartbeat ☒

Method OPTIONS ▾

Frequency seconds

From URI

To URI

Back Next

6. The **Add Server Configuration Profile - Advanced** window will open.
 - Check **Enable Grooming** box.
 - For **Interworking Profile**, select the profile created for Session Manager in **Section 7.2.2**.
 - Click on **Finish**.

Add Server Configuration Profile - Advanced

Enable DoS Protection ☐

Enable Grooming ☒

Interworking Profile Session Manager ▾

Signaling Manipulation Script None ▾

Securable ☐

Enable FGDN ☐

TCP Failover Port

TLS Failover Port

Back Finish

7.2.6 Server Configuration – Telenor

Repeat the steps in **Section 7.2.5**, with the following changes, to create a Server Configuration for the Avaya SBCE connection to Telenor.

1. Select **Add Profile** and enter a Profile Name (e.g., **Telenor**) and click on **Next** (not shown).
2. On the **Edit Server Configuration Profile - General** window, enter the following.
 - Select **Server Type: Trunk Server**.
 - **IP Address / FQDN: 192.168.250.10** (Telenor SBC IP address)
 - **Transport: Select UDP**.
 - **Port: 5060**.
 - Click on **Next**.

IP Address / FQDN	Port	Transport
192.168.250.10	5060	UDP

3. Under **Add Server Configuration Profile - Heartbeat**:
 - Select **Enable Heartbeat**.
 - **Method: Select PING**.
 - **Frequency: Enter 300** (or more).
 - **From URI and To URI: Enter ping@ipt.telenor.com**
 - Click on **Next** button.

Enable Heartbeat	<input checked="" type="checkbox"/>
Method	PING
Frequency	300 seconds
From URI	ping@ipt.telenor.com
To URI	ping@ipt.telenor.com

4. Under **Add Server Configuration Profile - Advanced** window:
- Select **Telenor** for Interworking Profile.
 - Select **Telenor** for Signaling Manipulation Script as configured in **Section 7.2.4**.

Add Server Configuration Profile - Advanced X

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	Telenor ▼
Signaling Manipulation Script	Telenor ▼
Securable	<input type="checkbox"/>
Enable FGDN	<input type="checkbox"/>
TCP Failover Port	5060
TLS Failover Port	5061

Back Finish

7.2.7 Routing – To Session Manager

This provisioning defines the Routing Profile for the connection to Session Manager.

1. Navigate to **Global Profiles > Routing** from the left-hand menu, and click on **Add** (not shown).
2. Enter a **Profile Name**: (e.g., **Session Manager**) and click **Next** (not shown).
3. The **Routing Profile** window will open. Using the default values shown, click on **Add**.
4. Populate the following fields:
 - **Priority/Weight = 1.**
 - **Server Configuration = Session Manager.**
 - **Next Hop Address:** Verify that the **100.20.2.165:5061 (TLS)** entry from the drop down menu is selected (Session Manager IP address). Also note that the **Transport** field is grayed out.
5. Click on **Finish**.

Routing Profile

X

URI Group	*	Time of Day	default
Load Balancing	Priority	NAPTR	<input type="checkbox"/>
Transport	None	Next Hop Priority	<input checked="" type="checkbox"/>
Next Hop In-Dialog	<input type="checkbox"/>	Ignore Route Header	<input type="checkbox"/>
ENUM	<input type="checkbox"/>	ENUM Suffix	

Add

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	Session Manager	100.20.2.165:5061 (TLS)	None	Delete

Back

Finish

7.2.8 Routing – To Telenor

Repeat the steps in **Section 7.2.7**, with the following changes, to add a Routing Profile for the Avaya SBCE connection to Telenor.

1. On the **Global Profiles → Routing** window (not shown), enter a **Profile Name**: (e.g., **Telenor**).
2. On the **Routing Profile** window, populate the following fields:
 - **Server Configuration: Telenor.**
 - **Next Hop Address:** Verify that the **192.168.250.10:5060 (UDP)** entry from the drop down menu is selected.
 - Click on **Finish**.

