



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring MTS Allstream SIP Trunking with Avaya Communication Server 1000 Release 7.5, Avaya Aura® Session Manager Release 6.1 and Avaya Aura® Session Border Controller Release 6.0 – Issue 1.0

Abstract

These Application Notes describe a solution comprised of Avaya Communication Server 1000 release 7.5 and MTS Allstream SIP Trunking. During the interoperability testing, Avaya Communication Server 1000 was able to interoperate with the MTS Allstream system via SIP trunk. This test was performed to verify SIP trunk features including basic call, call forward (all calls, busy, no answer), call transfer (blind and consult), conference, and voice mail. The calls are placed in both directions with various set types.

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

1. Introduction

This document provides a typical network configuration deployment of Avaya Communication Server 1000 (hereafter referred to as CS1000) and MTS Allstream SIP Trunking (hereafter referred to as MTS Allstream system). During the interoperability testing, all SIP trunk applicable feature test cases were executed to ensure the interoperability between MTS Allstream system and Avaya CS1000.

2. General Test Approach and Test Results

CS1000 release 7.5 was connected to Avaya Aura[®] Session Border Controller (hereafter referred to as AA-SBC) via Avaya Aura[®] Session Manager. AA-SBC was connected to the MTS Allstream system via SIP trunk. Various call types were made from CS1000 to the MTS Allstream system and vice versa to ensure the interoperability between CS1000 and the MTS Allstream system.

2.1. Interoperability Compliance Testing

The focus of this testing is to verify that CS1000 release 7.5 can interoperate with the MTS Allstream system. The following interoperability areas were covered.

- General call processing between CS1000 and MTS Allstream including:
 - Codec (G.711 u-law/ G.729/ptime 20ms, VAD disabled)
 - Hold/Retrieve on both ends
 - Music On Hold
 - CLID displays
 - Ring-back tone
 - Speech paths
 - Dialing plan support
 - Advanced features (Call on Mute, Call Park, Call Waiting)
 - Abandoned Call
- Call redirection verification: all supported methods (blind transfer, consultative transfer, call forward, and conference) including CLID. Call redirection is performed from both ends
- RFC2833/DTMF on both direction
- SIP Transport UDP
- Thru dialing via PBX Call Pilot
- Voice Mail Server CallPilot (hosted on Avaya system)
- Fax Transmission: fax was transmitted from both ends with codec G.711.
- Early Media Transmission.
- Static Registration

2.2. Test Results

The objectives outlined in **Section 2.1** were verified. All the applicable test cases were executed. However, the following observations were noted during the compliance testing:

1. For outbound calls from CS1000 to PSTN, MTS Allstream did not offer alternate CLID-Name and CLID-Number delivery.
 - Call scenario: Make an outbound SIP call from a CS1000 phone to a PSTN phone.
 - SIP observation: CS1000 sent "From" header with CLID-Name and CLID-Number.
 - Expected result: The call is established with 2 way speech paths. CLID Number and Name are displayed correctly.
 - Actual result: MTS Allstream did not modify CLID-Name provided by CS1000.
 - Recommendation: The CLID-Name from CS1000 should be verified and alternated by MTS Allstream. However, MTS Allstream currently passes through CLID provided by customer. There is no resolution available at this time.
2. Outbound E911 calls from CS1000 to PSTN are not supported by MTS Allstream.
 - Call scenario: Make an outbound 911 SIP call from a CS1000 phone.
 - SIP observation: N/A.
 - Expected result: The call is established with 2 way speech paths. The CLID Name/ Number and location information are displayed correctly on PSAT.
 - Actual result: N/A.
 - Resolution: Allstream did not support outbound E911 calls. There is no available resolution at this time.
3. For inbound toll free calls, the CLID Name was not delivered to CS1000.
 - Call scenario: Make an inbound SIP call from a PSTN phone to a CS1000 toll free number.
 - SIP observation: MTS Allstream translated inbound toll free calls to a DID number to send to CS1000 over SIP Trunks.
 - Expected result: Calls are established with 2 way speech paths. CLID Number and Name are displayed correctly.
 - Actual result: the call was established with good RTPs, CS1000 phones displayed the CLID Number, but the CLID Name was not delivered to CS1000.
 - Resolution: There is no available resolution at this time.
4. Outbound calls from CS1000 to PSTN with "Privacy: user" to hide CLID-Name, but MTS Allstream still delivers CLID-Name to PSTN.
 - Call scenario: Make an outbound SIP call from a CS1000 phone to a PSTN phone with "Privacy: user".
 - SIP observation: CS1000 sent "Privacy: user" header to MTS Allstream.
 - Expected result: Calls are established with 2 way speech paths. PSTN either does not display CLID Name of CS1000 phones or displays "private" or "anonymous", but it still is able to display CLID Number.
 - Actual result: CLID-Name was still being displayed at PSTN phones.

- Recommendation: MTA Allstream does not support “Privacy:user”. Thus, in order to hide CLID-Name, CS1000 should send CLID-Name “Anonymous” and “Privacy:none” to MTS Allstream system.
5. Recorded announcement lost about 3 seconds when PSTN phone calls to Voicemail hosted on CS1000.
 - Call scenario: Make a SIP call from PSTN to Voicemail DN hosted on CS1000.
 - SIP observation: CS1000 sent 180/SDP to transmit the early media for announcement.
 - Expected result: The recorded announcement is fully (in length) transmitted to PSTN.
 - Actual result: The early media was lost for about 3 seconds. First 3 seconds (of the recorded message) are not heard when the call goes to Voicemail.
 - Resolution: Known issue against Avaya CS1000 and there is no resolution available at this time.
 6. MTS Allstream could not offer codec order G.711, G.729.
 - Call scenario: Make an inbound SIP call from PSTN to CS1000 which has codec profile G.711, G.729 in order.
 - SIP observation: N/A.
 - Expected result: Calls are established with 2 way speech paths using the preferred codec. CLID Number and Name are displayed correctly.
 - Actual result: N/A
 - Resolution: MTS Allstream cannot offer codec order G.711, G.729 for testing. Thus codec negotiation with codec order G.711, G.729 offered by MTS Allstream has not being verified. There is no resolution available at this time.
 7. CS1000 phone held/ retrieved an outgoing call causing the display to be changed.
 - Call scenario: Make a SIP call from a CS1000 phone to PSTN, and perform “hold/ retrieve”.
 - SIP observation: N/A
 - Expected result: Calls are established with 2 way speech paths. Number and Name are displayed correctly with “hold/ retrieve” action.
 - Actual result: After retrieving the call, the telephone number previously displayed on CS1000 phones will be unavailable and replaced by Route ACOD – Trunk Channel ID.
 - Resolution: This is a known CS1000 issue and there is no resolution available at this time.

2.3. Support

For technical support on MTS Allstream, please contact MTS Allstream technical support at:

- Phone: 204-941-8557 or 1-800-542-8703
- Email: mts.special.needs@mts.ca
- Website: <http://www.mts.ca/mts/personal/support>

3. Reference Configuration

Figure 1 illustrates the test configuration used during the compliance testing between CS1000 and MTS Allstream.

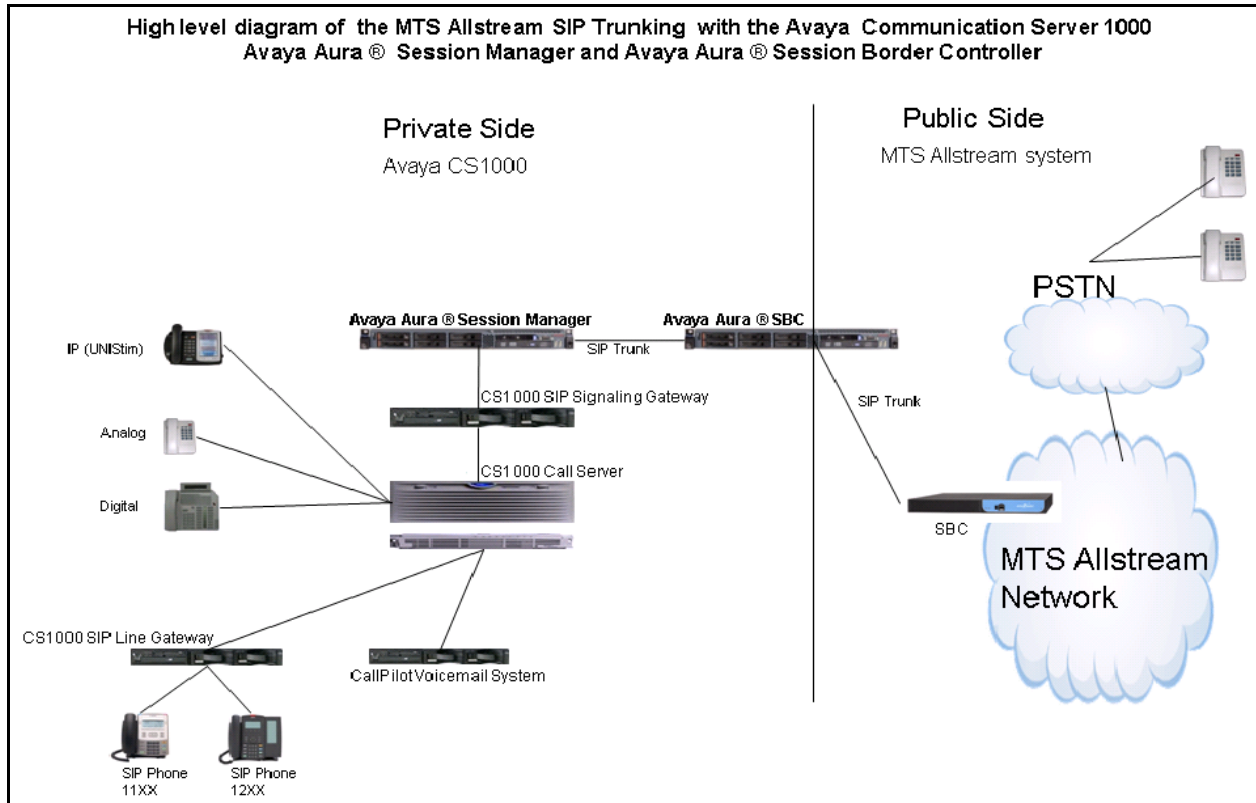


Figure 1- Network Diagram for Avaya CS1000 – MTS Allstream system

The following assumptions were made for this lab test configuration.

1. CS1000 R7.5 software and implementation of latest patches
2. MTS Allstream provides support to setup, configure, and troubleshoot on carrier switch for the duration of the testing.

During testing, the following activities were made to each test scenario:

1. Calls were checked for the correct call progress tones and cadences.
2. During the ringing state, the ring back tone and destination ringing were checked.
3. Calls were checked in both hands-free and handset mode due to internal Avaya requirement.
4. Calls were checked for speech path in both directions using spoken words to ensure clarity of speech.
5. The display(s) of the sets/clients involved were checked for consistent and expected CLID, name and redirection information both prior to answer and after call establishment.

6. The speech path and messaging system were observed for timely and quality End to End tone audio path generation and application responses.
7. The call server maintenance terminal window was used for the monitoring of BUG(s), ERR and AUD messages.
8. Speech path and display checked before and after calls were put on/off hold from each end.
9. Applicable files were screened on an hourly basis during the testing for messages that may indicate technical issues. This refers to Avaya PBX files.
10. Calls were checked to ensure that all resources such as Virtual trunks, TDM trunks, Sets and VGWs are released when a call scenario ends.