URI Group	Time of Day
*	default

Load Balancing	NAPTR
Priority	<input type="checkbox"/>

Transport	Next Hop Priority
None	<input checked="" type="checkbox"/>

Next Hop In-Dialog	Ignore Route Header
<input type="checkbox"/>	<input type="checkbox"/>

ENUM	ENUM Suffix
<input type="checkbox"/>	

Add

Priority / Weight	Server Configuration	Next Hop Address	Transport	Delete
1	Telenor	192.168.250.10:5060 (UDP)	None	Delete

Back Finish

7.2.9 Topology Hiding – Session Manager

The **Topology Hiding** screen allows users to manage how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the security of the network. It hides the topology of the enterprise network from external networks.

1. Navigate to **Global Profiles > Topology Hiding** from the left-hand side menu.
2. Click on **Add** button, enter **Profile Name:** (e.g., **Session Manager**), and click **Next** (not shown).
3. The **Topology Hiding Profile** window will open. Click on the **Add Header** button repeatedly to add headers.
4. Populate the fields as shown below, and click on **Finish** (not shown).

Topology Hiding Profiles: Session Manager

Add Rename Clone Delete

Topology Hiding Profiles

- default
- cisco_th_profile
- Session Manager**
- Telenor

Click here to add a description.

Topology Hiding

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

Edit

7.2.10 Topology Hiding – Telenor

Repeat the steps in **Section 7.2.9**, with the following changes, to create a Topology Hiding Profile for the Avaya SBCE connection to Telenor.

1. Enter a **Profile Name:** (e.g., **Telenor**).
2. Click on the **Add Header** button repeatedly to add headers.
3. Populate the fields as shown below, and click on **Finish** (not shown). Note that the **Overwrite Value** is **ipt.telenor.com** which is the SIP domain of Telenor.

Topology Hiding Profiles: Telenor

Add Rename Clone Delete

Topology Hiding Profiles

- default
- cisco_th_profile
- Session Manager
- Telenor**

Click here to add a description.

Topology Hiding

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

Edit

7.2.11 Domain Policies

The Domain Policies feature allows users to configure, apply and manage various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise.

7.2.12 Application Rules

Ensure that the Application rule used in the End Point Policy Group reflects the licensed sessions that the customer has purchased. In the lab setup, the default rule was used.

Note: It is not recommended to edit default rules. New rules should be added or cloned from default rules.

7.2.13 Border Rules

The Border rules specifies if NAT is utilized (on by default), as well as detecting SIP and SDP published IP addresses. In the solution as tested, the **default** rule was utilized. No customization was required.

7.2.14 Media Rules

The Media rules will be applied to both directions. In the solution as tested, the **default-low-med** rule was utilized. No customization was required.

7.2.15 Security Rules

The Security rule will be applied to both directions. In the solution as tested, the **default-low** rule was utilized. No customization was required.

7.2.16 Signaling Rules

Signaling rules are a mechanism on the Avaya SBCE to manipulate the signaling beyond simple header manipulation. Signaling rules allow action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message.

In the flow to Telenor, the SIP messages are manipulated to avoid the overhead of re-assembling fragmented UDP packets, reduce packet size and removed unnecessary headers. This is achieved by removing Avaya proprietary and unnecessary headers to reduce the SIP messages packet size to below the Maximum Transmission Unit (MTU) so that fragmentation does not occur.

To define the signaling rule, navigate to **Domain Policies > Signaling Rules** in the main menu on the left hand side.

1. Click on **Add** and enter details in the **Signaling Rule** pop-up box. In the **Rule Name** field enter a descriptive name such as **Telenor** for the signaling rule to remove Avaya proprietary and unnecessary headers.
2. Click on **Next** and **Next** again, then **Finish** (not shown).

Signaling Rules: Telenor

Click here to add a description.

Inbound

Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

Outbound

Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

Content-Type Policy

Enable Content-Type Checks	<input checked="" type="checkbox"/>
Action	Allow
Multipart Action	Allow
Exception List	Exception List

Select the **Request Headers** tab (not shown) and define the rules to remove Avaya proprietary headers and unnecessary headers as follows:

- Click on **Add In Header Control** (not shown).
- Check the **Proprietary Request Header** box to remove Avaya proprietary headers or uncheck it to remove unnecessary headers.
- Enter the name of the header to be removed in the **Header Name** field.
- Select **ALL** in the **Method Name** field.
- Check **Forbidden** in the **Header Criteria** options.
- In the **Presence Action** drop down menu, select **Remove Header**.
- Click on **Finish**.

The following example shows configuration for removal of **P-Location** header from request messages.