4. Equipment and Software Validated

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

Avaya system:

System	Software/Loadware version
Avaya CS1000 7.5 (CPPM)	<ul style="list-style-type: none"> ● Call Server: 7.50 Q GA plus latest DEPLIST – Issue: 01 Release: x2107.50, 2011-07-19 11:40:08 (est) ● SSG Server: 7.50.17 GA plus latest Service_Pack_Linux_7.50_17_20110719.ntl ● SLG Server: 7.50.17 GA plus latest Service_Pack_Linux_7.50_17_20110719.ntl
Avaya phones	<ul style="list-style-type: none"> ● 2002 p2: 0604DCJ (UNISim) ● 2004 p2: 0604DCJ (UNISim) ● 1140: 0625C6O (UNISim) ● 1120: 0624C6O (UNISim) ● 2007: 0621C6M (UNISim) ● 1220: 062AC6O (UNISim) ● SIP 1120, 1140: SIP12x0e04.00.04.00 ● SIP 1220,1240: SIP12x0e04.00.04.00
Avaya Aura [®] Session Border Controller	<ul style="list-style-type: none"> ● SBCT 6.0.2.0.3 (sbc E362P4)

MTS Allstream system:

System	Software/Loadware version
Genband S3	<ul style="list-style-type: none"> ● Release 5.2.2.12
CS2K	<ul style="list-style-type: none"> ● CVM13

The output of “dstat” command on Call Server:

<pre>pdt> dstat Call Server: -----</pre>

```
DepList name: core
  Filename: /var/opt/nortel/cs/fs/u/patch/deplist/mcore_01.cpl
  Issue : 01
  Release : x2107.50
  Created : 2011-07-19 11:40:08 (est)
  Number of patches: 60
  Patches Loaded: 60
  Patches In-service: 60
pdt>
```

The output of “pstat” command on SSG Server:

```
[admin@car2-mas ~]$ pstat
Product Release: 7.50.17.00
In system patches: 0

In System service updates: 10
PATCH# IN_SERVICE DATE SPECINS REMOVABLE NAME
0 Yes 07/01/11 NO YES cs1000-baseWeb-7.50.17.01-1.i386.000
1 Yes 11/05/11 NO YES cs1000-sps-7.50.17-01.i386.000
2 Yes 25/08/11 NO YES cs1000-patchWeb-7.50.17.16-1.i386.000
4 Yes 11/05/11 NO YES cs1000-shared-pbx-7.50.17-01.i386.000
5 Yes 11/05/11 NO YES cs1000-dbcom-7.50.17-02.i386.000
7 Yes 06/07/11 NO YES cs1000-vtrk-7.50.17.16-02.i386.000
9 Yes 06/07/11 NO YES cs1000-linuxbase-7.50.17.16-1.i386.000
10 Yes 06/07/11 NO YES cs1000-dmWeb-7.50.17.16-1.i386.000
11 Yes 06/07/11 NO YES cs1000-tps-7.50.17.16-4.i386.000
12 Yes 06/07/11 YES YES cs1000-Jboss-Quantum-7.50.17.16-4.i386.000
[admin@car2-mas ~]$
```

5. Avaya Communication Server 1000 Configuration

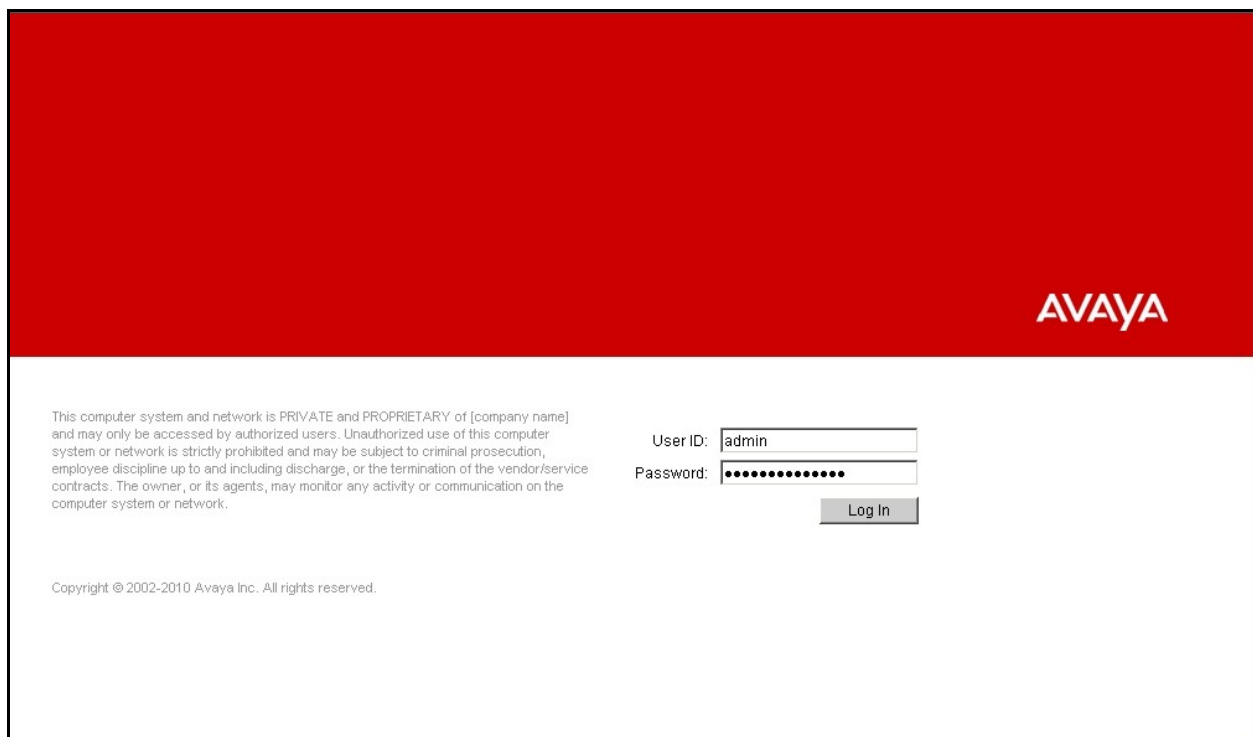
These Application Notes assume that the basic configuration has already been administered. For further information on Avaya Communications Server 1000, please consult references in **Section 9**.

The following sections describe the configuration details of CS1000 with a SIP trunk to the MTS Allstream system.

5.1. Login to CS1000 System

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

a) Open an instance of a web browser and connect to the UCM GUI at the following address: `http://<UCM IP address>` as shown in **Figure 2**. Log in using an appropriate Username and Password.



This computer system and network is PRIVATE and PROPRIETARY of [company name] and may only be accessed by authorized users. Unauthorized use of this computer system or network is strictly prohibited and may be subject to criminal prosecution, employee discipline up to and including discharge, or the termination of the vendor/service contracts. The owner, or its agents, may monitor any activity or communication on the computer system or network.

User ID:

Password:

Copyright © 2002-2010 Avaya Inc. All rights reserved.

Figure 2 – Login Unified Communications Management

b) The **Unified Communications Management** screen is displayed. Click on the **Element Name** of the CS1000 Element as highlighted in the red box as shown in **Figure 3**.

Avaya Unified Communications Management

Host Name: car2-sipl-ucm.bvwdev.com Software Version: 02.20.0009.01(3993) 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 EM on car2-cores	CS1000	7.5	135.10.97.90	New element.
2 EM on car2-ssq-carrier	CS1000	7.5	135.10.97.90	New element.
3 EM on cpppm3	CS1000	7.5	135.10.97.78	New element.
4 cpppm3.bvwdev.com (member)	Linux Base	7.5	135.10.97.150	Base OS element.
5 car2-mas.bvwdev.com (member)	Linux Base	7.5	135.10.97.171	Base OS element.
6 car2-sipl-ucm.bvwdev.com (primary)	Linux Base	7.5	135.10.97.163	Base OS element.
7 sipl75.bvwdev.com (member)	Linux Base	7.5	135.10.97.136	Base OS element.
8 car2-ssq2.bvwdev.com (member)	Linux Base	7.5	135.10.97.157	Base OS element.
9 car2-sps.bvwdev.com (member)	Linux Base	7.5	135.10.97.172	Base OS element.
10 car2-ssq-carrier.bvwdev.com (member)	Linux Base	7.5	135.10.97.167	Base OS element.

Figure 3 – Unified Communications Management

c) The CS1000 Element Manager **System Overview** page is displayed as shown in **Figure 4**.

CS1000 Element Manager

Managing: 10.10.97.90 Username: admin System Overview

System Overview

IP Address: 10.10.97.90
Type: Avaya Communication Server 1000E CPPM Linux
Version: 4121
Release: 750 Q. +

Copyright © 2002-2011 Avaya Inc. All rights reserved.

Figure 4 – Element Manager System Overview

5.1.2. Login to Call Server Command Line Interface (CLI)

- a) Using Putty, SSH to the IP address of the SSG Server with the admin account.
- b) Run the command “cslogin” and login with the appropriate admin account and password.
- c) Here are the logs.

```
login as: admin

      Avaya Inc. Linux Base 7.50
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@110.10.97.168's password:
Last login: Thu Mar 10 17:38:16 2011 from 110.10.97.172

/usr/bin/xauth: creating new authority file /home/admin/.Xauthority
[admin@car2-ssg-carrier ~]$ cslogin

SEC054 A device has connected to, or disconnected from, a pseudo tty without authenticating
login
USERID? admin
PASS?
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 logout immediately. This system may be monitored for
operational purposes at any time.

.
TTY #09 LOGGED IN ADMIN 17:42 10/3/2011

>
```

5.2. Administer a Node IP Telephony

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

5.2.1. Obtain Node IP address

These Application Notes assume that the basic configuration has already been administered and that a Node has already been created. This section describes the steps for configuring a Node (Node ID 2004) in the CS1000 IP network to work with MTS Allstream system. For further information on Avaya Communications Server 1000, please consult reference in **Section 9**.

a) Select **System -> IP Network -> Nodes: Servers, Media Cards**. **Figure 5** displays the **IP Telephony Nodes** page. Click on the Node ID of the CS1000 Element.

AVAYA **CS1000 Element Manager**

Managing: 110.10.97.90 Username: admin
System » IP Network » IP Telephony Nodes

IP Telephony Nodes

Click the Node ID to view or edit its properties.

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

<input type="checkbox"/> Node ID	Components	Enabled Applications	ELAN IP	Node/TLAN IPv4	Node/TLAN IPv6	Status
<input type="checkbox"/> 2000	1	LTPS, Gateway (SIPGw)	-	110.10.97.168		Synchronized
<input type="checkbox"/> 2001	1	LTPS, Gateway (SIPGw)	-	110.10.97.170		Synchronized
<input type="checkbox"/> 2002	1	SIP Line	-	110.10.97.164		Synchronized
<input type="checkbox"/> 2003	1	LTPS, Gateway (SIPGw)	-	110.10.97.158		Synchronized
<input type="checkbox"/> 2004	1	LTPS, Gateway (SIPGw)	-	110.10.97.190		Synchronized

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

Figure 5 – IP Telephony Nodes

b) The **Node Details** screen is displayed in **Figure 6** with the IP address of the CS1000 node. The **Node IP Address** is a virtual address which corresponds to the TLAN IP address of the SIP Signaling Gateway. The SIP Signaling Gateway uses this **Node IP Address** to communicate with other components to process the SIP call.