Note: During the test, the same was done for **Alert-Info**, **Av-Global-Session-ID**, **Endpoint-View**, **P-AV-Message-Id**, **P-Charging-Vector**, **x-nt-e164-clid**, **P-Asserted-Identity** and **P-Location** headers.

When finished, all the Request Headers defined will be displayed under the Request Headers tab as shown below.

Signaling Rules: Telenor

Add Filter By Device... Rename Clone Delete

Click here to add a description.

General Requests Responses **Request Headers** Response Headers Signaling QoS UCID

Add In Header Control Add Out Header Control

Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction		
1	Alert-Info	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
2	Av-Global-Session-ID	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
3	Endpoint-View	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
4	P-Asserted-Identity	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	x-nt-e164-clid	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete

The same is required for **Response Headers**. Select the **Response Headers** tab (not shown) and define the rules to remove Avaya proprietary headers as follows:

- Click on **Add In Header Control** (not shown).
- Check the **Proprietary Request Header** box to remove Avaya proprietary headers or uncheck it to remove unnecessary headers.
- Enter the name of the header to be removed in the **Header Name** field.
- Select **1XX** in the **Response Code** drop down menu, this will remove the header from 183 Session Progress and 180 Ringing messages.
- Select **ALL** in the **Method Name** field.
- Check **Forbidden** in the **Header Criteria** options.
- In the **Presence Action** drop down menu, select **Remove Header**.
- Click on **Finish**.

Repeat above process and select **2XX** in the **Response Code** so that the header is removed from 200 OK messages.

The following example shows configuration for removal of **Av-Global-Session-ID** header from 1XX responses.

The screenshot shows a dialog box titled "Edit Header Control" with a close button (X) in the top right corner. The dialog contains the following fields and options:

- Proprietary Response Header:** A checkbox that is checked.
- Header Name:** A text field containing "Av-Global-Session-ID".
- Response Code:** A dropdown menu with "1XX" selected.
- Method Name:** A dropdown menu with "ALL" selected.
- Header Criteria:** Three radio button options: "Forbidden" (selected), "Mandatory", and "Optional".
- Presence Action:** A dropdown menu with "Remove header" selected.
- Below the Presence Action dropdown, there are two text fields: "486" and "Busy Here".
- Finish:** A button at the bottom center of the dialog.

Note: During the test, the same was done for **Alert-Info**, **Av-Global-Session-ID**, **Endpoint-View**, **P-AV-Message-ID**, **P-Asserted-Identity**, **P-Charging-Vector** and **P-Location** headers. When finished, all the **Response Headers** defined will be shown under the **Response Headers** tab as shown below.

Signaling Rules: Telenor

Add Filter By Device... Rename Clone Delete

Click here to add a description.

General	Requests	Responses	Request Headers	Response Headers	Signaling QoS	UCID
Signaling Rules						
default						
No-Content-Type-Checks						
Telenor						
Session Manager						

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

As Telenor does not accept OPTIONS message, OPTIONS message should be removed from the **Requests** tab. On the **Requests** tab, click on **Add In Request Control**, populate as shown below then click on **Finish**:

Edit Request Control

Proprietary Request

Method Name

OPTIONS

In Dialog Action

Block with...

486

Busy Here

Out of Dialog Action

Block with...

486

Busy Here

Finish

In the flow to Session Manager, in order to ensure proper routing on Session Manager Route header must be removed. Repeat the same steps above to add a Signaling rule for Session Manager with only Route header removed in **Request Headers** tab.

Signaling Rules: Session Manager

Filter By Device... Rename Clone Delete

Click here to add a description.

General Requests Responses Request Headers Response Headers Signaling QoS UCID

Add In Header Control Add Out Header Control

Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction
1	Route	ALL	Forbidden	Remove Header	No	IN

Edit Delete

7.2.17 Endpoint Policy Groups

End point policy groups are required to implement the signaling rules. In the solution as tested, two groups were defined.

To add a new Policy Groups for Session Manager, navigate to **Domain Policies > End Point Policy Groups** in the main menu on the left hand side:

1. Click on **Add** button to add a new Policy Groups, name it as **Session Manager**.
2. Select **default** for **Application Rules**.
3. Select **default** for **Border Rules**.
4. Select **default-low-med** for **Media Rules**.
5. Select **default-low** for **Security Rules**.
6. Select **Session Manager** (created in Section 7.2.16) for **Signaling Rules**.

Policy Groups: Session Manager

Add Filter By Device... Rename Clone Delete

Click here to add a description.

Hover over a row to see its description.

Policy Group

Summary

Order	Application	Border	Media	Security	Signaling
1	default	default	default-low-med	default-low	Session Manager

Edit

Repeat the same steps to add another group for Telenor with the following change:

- Select **Telenor** (created in **Section 7.2.16**) for **Signaling Rules**.

Policy Groups: Telenor

Add Filter By Device... Rename Clone Delete

Click here to add a description.

Hover over a row to see its description.

Policy Group

Summary

Order	Application	Border	Media	Security	Signaling	
1	default	default	default-low-med	default-low	Telenor	Edit

Policy Groups

- default-low
- default-low-enc
- default-med
- default-med-enc
- default-high
- default-high-enc
- avaya-def-low-enc
- avaya-def-high-subscriber
- avaya-def-high-server
- Telenor**
- Session Manager

7.2.18 Session Policies

Session Policies are used to determine how the Avaya SBCE handles media packets. As Telenor requires the media endpoint must send at least one RTP/RTCP packet first, so Telenor can latch on this. Therefore, in case of media tromboning call type **Media Anchoring** must be disabled on Avaya SBCE.

To define a policy for Telenor, navigate to **Domain Policies > Session Policies** in the main menu on the left hand side.

1. Select **default** policy then click on **Clone**, enter a name (e.g., **Telenor**) and click on **Finish** (not shown).
2. Click on **Edit**.
3. Uncheck **Media Anchoring**.
4. Select **Media Tromboning Only** for **Call Type for Media Unanchoring**.
5. Click on **Finish**.

Media	
Media Anchoring	<input type="checkbox"/>
Media Forking Profile	None ▾
Converged Conferencing	<input type="checkbox"/>
Recording Server	<input type="checkbox"/>
Recording Type	Full Time ▾
Play Recording Tone	<input type="checkbox"/>
Call Termination on Recording Failure	<input type="checkbox"/>
Routing Profile	None ▾
Call Type for Media Unanchoring	Media Tromboning Only ▾
<div>Finish</div>	

7.3 Device Specific Settings

The **Device Specific Settings** feature for SIP allows you to view aggregate system information, and manage various device-specific parameters which determine how a particular device will function when deployed in the network. Specifically, you have the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality, end-point and session call flows.

7.3.1 Network Management

1. Select **Device Specific Settings** > **Network Management** from the menu on the left-hand side.
2. The **Interfaces** tab displays the enabled/disabled interfaces. In the reference configuration, interfaces A1 (private) and B1 (public) interfaces are used.
3. Select the **Networks** tab to display the IP provisioning for the A1 and B1 interfaces. These values are normally specified during installation. These can be modified by selecting **Edit**; however some of these values may not be changed if associated provisioning is in use.

7.3.2 Media Interfaces

1. Navigate to **Device Specific Settings** from the menu on the left-hand side (not shown).
2. Select **Media Interface**.
3. Click on **Add** (not shown). The **Add Media Interface** window will open. Enter the following:
 - **Name:** Int_med.
 - **IP Address:** 10.128.197.22 (Avaya SBCE A1 address).
 - **Port Range:** 35000-40000.
4. Click on **Finish** (not shown).
5. Click on **Add** (not shown). The **Add Media Interface** window will open. Enter the following:
 - **Name:** Ext_med.
 - **IP Address:** 192.168.5.48 (Avaya SBCE B1 address).
 - **Port Range:** 10000-10999. (Media port range that Telenor uses)
6. Click on **Finish** (not shown). Note that changes to these values require an application restart. The completed **Media Interface** screen is shown below.

Media Interface: sbce

Devices
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 Network	Port Range	
Int_med	10.128.197.22 A1 (A1, VLAN 0)	35000 - 40000	Edit Delete
Ext_med	192.168.5.48 B1 (B1, VLAN 0)	10000 - 10999	Edit Delete

7.3.3 Signaling Interface

1. Navigate to **Device Specific Settings** from the menu on the left-hand side (not shown).
2. Select **Signaling Interface**.
3. Click on **Add** (not shown) and enter the following:
 - **Name: Int_sig.**
 - **IP Address: 10.128.197.22** (Avaya SBCE A1 address).
 - **TLS Port: 5061.**
4. Click on **Finish** (not shown).
5. Click on **Add** again, and enter the following:
 - **Name: Ext_sig.**
 - **IP Address: 192.168.5.48** (Avaya SBCE B1 address).
 - **UDP Port: 5060.**
6. Click on **Finish** (not shown). Note that changes to these values require an application restart.