AVAYA CS1000 Element Manager

Managing: 110.10.97.90 Username: admin
System » IP Network » IP Telephony Nodes » Node Details

Node Details (ID: 2004 - LTPS, Gateway (SIPGw))

Embedded LAN (ELAN)

Gateway IP address: 110.10.97.65 *

Subnet mask: 255.255.255.192 *

Telephony LAN (TLAN)

Node IPv4 address: 110.10.97.190 *

Subnet mask: 255.255.255.192 *

Node IPv6 address:

IP Telephony Node Properties

- Voice Gateway (VGW) and Codecs
- Quality of Service (QoS)
- LAN
- SNTP
- Numbering Zones

Applications (click to edit configuration)

- SIP Line
- Terminal Proxy Server (TPS)
- Gateway (SIPGw)
- Personal Directories (PD)
- Presence Publisher

* Required Value.

Associated Signaling Servers & Cards

Select to add Add Remove Make Leader Print Refresh

Hostname	Type	Deployed Applications	ELAN IP	TLAN IPv4	Role
car2-mas	Signaling_Server	LTPS, Gateway, PD, Presence Publisher, IP Media Services	110.10.97.91	110.10.97.171	Leader

Show: ☐ IPv6 address

Note: Only server(s) that are not part of any other IP telephony node and deployed application(s) that match the service(s) selected for this node are available in the servers list .

Figure 6 –Node Details

5.2.2. Administer TPS

c) Continue from **Section 5.2.1**. On the **Node Details** page, select the **Terminal Proxy Server (TPS)** link as shown in **Figure 6**.

d) Check the **UNISTim Line Terminal Proxy Server** check box and then click **Save** as shown in **Figure 7**.

AVAYA CS1000 Element Manager

Managing: 110.10.97.90 Username: admin
System » IP Network » IP Telephony Nodes » Node Details » UNISTim Line Terminal Proxy Server (LTPS) Configuration

Node ID: 2004 - UNISTim Line Terminal Proxy Server (LTPS) Configuration Details

Firmware | DTLS | Network Connect Server

UNISTim Line Terminal Proxy Server: ☒ Enable proxy service on this node

Firmware

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

DTLS

DTLS policy: Off
Options: ☐ Client authentication
☐ Periodic re-keying

Network Connect Server

Primary network connect server (TL &N) 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**

Figure 7 – TPS Configuration Details

5.2.3. Administer Quality of Service (QoS)

e) Continue from **Section 5.2.1**. On the **Node Details** page, select the **Quality of Service (QoS)** link as shown in **Figure 6**.

f) The default Diffserv values are as shown in **Figure 8**. Click the **Save** button.

AVAYA **CS1000 Element Manager**

Managing: 110.10.97.90 Username: admin
System > IP Network > IP Telephony Nodes > Node Details > Quality of Service (QoS)

Node ID: 2004 - Quality of Service (QoS)

Diffserv Codepoint (DSCP)

Enable Avaya automatic QoS: ☐

Control packets: 40 (0-63)

Voice packets: 46 (0-63)

VLAN tagging: ☐ 802.1Q support

802.1Q bits value (802.1P): 5 (0-7)

* Required Value.

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

Save **Cancel**

Figure 8 – QoS Configuration Details

5.2.4. Synchronize the New Configuration

g) Continue from **Section 5.2.3**, return to the **Node Details** page (**Figure 6**) and click on the **Save** button.

h) The **Node Saved** screen is displayed. Click on the **Transfer Now** (not shown).

i) The **Synchronize Configuration Files** screen is displayed. Check the Signaling Server check box and click on the **Start Sync** (not shown).

j) When the synchronization completes, check the Signaling Server check box and click on the **Restart Applications** (not shown).

5.3. Administer Voice Codec

5.3.1. Enable Voice Codec, Node IP Telephony.

- Select **IP Network -> Nodes: Servers, Media Cards -> Configuration** from the left pane, and in the **IP Telephony Nodes** screen, select the **Node ID** of the CS1000 system. The **Node Details** screen is displayed. (See in **Section 5.2.1** for more detail).
- On the **Node Details** page as shown in **Figure 6**, click on **Voice Gateway (VGW) and Codec**.
- The MTS Allstream SIP Trunk supports voice codec G.729 and G.711 as fallback, payload size 20 ms, with VAD disabled. **Figures 9a** and **9b** show voice codec profile configured on CS1000.

AVAYA CS1000 Element Manager

Managing: 110.10.97.90 Username: admin
System » IP Network » IP Telephony Nodes » Node Details » VGW and Codecs

Node ID: 2004 - Voice Gateway (VGW) and Codecs

General | Voice Codecs | Fax

Voice Codecs

Codec G711: ☒ Enabled (required)
Voice payload size: 20 (milliseconds per frame)
Voice playout (jitter buffer) delay: 40 80 (milliseconds)
Nominal Maximum
Maximum delay may be automatically adjusted based on nominal settings.
☐ Voice Activity Detection (VAD)

Codec G722: ☐ Enabled
Voice payload size: 20 (milliseconds per frame)
Voice playout (jitter buffer) delay: 40 80 (milliseconds)
Nominal Maximum
Maximum delay may be automatically adjusted based on nominal settings.

Codec G729: ☒ Enabled
Voice payload size: 20 (milliseconds per frame)

* Required Value.

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

Save Cancel

Figure 9a – Voice Codec G.711 Configuration Details

AVAYA CS1000 Element Manager

Managing: 110.10.97.90 Username: admin
System » IP Network » IP Telephony Nodes » Node Details » VGW and Codecs

Node ID: 2004 - Voice Gateway (VGW) and Codecs

General | Voice Codescs | Fax

Codec G729: ☒ Enabled
Voice payload size: 20 (milliseconds per frame)
Voice playout (jitter buffer) delay: 40 80 (milliseconds)
Nominal Maximum
Maximum delay may be automatically adjusted based on nominal settings.
☐ Voice Activity Detection (VAD)
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

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

Figure 9b – Voice Codec G.729 Configuration Details

d) For Fax over IP, MTS Allstream supports G.711 as default and does not support T.38. Even though CS1000 does not have an option to disable T.38, it is still capable to use G.711 for fax calls. **Figure 9c** shows **Modem Pass Through** was selected for Node 2004; this configuration enables codec G.711 to be used to transmit or receive fax calls between CS1000 and MTS Allstream.

AVAYA CS1000 Element Manager

Managing: 110.10.97.90 Username: admin
System » IP Network » IP Telephony Nodes » Node Details » VGW and Codecs

Node ID: 2004 - 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 (squellch 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: 40 160 (milliseconds)

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

Figure 9c – Fax Codec G.711 Configuration Details

e) Click **Save**.

f) Synchronize the new configuration (please refer to **Section 5.2.4** for more detail).

5.3.2. Enable Voice Codec on Media Gateways.

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

a) From the left menu of the Element Manager page in **Figure 6**, select the **IP Network** -> **Media Gateways** menu item. The Media Gateways page will appear (not shown). Click on **MGC** which is located on the right of the page.

b) The MTS Allstream SIP Trunk supports voice codec G.729 and G.711 as fallback, payload size 20 ms, with VAD disabled. **Figure 10a** shows codec profile configured for Media Gateway.

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 (NAT)
 - QoS Thresholds
 - Personal Directories
 - Unicode Name Directory
 - + Interfaces
 - Engineered Values
 - + Emergency Services
 - + Geographic Redundancy
 - + Software
 - Customers
 - Routes and Trunks

- Codec G711 **Select** ☒

Codec name G711

Voice payload size 20 (ms/frame)

Voice playout (jitter buffer) nominal delay 40

Modifications may cause changes to dependent settings

Voice playout (jitter buffer) maximum delay 80

Modifications may cause changes to dependent settings

VAD ☐

- Codec G729A **Select** ☒

Codec name G729A

Voice payload size 20 (ms/frame)

Voice playout (jitter buffer) nominal delay 40

Modifications may cause changes to dependent settings

Voice playout (jitter buffer) maximum delay 80

Modifications may cause changes to dependent settings

VAD ☐

Figure 10a – Media Gateways G.729 and G.711 Configuration Details

c) For Fax over IP, MTS Allstream supports G.711 as default and does not support T.38. Even though CS1000 does not have an option to disable T.38, it is still capable to use G.711 for fax calls. **Figure 10b** shows **Modem Pass Through** was selected for Media Gateway; this configuration enables codec G.711 to be used to transmit or receive fax call between CS1000 and MTS Allstream.

AVAYA CS1000 Element Manager

- 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)
- Rfactor calculation ☐
- DTMF tone detection ☒
- Enable low latency mode ☐
- Remove DTMF delay (squench 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	Select	<input checked="" type="checkbox"/>
+ Codec	G729A	Select	<input checked="" type="checkbox"/>
+ Codec	G723.1	Select	<input type="checkbox"/>
+ Codec	T38 FAX	Select	<input checked="" type="checkbox"/>
+ QoS			

Figure 10b – Media Gateways ModemPassThrough (G.711) Configuration Details

5.4. Administer Zones and Bandwidth

This section describes the steps to create 2 zones: zone 10 for VGW and IP phones, and zone 255 for IP SIP Trunk.

5.4.1. Create a zone for IP phones (zone 10)

The following figures show how to configure a zone for IP sets and VGW for bandwidth management purposes. The bandwidth strategy can be adjusted to preference.

a) Select **IP Network** -> **Zones** configuration from the left pane, click on the **Bandwidth Zones** as shown in **Figure 11**.

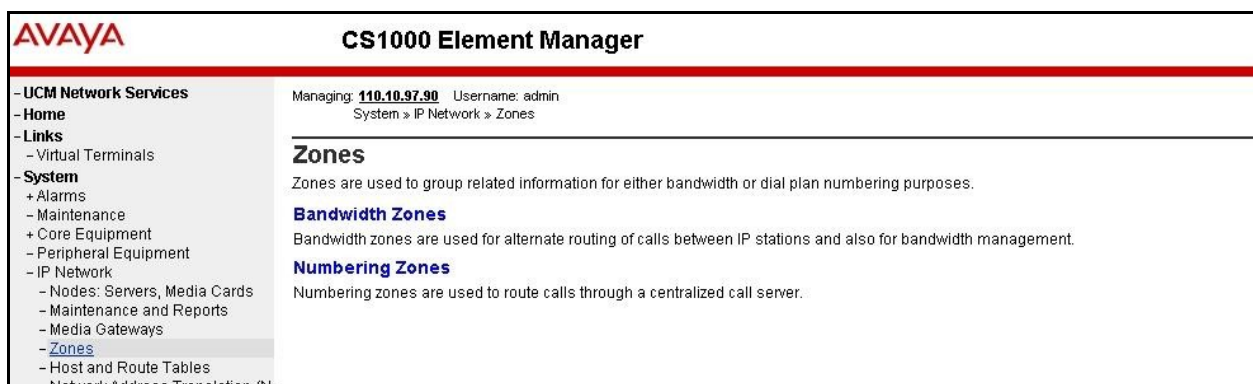


Figure 11 –Zones Page

b) The **Bandwidth Zones** screen is displayed as shown in **Figure 12**. Click **Add**.