Signaling Interface: sbce

Devices
sbce

Signaling Interface

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

Add

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
Int_sig	10.128.197.22 A1 (A1, VLAN 0)	---	---	5061	None	Edit Delete
Ext_sig	192.168.5.48 B1 (B1, VLAN 0)	---	5060	---	None	Edit Delete

7.3.4 Endpoint Flows – For Session Manager

1. Navigate to **Device Specific Settings → Endpoint Flows** from the menu on the left-hand side (not shown).
2. Select the **Server Flows** tab (not shown).
3. Click on **Add**, (not shown) and enter the following:
 - **Name: Session Manager.**
 - **Server Configuration: Session Manager.**
 - **URI Group: ***
 - **Transport: ***
 - **Remote Subnet: ***
 - **Received Interface: Ext_sig.**
 - **Signaling Interface: Int_sig.**
 - **Media Interface: Int_med.**
 - **End Point Policy Group: Telenor.**
 - **Routing Profile: Telenor.**
 - **Topology Hiding Profile: Session Manager.**
 - Let other values default.
4. Click on **Finish**.

Edit Flow: Session ManagerX

Flow Name	<input type="text" value="Session Manager"/>
Server Configuration	<input type="text" value="Session Manager"/>
URI Group	<input type="text" value="*/"/>
Transport	<input type="text" value="*/"/>
Remote Subnet	<input type="text" value="*/"/>
Received Interface	<input type="text" value="Ext_sig"/>
Signaling Interface	<input type="text" value="Int_sig"/>
Media Interface	<input type="text" value="Int_med"/>
Secondary Media Interface	<input type="text" value="None"/>
End Point Policy Group	<input type="text" value="Telenor"/>
Routing Profile	<input type="text" value="Telenor"/>
Topology Hiding Profile	<input type="text" value="Session Manager"/>
Signaling Manipulation Script	<input type="text" value="None"/>
Remote Branch Office	<input type="text" value="Any"/>

Finish

7.3.5 Endpoint Flows – For Telenor

Repeat step 1 through 4 from Section 7.3.4, with the following changes:

- **Name:** Telenor.
- **Server Configuration:** Telenor.
- **Received Interface:** Int_sig.
- **Signaling Interface:** Ext_sig.
- **Media Interface:** Ext_sig.
- **End Point Policy Group:** Session Manager.
- **Routing Profile:** Session Manager.
- **Topology Hiding Profile:** Telenor.

Edit Flow: TelenorX

Flow Name	<input type="text" value="Telenor"/>
Server Configuration	<input type="text" value="Telenor"/>
URI Group	<input type="text" value="*/"/>
Transport	<input type="text" value="*/"/>
Remote Subnet	<input type="text" value="*/"/>
Received Interface	<input type="text" value="Int_sig"/>
Signaling Interface	<input type="text" value="Ext_sig"/>
Media Interface	<input type="text" value="Ext_med"/>
Secondary Media Interface	<input type="text" value="None"/>
End Point Policy Group	<input type="text" value="Session Manager"/>
Routing Profile	<input type="text" value="Session Manager"/>
Topology Hiding Profile	<input type="text" value="Telenor"/>
Signaling Manipulation Script	<input type="text" value="None"/>
Remote Branch Office	<input type="text" value="Any"/>

Finish

7.3.6 Session Flows

A session flow must be defined to apply the session policy defined in **Section 7.2.18**. Navigate to **Device Specific Settings → Session Flows** from the menu on the left-hand side (not shown).

1. Click on **Add**.
2. Enter a name in **Flow Name** (e.g., **Telenor**).
3. Select **Telenor** (defined in Section 7.2.18) for **Session Policy**.
4. Check to **Has Remote SBC**.
5. Click on **Finish**.

Add Flow X

Flow Name Telenor

URI Group #1 *

URI Group #2 *

Subnet #1
Ex: 192.168.0.1/24 *

SBC IP Address *

SBC IP Address *

Subnet #2
Ex: 192.168.0.1/24 *

SBC IP Address *

SBC IP Address *

Session Policy Telenor

Has Remote SBC ☒

Finish

8. Verification Steps

The following steps may be used to verify the configuration.