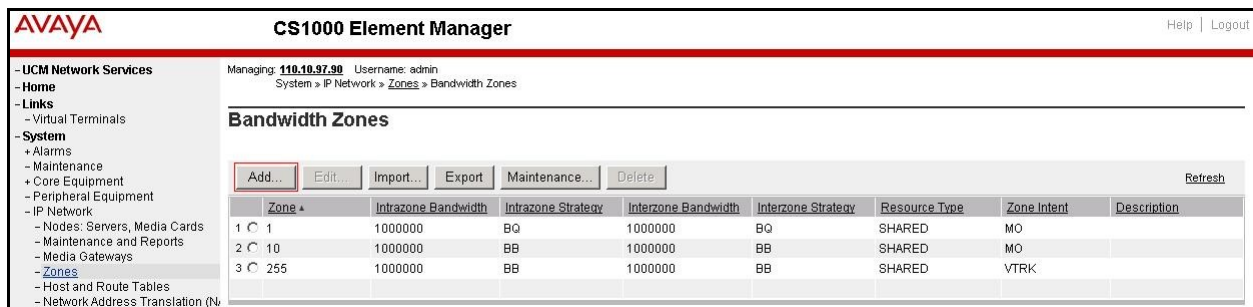


Figure 12 –Bandwidth Zones

c) In the **Add Bandwidth Zone** screen (not shown), click on **Zone Basic Property and Bandwidth Management**, select the values as shown (in red box) in **Figure 13**, and click on the **Submit** button.

- **INTRA_STGY**: bandwidth configuration for local calls.
- **INTER_STGY**: bandwidth configuration for the calls over trunk.
- **BQ**: G711 is first choice and G729 is second choice.
- **BB**: G729 is first choice and G711 is second choice.
- **MO**: is used for IP phones, VGW
- **VTRK**: is used for virtual trunk.

The MTA Allstream SIP Trunk support G.729 as the first choice, G.711 as fallback. So the **MO** Zone 10 was configured with **Strategy Best Bandwidth (BB)**.

Input Description	Input Value
Zone Number (ZONE):	10 * (1 - 8000)
Intrazone Bandwidth (INTRA_BW):	1000000 (0 - 10000000)
Intrazone Strategy (INTRA_STGY):	Best Bandwidth (BB)
Interzone Bandwidth (INTER_BW):	1000000 (0 - 10000000)
Interzone Strategy (INTER_STGY):	Best Bandwidth (BB)
Resource Type (RES_TYPE):	Shared (SHARED)
Zone Intent (ZBRN):	MO (MO)
Description (ZDES):	

Submit Refresh Cancel

Figure 13 –Bandwidth Management Configuration Details– IP phone

5.4.2. Create a zone for virtual SIP trunk (zone 255)

Follow **Section 5.4.1** to create a zone for the virtual trunk. The difference is in the **Zone Intent (ZBRN)** field. Select **VTRK** for virtual trunk (**Figure 14**) and then click on the **Submit** button.

The MTS Allstream SIP Trunk support G.729 as the first choice, G.711 as fallback. So the **VTRK Zone 255** was configured with **Strategy Best Bandwidth (BB)**.

AVAYA CS1000 Element Manager

Managing: **110.10.97.90** Username: admin
System » IP Network » Zones » Bandwidth Zones » Bandwidth Zones 255 » Edit Bandwidth Zone » Zone Basic Property and Bandwidth Management

Zone Basic Property and Bandwidth Management

Input Description	Input Value
Zone Number (ZONE):	255 * (1 - 8000)
Intrazone Bandwidth (INTRA_BW):	1000000 (0 - 10000000)
Intrazone Strategy (INTRA_STGY):	Best Bandwidth (BB) ▼
Interzone Bandwidth (INTER_BW):	1000000 (0 - 10000000)
Interzone Strategy (INTER_STGY):	Best Bandwidth (BB) ▼
Resource Type (RES_TYPE):	Shared (SHARED) ▼
Zone Intent (ZBRN):	VTRK (VTRK) ▼
Description (ZDES):	

Submit **Refresh** **Cancel**

Figure 14 –Bandwidth Management Configuration Details– Virtual Trunk

5.5. Administer SIP Trunk Gateway

This section describes the steps for establishing a SIP IP connection between SIP Signalling Gateway (SSG) to Session Manager.

5.5.1. Integrated Services Digital Network (ISDN)

a) Select **Customers** in the left pane. The **Customers** screen is displayed. Click on the link associated with the appropriate customer, in this case **04**. The system can support more than one customer with different network settings and options. The **Customer 04 Edit** page will appear (not shown). Select the **Feature Packages** option from this page.

b) The screen is updated with a list of **Feature Packages** populated. Select **Integrated Services Digital Network** to edit its parameters. The screen is updated with parameters populated below **Integrated Services Digital Network**. Check the **Integrated Services Digital Network (ISDN)** checkbox, and retain the default values for all remaining fields (**Figure 15**). Scroll down to the bottom of the screen, and click on the **Save** button at the bottom of the page.

AVAYA CS1000 Element Manager

Package: 145

- Integrated Services Digital Network
+ Dial Access Prefix on CLID table entry option

Integrated Services Digital Network: ☒

- Virtual private network identifier: 4 (1 - 16383)

- Private network identifier: 4 (1 - 16383)

- Node DN: 2004

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

Business sub group consult-only: 65535 (0 - 65535)

Prefix 1:

Prefix 2:

Home number plan area code: (200 - 999)

Prefix for central office: (100 - 9999)

Home location code: (100 - 99999999)

Local steering code:

Calling number type: CLID feature displays the set's Prime DN

Redirection count for ISDN calls: 5

CLID information for incoming/outgoing calls: No manipulation is done

Public service telephone networks: ☐

+ Flexible Services **Package: 152**

+ Network Attendant Service **Package: 159**

+ Flexible Numbering Plan **Package: 160**

+ Trunk Failure Monitor **Package: 182**

+ Radio Paging **Package: 187**

+ DPNSS Network Services **Package: 231**

+ M911 Enhancement Display **Package: 249**

+ Called Party Control on Internal Calls **Package: 310**

+ DPNSSI Message Waiting Indication **Package: 325**

+ M3900 Product Enhancement **Package: 386**

+ IP Media Services **Package: 422**

Figure 15 –Customer – ISDN Configurations

5.5.2. Administer SIP Trunk Gateway to Session Manager

a) Select **IP Network -> Nodes: Servers, Media Cards** configuration from the left pane, and in the **IP Telephony Nodes** screen, select the **Node ID** of this CS1000 system. The **Node Details** screen is displayed as shown in **Figure 6, Section 5.2.1**.

b) On the **Node Details** screen, select **Gateway (SIPGw)** (not shown).

c) Under **General** tab of the **Virtual Trunk Gateway Configuration Details** screen, enter the following testing values (highlighted in red boxes) for the specified fields, and retain the default values for the remaining fields as shown in **Figure 16**. The parameters (highlighted in red boxes) are filled in, which were obtained when user creates a SIP Entity on the Session Manager (these are shown in **Section 5.8.4**).

- Vtrk gateway application: SIP Gateway (SIPGw)
- SIP domain name: mtsallstream.com
- Local SIP port: 5060
- Gateway endpoint name: car2-ssg-mtsallstream
- Application node ID: 2004

AVAYA CS1000 Element Manager

Managing: 110.10.97.90 Username: admin
System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration

Node ID: 2004 - 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: mtsallstream.com *
Local SIP port: 5060 * (1 - 65535)
Gateway endpoint name: car2-ssg-mtsallstream *
Gateway password: *
Application node ID: 2004 * (0-9999)
Enable failsafe NRS: ☐
SIP ANAT: ☒ IPv4 ☐ IPv6

Virtual Trunk Network Health Monitor

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

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

Figure 16 – Virtual Trunk Gateway Configuration Details Page 1

d) Click on the **SIP Gateway Settings** tab, under **Proxy or Redirect Server**, enter the IP address of Session Manager and value highlighted in the red box for the specified fields, and retain the default values for the remaining fields as shown in **Figure 17**.

AVAYA CS1000 Element Manager

Managing: 110.10.97.90 Username: admin
System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration

Node ID: 2004 - Virtual Trunk Gateway Configuration Details

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

Proxy Or Redirect Server:

Proxy Server Route 1:

Primary TLAN IP address: 110.10.97.198
The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"

Port: 5060 (1 - 65535)

Transport protocol: UDP

Options: ☐ Support registration
☐ Primary CDS proxy

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

Figure 17 – Virtual Trunk Gateway Configuration Details Page 2

e) On the same page as shown in **Figure 17**, scroll down to the **SIP URI Map** section (**Figure 18**).

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

- **National**: leave this SIP URI field as blank
- **Subscriber**: leave this SIP URI field as blank
- **Special Number**: leave this SIP URI field as blank
- **Unknown**: leave this SIP URI field as blank

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

- **UDP**: leave this SIP URI field as blank
- **CDP**: leave this SIP URI field as blank
- **Special Number**: leave this SIP URI field as blank
- **Vacant number**: leave this SIP URI field as blank
- **Unknown**: leave this SIP URI field as blank

Then click on the **Save** button.

AVAYA

CS1000 Element Manager

Managing: 110.10.97.90 Username: admin
 System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration

Node ID: 2004 - 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:	<input type="text"/>	Used for making VTRK call from agent.
Converged telephone call forward DN:	<input type="text"/>	
RAN route for announce:	<input type="text"/>	(route number 0 - 511)
Wait time before RAN queue:	<input type="text" value="1"/>	(-1 - 32767 msec)

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

Figure 18 – Virtual Trunk Gateway Configuration Details Page 3

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

5.5.3. Administer Virtual D-Channel

a) Select **Routes and Trunks -> D-Channels** from the left pane to display the **D-Channels** screen. In the **Choose a D-Channel Number** field, select an available D-channel from the drop-down list as shown in **Figure 19**. Click on **to Add** button.

AVAYA CS1000 Element Manager

Managing: **110.10.97.90** Username: admin
Routes and Trunks » D-Channels

D-Channels

Maintenance

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

Configuration

Choose a D-Channel Number: and type:

- Channel: 100	Type: DCH	Card Type: DCIP	Description: CenturyLink	<input type="button" value="Edit"/>
- Channel: 101	Type: DCH	Card Type: DCIP	Description: XO	<input type="button" value="Edit"/>
- Channel: 102	Type: DCH	Card Type: DCIP	Description: sipi	<input type="button" value="Edit"/>
- Channel: 103	Type: DCH	Card Type: DCIP	Description: BellCanada	<input type="button" value="Edit"/>
- Channel: 104	Type: DCH	Card Type: DCIP	Description: MTSAllStream	<input type="button" value="Edit"/>

Figure 19 – D-Channels

b) The D-Channels Property Configuration screen is displayed as shown in **Figure 20**. Enter the following values for the specified fields, and retain the default values for the remaining fields.

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

AVAYA CS1000 Element Manager Help | Logout

- UCM Network Services

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

Action Device And Number (ADAN): DCH

D channel Card Type: DCIP

Designator: carrier

Recovery to Primary: ☐

PRI loop number for Backup D-channel:

User: Integrated Services Signaling Link Dedicated (ISLD)

Interface type for D-channel: Meridian Meridian1 (SL1)

Country: ETS 300 =102 basic protocol (ETSI)

D-Channel PRI loop number:

Primary Rate Interface: more PRI

Secondary PRI2 loops:

Meridian 1 node type: Slave to the controller (USR)

Release ID of the switch at the far end: 25

Central Office switch type: 100% compatible with Bellcore standard (STD)

Integrated Services Signaling Link Maximum: 4000 Range: 1 - 4000

Signalling server resource capacity: 3700 Range: 0 - 3700

+ Basic options (BSOFT)

- Advanced options (ADVOPT)

- Layer 3 call control message count per 5 second time interval: 300 Range: 60 - 350
- Number of Status Enquiry Messages sent within 128 ms: 1
- Map channel number to timeslots on a PRI2 loop: ☒

+ H323 Overlap Signaling Settings (H323)

--Overlap Timer: 1

- Multilocation Business Group Allowed: ☐

- Network Attendant Service Allowed: ☒

+ - Link Access Protocol for D-channel (LAPD)

+ Feature Packages

Submit Refresh Delete Cancel

Figure 20 – D-Channels Configuration Details

c) Click on the **Basic Options** and click on the **Edit** button at the **Remote Capabilities (RCAP)** attribute. The **Remote Capabilities Configuration** page will appear. Then check on the **ND2** and the **MWI** checkboxes as shown in **Figure 21** and **Figure 22**.

AVAYA CS1000 Element Manager Help | Logout

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

D channel Card Type:

Designator:

Recovery to Primary: ☐

PRI loop number for Backup D-channel:

User:

Interface type for D-channel:

Country:

D-Channel PRI loop number:

Primary Rate Interface:

Secondary PRI2 loops:

Meridian 1 node type:

Release ID of the switch at the far end:

Central Office switch type:

Integrated Services Signaling Link Maximum: Range: 1 - 4000

Signalling server resource capacity: Range: 0 - 3700

- Basic options (BSCOPT)

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

- PINX customer number:

- Progress signal:

- Calling Line Identification:

- Output request Buffers:

- D-channel transmission Rate:

- Channel Negotiation option:

- Remote Capabilities:

+ - Change protocol timer value (TIMR)

- B channel Service messaging: ☐

+ Advanced options (ADVOPT)

+ Feature Packages

Figure 21 – D-Channels Configuration Details

AVAYA

CS1000 Element Manager

Help | Logout

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

Call transfer integer (CTI) ☐

Call transfer object (CTO) ☐

Diversion info. is sent using integer value (DV1I) ☐

Diversion info. is sent using object identifier (DV1O) ☐

Rerouting requests processed using integer value (DV2I) ☐

Rerouting requests processed using object identifier (DV2O) ☐

Diversion info. sent. rerouting requests processed (DV3I) ☐

EuroISDN - div. info sent. rerouting req. processed (DV3O) ☐

Call transfer notification and invocation to EuroISDN (ECTO) ☐

Malicious call identification (MCID) ☐

MCDN QSIG conversion (MQC) ☐

Remote D-channel is on a MSDL card (MSL) ☐

Message waiting interworking with DMS-100 (MWM) ☒

Network access data (NAC) ☐

Network call trace supported (NCT) ☐

Network name display method 1 (ND1) ☐

Network name display method 2 (ND2) ☒

Network name display method 3 (ND3) ☐

Name display - integer ID coding (NDI) ☐

Name display - object ID coding (NDO) ☐

Path replacement uses integer values (PRI) ☐

Path replacement uses object identifier (PRO) ☐

Release Link Trunks over IP (RLTI) ☐

Remote virtual queuing (RVQ) ☐

Trunk anti-tromboning operation (TAT) ☐

User to user service 1 (UUS1) ☐

NI-2 name display option. (NDS) ☐

Message waiting indication using integer values (QMWI) ☐

Message waiting indication using object identifier (QMWI) ☐

User to user signalling (UUI) ☐

Return - Remote Capabilities

Cancel

Figure 22 – Remote Capabilities Configuration Details

- d) Click on the **Return – Remote Capabilities** button.
- e) Click on the **Submit** button (not shown).

5.5.4. Administer Virtual Super-Loop

Select **System** -> **Core Equipments** -> **Superloops** from the left pane to display the **Superloops** screen. If the Superloop does not exist, please click “**Add**” button to create a new one as shown in **Figure 23**. In this example, Superloop 100 is being added and used.

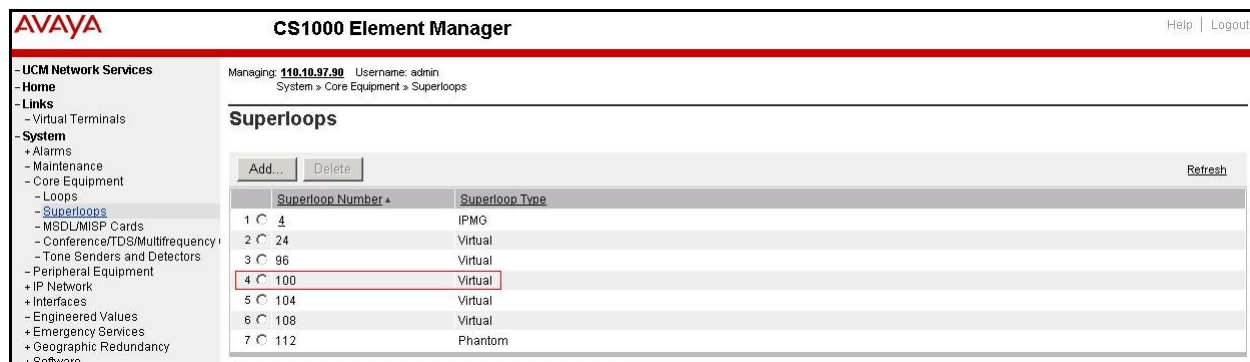


Figure 23 – Administer Virtual Super-Loop

5.5.5. Enable Music for Customer Data Block

a) Select **Customers** in the left pane. The **Customers** screen is displayed. Click on the link associated with the appropriate customer, in this case **04**. The system can support more than one customer with different network settings and options. The **Customer 04 Edit** page will appear (not shown). Select the **Feature Packages** option from this page.

b) The screen is updated with a list of **Feature Packages** populated. Select **Enhanced Music** to edit its parameters. Check to enable music for Customer 04, define music route 54 as shown in the redbox of **Figure 24**. The CS1000 system has been pre-configured with music route 54.

AVAYA CS1000 Element Manager

Feature Package	Package Number
+ Distinctive Ringing	Package: 74
+ Departmental Listed Directory Number	Package: 76
+ Command Status Link	Package: 77
+ Pretranslation	Package: 92
+ Dialed Number Identification System	Package: 98
+ Malicious Call Trace	Package: 107
+ Incoming Digit Conversion	Package: 113
+ Directed Call Pickup	Package: 115
- Enhanced Music	Package: 119
+ Station Camp-On	Package: 121
+ Integrated Digital Access	Package: 122
+ Digital Private Network Signaling System 1	Package: 123
+ 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
+ Flexible Services	Package: 152
+ Network Attendant Service	Package: 159
+ Flexible Numbering Plan	Package: 160
+ Trunk Failure Monitor	Package: 182
+ Radio Paging	Package: 187
+ DPNSS Network Services	Package: 231
+ M911 Enhancement Display	Package: 249
+ Called Party Control on Internal Calls	Package: 310
+ DPNSSI Message Waiting Indication	Package: 325
+ M3900 Product Enhancement	Package: 386
+ IP Media Services	Package: 422

Music for sets: ☒

- Music Route for sets: 54

Figure 24 – Enable Music for Customer 04

c) Scroll down to the bottom of the screen, and click on the **Save** button at the bottom of the page.

5.5.6. Administer Virtual SIP Routes

a) Select **Routes and Trunks** -> **Routes and Trunks** from the left pane to display the **Routes and Trunks** screen. In this example, **Customer 04** is being used. Click on the **Add route** button as shown in **Figure 25**.

AVAYA CS1000 Element Manager

Managing: **110.10.97.90** Username: admin
Routes and Trunks » Routes and Trunks

Routes and Trunks

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

Figure 25 – Add route

b) The **Customer 4, New Route Configuration** screen is displayed next. Scroll down until the **Basic Configuration** section is displayed and enter the following values for the specified fields, and retain the default values for the remaining fields as shown in **Figure 26a**.

- **Route Number (ROUT):** Select an available route number.
- **Designator field for trunk (DES):** A descriptive text.
- **Trunk Type (TKTP):** TIE trunk data block (TIE)
- **Incoming and Outgoing trunk (ICOG):** Incoming and Outgoing (IAO)
- **Access Code for the trunk route (ACOD):** An available access code.
- Check the field **The route is for a virtual trunk route (VTRK)**, to enable four additional fields to appear.
- For the **Zone for codec selection and bandwidth management (ZONE)** field, enter 255 (created in **Section 5.4.2**).

- For the **Node ID of signaling server of this route (NODE)** field, enter the node number 2004 (created in **Section 5.2.1**).
- Select **SIP (SIP)** from the drop-down list for the **Protocol ID for the route (PCID)** field.
- Check the **Integrated Services Digital Network option (ISDN)** checkbox to enable additional fields to appear. Enter the following values for the specified fields, and retain the default values for the remaining fields. Scroll down to the bottom of the screen.
 - **Mode of operation (MODE):** Route uses **ISDN Signalling Link (ISLD)**
 - **D channel number (DCH):** D-Channel number 104 (created in **Section 5.5.3**)
 - **Network calling name allowed (NCNA):** Check the field.
 - **Network call redirection (NCRD):** Check the field.
 - **Insert ESN access code (INAC):** Check the field.

AVAYA CS1000 Element Manager

Managing: **110.10.97.90** Username: admin
Routes and Trunks » Routes and Trunks » Customer 4, Route 104 Property Configuration

Customer 4, Route 104 Property Configuration

- Basic Configuration

Route data block (RDB) (TYPE): RDB

Customer number (CUST): 04

Route number (ROUT): 104

Designator field for trunk (DES): MTSALLSTREAM

Trunk type (TKTP): TIE

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

Access code for the trunk route (ACOD): 8104

Trunk type M911P (M911P): [checkbox]

The route is for a virtual trunk route (VTRK): [checkbox]

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

- Node ID of signaling server of this route (NODE): 2004 (0 - 9999)

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

- Print correlation ID in CDR for the route (CRID): [checkbox]

Integrated services digital network option (ISDN): [checked]

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

- D channel number (DCH): 104 (0 - 254)

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

- Private network identifier (PNI): 00004 (0 - 32700)

- Network calling name allowed (NCNA): [checked]

- Network call redirection (NCRD): [checked]

- Trunk route optimization (TRO): [checkbox]

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

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

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

- Insert ESN access code (INAC): [checked]

Figure 26a – Route Configuration Details Pages 1

- Click on **Basic Route Options**, check **North American toll scheme (NATL)** and **Incoming DID digit conversion on this route (IDC)**, input **DCNO 0** for both **Day IDC Tree Number** and **Night IDC Tree Number** as shown in **Figure 26b**.