8.1 Avaya Session Border Controller for Enterprise

Log into the Avaya SBCE as shown in **Section 7**. Across the top of the display are options to display **Alarms**, **Incidents**, **Logs**, and **Diagnostics**. In addition, the most recent Incidents are listed in the lower right of the screen.

Protocol Traces

The Avaya SBCE can take internal traces of specified interfaces.

1. Navigate to **Device Specific Settings → Troubleshooting → Trace**.
2. Select the **Packet Capture** tab and select the following:
 - Select the desired **Interface** from the drop down menu (e.g., **All**).
 - Specify the **Maximum Number of Packets to Capture** (e.g., **5000**).
 - Specify a **Capture Filename** (e.g., **TEST.pcap**).
 - Unless specific values are required, the default values may be used for the **Local Address**, **Remote Address**, and **Protocol** fields.
 - Click **Start Capture** to begin the trace.

The screenshot shows the 'Trace: sbce' window with the 'Packet Capture' tab selected. The 'Packet Capture Configuration' section displays the following settings: Status is 'Ready', Interface is 'B1', Local Address is '10.2.2.135', Remote Address is '*', Protocol is 'All', Maximum Number of Packets to Capture is '3000', and Capture Filename is 'test.pcap'. There are 'Start Capture' and 'Clear' buttons at the bottom.

The capture process will initialize and then display the following **In Progress** status window:

The screenshot shows the 'Trace: sbce' window with the 'Packet Capture' tab selected. A blue banner at the top states: 'A packet capture is currently in progress. This page will automatically refresh until the capture completes.' The 'Packet Capture Configuration' section displays the following settings: Status is 'In Progress', Interface is 'B1', Local Address is '10.2.2.135', Remote Address is '*', Protocol is 'All', Maximum Number of Packets to Capture is '3000', and Capture Filename is 'test.pcap'. There is a 'Stop Capture' button at the bottom.

3. Run the test.
4. When the test is completed, select the **Stop Capture** button shown above.
5. Click on the **Captures** tab and the packet capture is listed as a *.pcap* file with the date and time added to filename specified in **Step 2**.
6. Click on the **File Name** link to download the file and use Wireshark to open the trace.

Trace: sbce

Devices
sbce

Packet Capture
Captures

Refresh

File Name	File Size (bytes)	Last Modified	
test_20160405184126.pcap	0	April 5, 2016 6:41:26 PM AEST	Delete

The following section details various methods and procedures to help diagnose call failure or service interruptions. As detailed in previous sections, the demarcation point between the Telenor SIP Trunk service and the customer SIP PABX is the customer SBC.

On either side of the SBC, various diagnostic commands and tools may be used to determine the cause of the service interruption. These diagnostics can include:

- Ping from the SBC to the network gateway.
- Ping from the SBC to DNS.
- Note any Incidents or Alarms on the Dashboard screen of the SBC.

Diagnostics

AVAYA

Devices
sbce

Full Diagnostic
Ping Test

Start Diagnostic

Task Description	Status
✓ EMS Link Check	M1 is operating within normal parameters with a full duplex connection at 1Gb/s.
✓ SBC Link Check: A1	A1 is operating within normal parameters with a full duplex connection at 1Gb/s.
✓ SBC Link Check: B1	B1 is operating within normal parameters with a full duplex connection at 1Gb/s.
✓ Ping: SBC (A1) to Gateway (10.128.197.1)	Average ping from 10.128.197.22 [A1] to 10.128.197.1 is 0.288ms.
✗ Ping: SBC (A1) to Primary DNS (8.8.8.8)	Error: Unable to reach 8.8.8.8 from 10.128.197.22 [A1].
✓ Ping: SBC (B1) to Gateway (103.199.6.17)	Average ping from 103.199.6.29 [B1] to 103.199.6.17 is 2.445ms.
✓ Ping: SBC (B1) to Primary DNS (8.8.8.8)	Average ping from 103.199.6.29 [B1] to 8.8.8.8 is 43.468ms.

Incident Viewer

AVAYA

Device

All

 Category

All

Clear Filters

Refresh

Generate Report

Displaying results 1 to 15 out of 44.