AVAYA CS1000 Element Manager

- UCM Network Services
 - Home
 - Links
 - Virtual Terminals
 - System
 - + Alarms
 - Maintenance
 - Core Equipment
 - Loops
 - Superloops
 - MSDLMISP Cards
 - Conference/TDS/Multifrequency
 - Tone Senders and Detectors
 - 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

- Network call redirection (NCRD) : ☒
- Trunk route optimization (TRO) : ☐
- Recognition of DTI2 ABCD FALT signal for ISL (FALT) : ☐
- Channel type (CHTY) : B-channel (BCH)
- Call type for outgoing direct dialed TIE route (CTYP) : Unknown Call type (UKWN)
- Insert ESN access code (INAC) : ☒
- Integrated service access route (ISAR) : ☐
- Display of access prefix on CLID (DAPC) : ☐
- Mobile extension route (MBXR) : ☐
- Mobile extension outgoing type (MBXOT) : National number (NPA)
- Mobile extension timer (MBXT) : 0 (0 - 8000 milliseconds)
- Calling number dialing plan (CNDP) : Unknown (UKWN)

- Basic Route Options

- Attendant announcement (ATAN) : No Attendant Announcement (NO)
- Billing number required (BILN) : ☐
- Call detail recording (CDR) : ☐
- North American toll scheme (NATL) : ☒
- Controls or timers (CNTL) : ☐
- Conventional (Tie trunk only) (CNVT) : ☐
- Incoming DID digit conversion on this route (IDC) : ☒
 - Day IDC tree number (DCNO) : 0 (0 - 254)
 - Night IDC tree number (NDNO) : 0 (0 - 254)
- Display external dialed digits (DEXT) : ☐
- Multifrequency compelled or MFC signaling (MFC) : No MFC (NO)
- Process notification networked calls (PNNC) : ☐

+ Network Options

+ General Options

+ Advanced Configurations

Submit Refresh Delete Cancel

Figure 26b – Route Configuration Details Pages 2

- Click on **Advance Configurations**; check **Music-on-holds** to enable music on hold on the route. Input music route 54 to the boxes as shown in **Figure 26c**. The CS1000 system has been pre-configured with route 54 as a music route.

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 (NAT)
 - 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

- Advanced Configurations

Malicious call trace alarm is allowed for external calls (ALRM): ☐

Allow last re-directing number (ARDN): ARDN (NO)

ANI identifier number (ANTG):

AC15 timed reminder recall (ATTR): ☐

Auto terminate (AUTO): ☐

Collect call blocking allowed (CCBA): ☐

Call forward restriction (CFWR): ☐

Maximum number of CNH digits (CLEN): 10

Time (in seconds) that an extension is allowed to ring or be On-hold or Call Park before the trunk is disconnected (DCT): 0 (0 - 511)

North American distinctive ringing for incoming calls (DRNG): ☐

Home local number (HLCL):

Home national number (HNTN):

In-band automatic number identification route (IANI): ☐

Incoming identifier send (ICIS): ☒

Internal/external definition (IDEF): Use network info (NET)

Identify originating party (IDOP): ☐

Insert (INST):

Manual outgoing trunk route (MANO): ☐

Manual route (MNL): ☐

Music on-hold (MUS): ☒

Music route number (MRT): 54 (0 - 511)

Outgoing identifier send (OGIS): ☒

Off-hook timer delay (OHTD): ☐

Outpulsing route (OPR): ☐

Pseudo answer (PANS): ☒

Periodic clearing signal (PECL): ☐

Privacy indicator ignored (PII): ☐

Figure 26c – Route Configuration Details Pages 3

c) Click on the **Submit** button.

5.5.7. Administer Virtual Trunks

a) Continue from **Section 5.5.5**, click **Submit**, the **Routes and Trunks** screen is displayed and updated with the newly added route. In the example, Route 104 was being added. Click on the **Add trunk** button next to the newly added route 104 as shown in **Figure 27**.

AVAYA CS1000 Element Manager

Managing: **110.10.97.90** Username: admin
Routes and Trunks > Routes and Trunks

Routes and Trunks

Customer	Total routes	Total trunks	Action
+ Customer: 0	Total routes: 3	Total trunks: 34	Add route
+ Customer: 1	Total routes: 2	Total trunks: 34	Add route
+ Customer: 3	Total routes: 2	Total trunks: 34	Add route
- Customer: 4	Total routes: 3	Total trunks: 66	Add route

Route	Type	Description	Edit	Add trunk
+ Route: 54	Type: MUS	Description: MUSIC	Edit	Add trunk
+ Route: 102	Type: TIE	Description: SIPL	Edit	Add trunk
+ Route: 104	Type: TIE	Description: MTSALLSTREAM	Edit	Add trunk

Figure 27 – Route and Trunks

b) The **Customer 4, Route 104, Trunk 1 Property Configuration** screen is displayed in **Figure 28**. Enter the following values for the specified fields and retain the default values for the remaining fields. The Media Security (sRTP) has to be disabled at the trunk level by editing the **Class of Service (CLS)** at the bottom basic trunk configuration page. Click on the **Edit** button as shown in **Figure 28**.

- The **Multiple trunk input number (MTINPUT)** field may be used to add multiple trunks in a single operation, or repeat the operation for each trunk. In the sample configuration, 32 trunks were created.
- **Trunk data block (TYPE): IP Trunk (IPTI)**
- **Terminal Number (TN):** Available terminal number (created in **Section 5.5.4**)
- **Designator field for trunk (DES):** A descriptive text
- **Extended Trunk (XTRK): Virtual trunk (VTRK)**
- **Member number (RTMB):** Current route number and starting member
- **Start arrangement Incoming (STRI): Immediate (IMM)**

- **Start arrangement Outgoing (STRO): Immediate (IMM)**
- **Trunk Group Access Restriction (TGAR):** Desired trunk group access restriction level
- **Channel ID for this trunk (CHID):** An available starting channel ID

AVAYA CS1000 Element Manager Help |

Managing: **110.10.97.90** Username: admin
Routes and Trunks > Routes and Trunks > Customer 4, Route 104, Trunk 1 Property Configuration

Customer 4, Route 104, Trunk 1 Property Configuration

- Basic Configuration

Auto increment member number: ☒

Trunk data block:

Terminal number:

Designator field for trunk:

Extended trunk:

Member number:

Level 3 Signaling:

Card density:

Start arrangement Incoming:

Start arrangement Outgoing:

Trunk group access restriction:

Channel ID for this trunk:

Class of Service:

+ Advanced Trunk Configurations

Figure 28 – New Trunk Configuration Details

c) For **Media Security**, select **Media Security Never (MSNV)**. Enter the remaining values for the specified fields as shown in **Figure 29**. Scroll down to the bottom of the screen and click **Return Class of Service** and then 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
 - + 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

- Loop Break Supervised COT:
 - Make-break ratio for dial pulse:
 - Manual Incoming:
 - Media Security: **Media Security Never (MSNV)**
 - Network Hook Flash Over M911P:
 - Polarity:
 - Priority:
 - Restriction level: **Unrestricted (UNR)**
 - Reversed Ear Piece:
 - Short or long line:
 - Transmission Class of Service:
 - Warning Tone:
 - Reversed Ear Piece:
 - ARF Supervised COT:

Figure 29 – Class of Service Configuration Details Page

5.5.8. Administer Calling Line Identification Entries

a) Select **Customers > 04 > ISDN and ESN Networking**. Click on **Calling Line Identification Entries** as shown in Figure 30.

AVAYA CS1000 Element Manager

Managing: 110.10.97.98 Username: admin
Customers > Customer 04 > Customer Details > ISDN and ESN Networking

ISDN and ESN Networking

General Properties

Flexible trunk to trunk connection option:

Flexible orbiting prevention timer:

Country code:
(0 - 9999)

Code for processing the called number

National access code:

International access code:

Options: ☒ Transfer on ringing of supervised external trunks
☒ Connection of supervised external trunks

Network option: ☐ Coordinated dialing plan routing

Integrated services digital network: ☒

Microsoft converged office dialing plan:

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

Calling Line Identification

Information for incoming/outgoing calls:

Size:
(0 - 4000)

Country code:
(0 - 9999)

Code displayed as part of calling number

Calling Line Identification Entries

Save Cancel

Figure 30 – ISDN and ESN Networking

b) Click on **Add** as shown in Figure 31.

AVAYA CS1000 Element Manager

Managing: 110.10.97.98 Username: admin
Customers > Customer 04 > 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 Refresh

Entry Id	National Code	Local Code	Home location code	Local steering code	Use DN as DID	Emergency Local Code
----------	---------------	------------	--------------------	---------------------	---------------	----------------------

Save Cancel

Figure 31 – Calling Line Identification Page

c) Add entry **0** as shown in **Figure 32**

- **National Code:** leave as blank
- **Local Code:** input prefix digits assigned by Service Provider, in this case it is 6 digits – 647776. This **Local Code** will be used for call display purpose of outbound international call configuration in **Section 5.6.6** where the **Special Number 0** is associated with Call Type = Unknown.
- **Home Location Code:** input prefix digits assigned by Service Provider, in this case it is 6 digits - 647776. This **Home Location Code** will be used for call display purpose for Call Type = National (NPA).
- **Local Steering Code:** input prefix digits assigned by Service Provider, in this case it is 6 digits - 647776. This **Local Steering Code** will be used for call display purpose for Call Type = Local Subscriber (NXX).
- **Calling Party Name Display:** Uncheck for **Roman characters**.

The screenshot shows the AVAYA CS1000 Element Manager interface. The top bar includes the AVAYA logo, the title 'CS1000 Element Manager', and links for 'Help' and 'Logout'. The left sidebar contains a navigation tree with categories like 'UCM Network Services', 'Home', 'Links', 'System', 'Customers', 'Routes and Trunks', 'Dialing and Numbering Plans', 'Phones', 'Tools', and 'Security'. The main content area is titled 'Edit Calling Line Identification 0' and contains the following sections:

- General Properties:**
 - National Code: [] (0 - 999999) Code for national home number
 - Local Code: [647776] (1-12 digits) Code for home local number or listed DN
 - Home Location Code: [647776] (1-7 digits)
 - Local Steering Code: [647776] (1-7 digits)
 - Use DN as DID: [YES]
- Emergency Services Access:**
 - Emergency Local Code: [] (1-12 digits) Code for home local number during Emergency calls
 - Emergency Options:
 - ☐ Home national number for emergency services access calls
 - ☒ Append the originating directory number for emergency services access calls
- Calling Party Name Display:**
 - Roman characters: ☐
 - CPND Name: [] first name, last name
 - Expected Length: []
 - Display Format: [First name, Last name]

At the bottom right, there are 'Save' and 'Cancel' buttons.

Figure 32 – Edit Calling Line Identification 0

d) Click on **Save**.

5.5.9. Enable External Trunk to Trunk Transferring

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

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

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

TYPE NET_DATA
CUST 4
OPT
...
TRNX YES
EXTT YES
...
```

5.6. Administer Dialing Plans

5.6.1. Define ESN Access Codes and Parameters (ESN)

a) Select **Dialing and Numbering Plans** -> **Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen. Select **ESN Access Code and Parameters (ESN)** as shown in **Figure 33**.

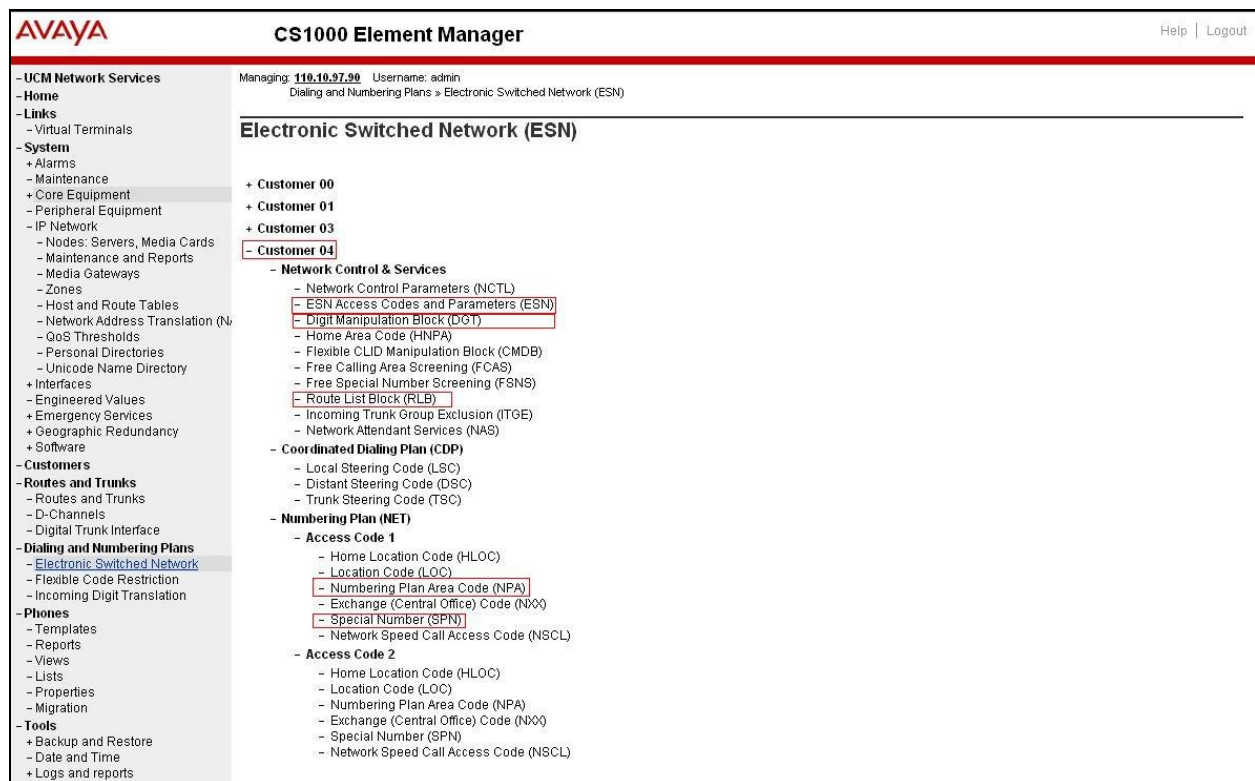


Figure 33 – Electronic Switch Network (ESN)

b) In the **ESN Access Codes and Basic Parameters** page, define **NARS/ BARS Access Code 1** as shown in **Figure 34**.

AVAYA CS1000 Element Manager

Managing: **110.10.97.90** Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 04 » Network Control & Services » ESN Access Codes and Basic Parameters

ESN Access Codes and Basic Parameters

General Properties

NARS/BARS Access Code 1:

NARS Access Code 2:

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

Expensive Route Warning Tone: ☒

- Expensive Route Delay Time: (0 - 10)

Coordinated Dialing Plan feature for this customer: ☒

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

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

Routing Controls: ☐

Check for Trunk Group Access Restrictions: ☐

Limits

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

Maximum number of Route Lists: (0 - 2000)

Maximum number of CLID manipulation tables: (1 - 256)

Maximum number of Supplemental Digit restriction blocks: (0 - 1500)

Figure 34 – ESN Access Codes and Basic Parameters

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

5.6.2. Associate NPA and SPN call to ESN Access Code 1

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

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

TYPE NET_DATA
CUST 4
OPT
AC2 xNPA xSPN
FNP
CLID
...
```