Type	ID	Date	Time	Category	Device	Cause
Server Heartbeat	729881580397602	4/4/16	7:46 PM	Policy	sbce	Heartbeat Successful, Server is UP
Server Heartbeat	729881580396121	4/4/16	7:46 PM	Policy	sbce	Heartbeat Successful, Server is UP
Server Heartbeat	729881580393451	4/4/16	7:46 PM	Policy	sbce	Heartbeat Successful, Server is UP
Server Heartbeat	729881402194116	4/4/16	7:40 PM	Policy	sbce	Heartbeat Successful, Server is UP

8.2 Avaya CS1000

SIP Trunk monitoring (ld 32): Place an inbound call from PSTN to an Avaya CS1000 phone. Then check the SIP trunk status by using ld 32, and verify one trunk is BUSY.

```
>ld 32
NPR000
.stat 92 0
009 UNIT(S) IDLE
001 UNIT(S) BUSY
000 UNIT(S) DSBL
000 UNIT(S) MBSY
```

After the call is released, check that SIP trunk status. It should change to the IDLE state.

```
>ld 32
NPR000
.stat 92 0
010 UNIT(S) IDLE
000 UNIT(S) BUSY
000 UNIT(S) DSBL
000 UNIT(S) MBSY
```

8.3 Avaya Aura® Session Manager Status

The Session Manager configuration may be verified via System Manager.

1. Using the procedures described in **Section 6**, access the System Manager GUI. From the **Home** screen, under the **Elements** heading, select **Session Manager**.

Home / Elements / Session Manager / Dashboard [Help ?](#)

Session Manager Dashboard

This page provides the overall status and health summary of each administered Session Manager.

Session Manager Instances

Service State: ▼ Shutdown System: ▼ As of 11:25 AM

1 Item [Show](#) All ▼ Filter: Enable

<input type="checkbox"/>	Session Manager	Type	Tests Pass	Alarms	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Data Replication	User Data Storage Status	License Mode	Version
<input type="checkbox"/>	sm01	Core	✓	0/0/0	Up	Accept New Service	2/4	0	0/0	✓	✓	Normal	7.0.1.1.701114

Select : All, None

2. The Session Manager Dashboard is displayed. Note that the **Test Passed**, **Alarms**, **Service State**, and **Data Replication** columns.
3. Clicking on the **2/4** entry in the **Entity Monitoring** column, results in the following display:

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: [sm01](#)

Summary View

Status Details for the selected Session Manager:

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

<input type="radio"/>	SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input type="radio"/>	cs1k	100.20.2.197	5060	TLS	FALSE	UP	200 OK	UP
<input type="radio"/>	sbce-A1	10.128.197.22	5060	TLS	FALSE	UP	486 Busy Here	UP
<input type="radio"/>	aam	100.20.2.167	5060	TCP	FALSE	DOWN	500 Server Internal Error: Destination Unreachable	DOWN
<input type="radio"/>	cm-simplex	100.20.2.166	5061	TLS	FALSE	DOWN	500 Service Unavailable (no media resources)	DOWN

8.4 Telephony Services

1. Place inbound/outbound calls, answer the calls, and verify that two-way talk path exists. Verify that the call remains stable for several minutes and disconnects properly.
2. Verify basic call functions such as hold, transfer, and conference.
3. Verify the use of DTMF signaling.

9. Conclusion

As illustrated in these Application Notes, Avaya Communication Server 1000 Release 7.6 SP8, Avaya Aura® Session Manager Release 7.0.1 SP1, and Avaya Session Border Control for Enterprise Release 7.1 SP1 can be configured to interoperate successfully with Telenor SIP Trunk service. This solution allows enterprise users access to the PSTN using the Telenor SIP Trunk service connection. Please refer to **Section 2.2** for exceptions.

10. Additional References

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

- [1] *Deploying Avaya Aura® System Manager Release 7.0.1.*
- [2] *Administering Avaya Aura® System Manager for Release 7.0.1.*
- [3] *Administering Avaya Aura® Session Manager Release 7.0.1.*
- [4] *Deploying Avaya Aura Session Manager Release 7.0.1.*
- [5] *Deploying Avaya SBCE on VMware in Virtualized Environment Release 7.1.*
- [6] *Administering Avaya Session Border Controller Release 7.1.*
- [7] *Document Collection - Communication Server 1000 Release 7.6.*
- [8] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [9] *RFC 3515, The Session Initiation Protocol (SIP) Refer Method*, <http://www.ietf.org/>
- [10] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>

Product documentation for Telenor SIP Trunk service is available from Telenor.

©2017 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.