- c) Verify Customer Net_Data block by using LD 21.

```
>ld 21
PT1000

REQ: prt
TYPE: net
TYPE NET_DATA
CUST 4

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

5.6.3. Digit Manipulation Block (DMI)

a) Select **Dialing and Numbering Plans** -> **Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen. Select **Digit Manipulation Block (DGT)** as shown in **Figure 33**.

b) In the Choose a DMI Number field, select an available DMI from the drop-down list and click to **Add** as shown in **Figure 35**.

The screenshot displays the Avaya CS1000 Element Manager web interface. On the left is a navigation tree under 'UCM Network Services' with categories like Home, Links, System, Customers, Routes and Trunks, Dialing and Numbering Plans, and Phones. The 'Dialing and Numbering Plans' section is expanded, showing 'Electronic Switched Network' as the selected item. The main content area is titled 'Digit Manipulation Block List'. At the top of this area, it shows 'Managing: 135.10.97.90' and 'Username: admin'. Below this is a breadcrumb trail: 'Dialing and Numbering Plans > Electronic Switched Network (ESN) > Customer 04 > Network Control & Services > Digit Manipulation Block List'. The main heading is 'Digit Manipulation Block List'. Below the heading, there is a form with the text 'Please choose the' followed by a dropdown menu currently showing 'Digit Manipulation Block Index 1' and a red 'to Add' button.

Figure 35 – Digit Manipulation Block List

c) Enter **0** for the **Number of leading digits to be Deleted (Del)** field and select **NPA (NPA)** for the **Call Type to be used by the manipulated digits (CTYP)** and then click **Submit** as shown in **Figure 36**.

AVAYA **CS1000 Element Manager** Help | Logout

Managing: **110.10.97.90** Username: admin
Dialing and Numbering Plans > [Electronic Switched Network \(ESN\)](#) > Customer 04 > Network Control & Services > [Digit Manipulation Block List](#) > Digit Manipulation Block

Digit Manipulation Block

Digit Manipulation Index numbers:

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

Insert:

IP Special Number: ☐

Call Type to be used by the manipulated digits:

Left Sidebar:

- 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 (NAT)
 - 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

Figure 36 – Digit Manipulation Block

5.6.4. Route List Block (RLB) (RLB 104)

This section shows how to add a RLB associated with the DMI created in **Section 5.6.3**.

- Select **Dialing and Numbering Plans -> Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen. Select **Route List Block (RLB)** as shown in **Figure 33**.
- Select an available value in the textbox for the **route list index** and click on the “**to Add**” button (in this case is 104) (**Figure 37**).

The screenshot displays the AVAYA CS1000 Element Manager web interface. The top header includes the AVAYA logo, the title "CS1000 Element Manager", and links for "Help" and "Logout". The left sidebar contains a navigation tree with categories like "UCM Network Services", "Home", "Links", "System", "Customers", "Routes and Trunks", "Dialing and Numbering Plans", and "Phones". The "Dialing and Numbering Plans" category is expanded, showing "Electronic Switched Network" as the selected option. The main content area shows the "Route List Blocks" configuration page. It includes a breadcrumb trail: "Managing: 110.10.97.90 Username: admin > Dialing and Numbering Plans > Electronic Switched Network (ESN) > Customer 04 > Network Control & Services > Route List Blocks". Below the title "Route List Blocks", there is a form with the label "Please enter a route list index" followed by a text input field containing "104", a range indicator "(0 - 1999)", and a "to Add" button. Below this, a table lists the existing route list blocks, with one entry visible: "Route List Block Index -- 104" with an "Edit" button next to it.

Figure 37 – Route List Blocks

c) Enter the following values for the specified fields, and retain the default values for the remaining fields (**Figure 38**). Scroll down to the bottom of the screen, and click on the **Submit** button.

- **Route number (ROUT): 104** (created in **Section 5.5.5**)
- **Digit Manipulation Index (DMI): 1** (created in **Section 5.6.3**)

The screenshot displays the AVAYA CS1000 Element Manager interface. On the left is a navigation tree with categories like UCM Network Services, System, Customers, Routes and Trunks, Dialing and Numbering Plans, Phones, Tools, and Security. The main area is titled 'General Properties' and contains several configuration sections:

- General Properties:** Includes a text field for 'Entry Number for the Route List' (value: 0).
- Indexes:** Contains dropdowns for 'Time of Day Schedule' (0), 'Facility Restriction Level' (0, range 0-7), 'Digit Manipulation Index' (1, highlighted), 'ISL D-Channel Down Digit Manipulation Index' (0, range 0-1999), 'Free Calling Area Screening Index' (0), 'Free Special Number Screening Index' (0), 'Business Network Extension Route' (checkbox), and 'Incoming CLID Table' (0, range 0-255).
- Options:** Includes checkboxes for 'Local Termination entry', 'Skip Conventional Signaling', 'Use Tone Detector', 'Conversion to LDN', and 'Expensive Route'. It also has dropdowns for 'Strategy on Congestion' (No Reroute (NRR)), 'QSIG Alternate Routing Causes' (QSIG Alternate Routing Cause 1), 'Preferred Routing' (Preferred Route 1), and 'ISDN Drop Back Busy' (Drop Back Disabled (DBD)).
- VNS Options:** Includes a checkbox for 'Entry is a VNS Route'.

At the bottom right, there are four buttons: 'Submit' (highlighted with a red box), 'Refresh', 'Delete', and 'Cancel'.

Figure 38 – Route List Blocks Configuration Details

5.6.5. Inbound Call Digit Translation

This section describes the steps for receiving calls from PSTN via the MTS Allstream system.

a) Select **Dialing and Numbering Plans -> Incoming Digit Translation** from the left pane to display the **Incoming Digit Translation** screen. Click on the **Edit IDC** button (**Figure 39**).

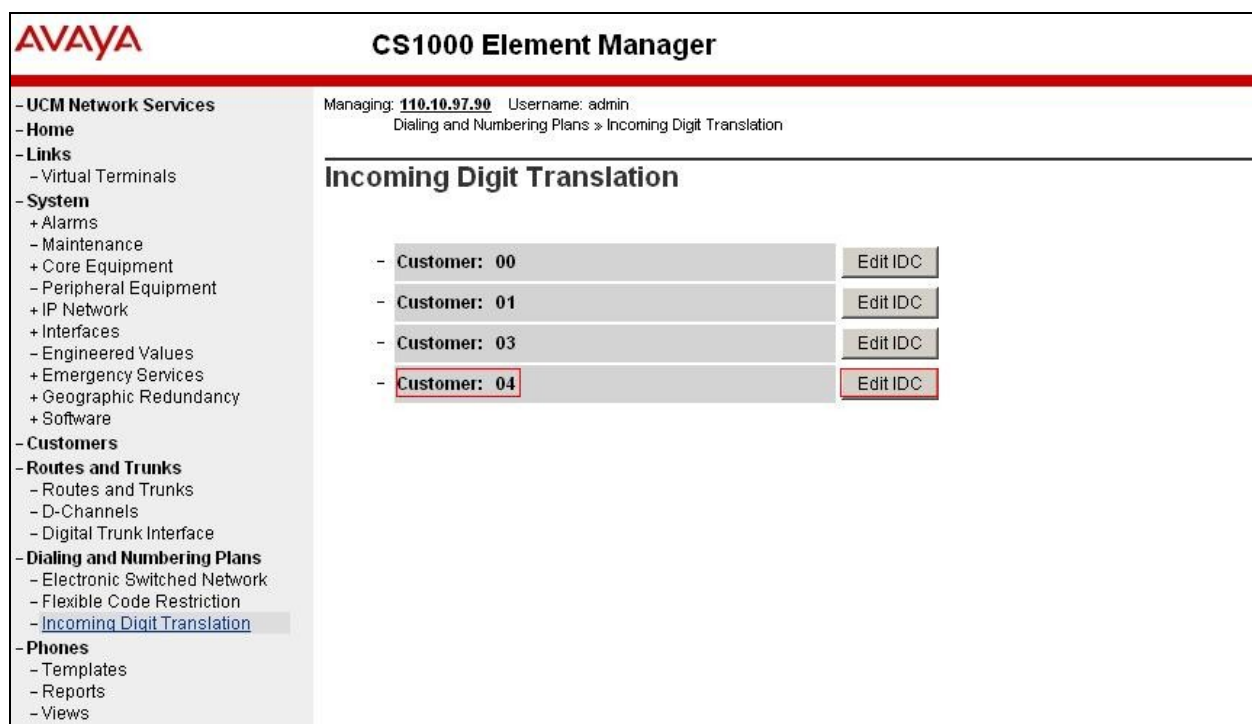


Figure 39 – Incoming Digit Translation

b) Click on **New DCNO** to create the digit translation mechanism. In this example, Digit Conversion Tree Number (DCNO) 0 has been created as shown in **Figure 40**.

AVAYA **CS1000 Element Manager**

Managing: **110.10.97.90** Username: admin
Dialing and Numbering Plans > Incoming Digit Translation > Customer 04

Customer 04 Incoming Digit Conversion Property

- Digit Conversion Tree Number: 0	Edit DCNO
- Digit Conversion Tree Number: 1	New DCNO
- Digit Conversion Tree Number: 2	New DCNO
- Digit Conversion Tree Number: 3	New DCNO
- Digit Conversion Tree Number: 4	New DCNO
- Digit Conversion Tree Number: 5	New DCNO
- Digit Conversion Tree Number: 6	New DCNO
- Digit Conversion Tree Number: 7	New DCNO
- Digit Conversion Tree Number: 8	New DCNO
- Digit Conversion Tree Number: 9	New DCNO
- Digit Conversion Tree Number: 10	New DCNO
- Digit Conversion Tree Number: 11	New DCNO
- Digit Conversion Tree Number: 12	New DCNO
- Digit Conversion Tree Number: 13	New DCNO

Navigation Menu:

- 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

Figure 40 – Incoming Digit Conversion Property

c) Detail configuration of the **DCNO** is shown in **Figure 41**. The **Incoming Digits** can be added to map to the **Converted Digits** which would be the CS1000 system phones DN. This **DCNO** has been assigned to route 104 as shown in **Figure 26**.

In the following configuration, incoming calls from PSTN with prefix 64777612XX will be translated to CS1K DN 12XX. The DID 6477761233 is translated to 3111 for Voicemail accessing purpose.

Managing: 110.10.97.90 Username: admin
Dialing and Numbering Plans > Incoming Digit Translation > Customer 04 > Digit Conversion Tree 0 Configuration

Digit Conversion Tree 0 Configuration

Regular IDC tree
Send calling party DID disabled

Buttons: Add... Delete IDC Delete IDC tree Refresh

	Incoming Digits	Converted Digits	CPND Name	CPND language
1	647776121	121		
2	647776122	122		
3	6477761230	1230		
4	6477761231	1231		
5	6477761232	1232		
6	6477761233	3111		

Figure 41 – Digit Conversion Tree Configuration

5.6.6. Outbound Call - Special Number Configuration

There are special numbers which have been configured to be used for this testing. For example, **0** to reach Service Provider operator, **0+10** digits to reach Service Provider operator assistant, **011** prefix for international call, **1** for national long distance call, **411**, **911** and so on.

a) Select **Dialing and Numbering Plans** -> **Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen. Select **Special Number (SPN)** as shown in **Figure 33**.

b) Enter SPN and then click on the “to Add” button. **Figure 42** shows all the special numbers used for this testing.

Special Number: 0

- **Flexible length:** 0 (flexible, unlimited and accept the character # to ending dial number)
- **CallType:** NONE
- **Route list index:** 104, created in **Section 5.6.4**

Special Number: 1

- **Flexible length:** 0 (flexible, unlimited and accept the character # to ending dial number)
- **CallType:** NATL
- **Route list index:** 104, created in **Section 5.6.4**

Special Number: 411

- **Flexible length:** 3
- **CallType:** NATL
- **Route list index:** 104, created in **Section 5.6.4**

Special Number: 911

- **Flexible length:** 3
- **CallType:** NATL
- **Route list index:** 104, created in **Section 5.6.4**

AVAYA

CS1000 Element Manager

- 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: **110.10.97.90** Username: admin
Dialing and Numbering Plans » **Electronic Switched Network (ESN)** » Customer 04 » Numbering Plan (NET) » Access Code 1 » Special Number List

Special Number List

Please enter a Special Number to Add

- Special Number -- 0 Flexible length: 0 International dialing plan: NO Type of call that is defined by the special number: NONE Route list index: 104	Edit
- Special Number -- 1 Flexible length: 0 Type of call that is defined by the special number: NONE Route list index: 104	Edit
- Special Number -- 411 Flexible length: 3 Inhibit time-out handler: NO Type of call that is defined by the special number: NONE Route list index: 104	Edit
- Special Number -- 911 Flexible length: 3 Inhibit time-out handler: NO Type of call that is defined by the special number: NONE Route list index: 104	Edit

Figure 42 – Special Number List

5.6.7. Outbound Call - Numbering Plan Area (NPA)

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

- Select **Dialing and Numbering Plans -> Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen. Select **Numbering Plan Area Code (NPA)** as shown in **Figure 33**.
- Enter area code desired in the textbox and click on the “**to Add**” button. **Figure 43** shows NPA numbers **613** and **416** were configured for this testing. These codes are associated to the SIP route.

The screenshot displays the AVAYA CS1000 Element Manager web interface. The left sidebar contains a navigation tree with categories like UCM Network Services, Home, Links, System, Customers, Routes and Trunks, Dialing and Numbering Plans, and Phones. The 'Dialing and Numbering Plans' section is expanded, and 'Electronic Switched Network' is selected. The main content area shows the 'Numbering Plan Area Code List' page. At the top, it indicates the user is managing '110.10.97.90' as 'admin'. Below this, a breadcrumb trail shows the path: 'Dialing and Numbering Plans > Electronic Switched Network (ESN) > Customer 04 > Numbering Plan (NET) > Access Code 1 > Numbering Plan Area Code List'. The page title is 'Numbering Plan Area Code List'. There is a form to 'Please enter an area code' with a 'to Add' button. Below this, a table lists the configured NPAs:

Numbering Plan Area Code	Route List Index	Incoming Trunk group Exclusion Index	Action
416	104	NONE	Edit
613	104	NONE	Edit

Figure 43 – Numbering Plan Area Code List

5.7. Administer Phone

This section describes the creation of CS1000 clients used in this testing configuration.

5.7.1. Phone creation

- a) Refer to **Section 5.5.4** to create a virtual super-loop - **108** used for IP phone.
- b) Refer to **Section 5.4.1** to create a bandwidth zone - **10** for IP phone.
- c) Login Call Server CLI (please refer to **Section 5.1.2** for more detail).
- d) Create an IP phone by using LD 11.

```
REQ: prt
TYPE: 2002p2
TN 108 0 0 15
DATE
PAGE
DES
MODEL_NAME
EMULATED
KEM_RANGE

DES MTS
TN 108 0 00 15 VIRTUAL
TYPE 2002P2
CDEN 8D
CTYP XDLC
CUST 4
NUID
NHTN
CFG_ZONE 00010
CUR_ZONE 00010
MRT
ERL 12345
ECL 0
FDN 1230
TGAR 2
LDN NO
NCOS 7
SGRP 0
RNPG 0
SCI 0
SSU
LNRS 16
XLST
SCPW
SFLT NO
CAC_MFC 0
CLS UNR FBA WTA LPR MTD FNA HTA TDD HFA CRPD
MWD LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
POD SLKD CCSD SWD LNA CNDA
CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBF
ICDD CDMD LLCN MCTD CLBD AUTU
GPUD DPUD DNDD CFXD ARHD FITD CLTD ASCD
```

CPFA CPTA ABDD CFHD FICD NAID BUZZ AGRD MOAD
 UDI RCC HBTD AHD IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
 DRDD EXR0
 USMD USRD ULAD CCBD RTDD RBDD RBHD PGND OCBD FLXD FTTC DNDY DNO3 MCBN
 FDSO NOVD VOLA VOUD CDMR PRED RECD MCDD T87D SBMD
 KEM2 MSNV FRA PKCH MUTA MWTD DVLD CROD ELCD
 CPND_LANG ENG
 RCO 0
 HUNT 1230
 LHK 0
 PLEV 02
 PUID
 UPWD
 DANI NO
 AST
 IAPG 0
 AACS NO
 ITNA NO
 DGRP
 MLWU_LANG 0
 MLNG ENG
 DNDR 0
KEY 00 SCR 1223 0 MARP
CPND
CPND_LANG ROMAN
NAME MTS i2002p2
XPLN 13
DISPLAY_FMT FIRST, LAST
 01
 02 MSB
 03
 04
 05
 06
 07
 08
 09
 10
 11
 12
 13
 14
 15
 16
 17 TRN
 18 AO6
 19 CFW 16
 20 RGA
 21 PRK
 22 RNP
 23
 24 PRS
 25 CHG
 26 CPN
 27

```
28
29
30
31
DATE 8 AUG 2011
```

NACT

5.7.2. Enable Privacy for Phone

In this section, it shows how to enable Privacy for a phone by changing its class of service (CLS). By modifying the configuration of the phone created in **Section 5.7.1**, the display of outbound calls will be changed appropriately.

a) To hide display name, set CLS to **namd**. CS1000 will include “Privacy:user” in the SIP message header before sending to Service Provider.

```
>ld 11
REQ: chg
TYPE: 2002p2
TN 108 0 0 15
SCH3928
TN 108 0 0 15
ECHG yes
ITEM cls namd
...
```

b) To hide display number, set CLS to **ddgd**. CS1000 will include “Privacy:id” in the SIP message header before sending to Service Provider.

```
>ld 11
REQ: chg
TYPE: 2002p2
TN 108 0 0 15
SCH3928
TN 108 0 0 15
ECHG yes
ITEM cls ddgd
...
```


c) To hide display name and number, set CLS to **namd, ddgd**. CS1000 will include “Privacy:id, user” in the SIP message header before sending to Service Provider.

```
>ld 11
REQ: chg
TYPE: 2002p2
TN 108 0 0 15
SCH3928
TN 108 0 0 15
ECHG yes
ITEM cls namd ddgd
...
```

d) To allow display name and number, set CLS to **nama, ddga**. CS1000 will send header “Privacy:none” to Service Provider.

```
>ld 11
REQ: chg
TYPE: 2002p2
TN 108 0 0 15
SCH3928
TN 108 0 0 15
ECHG yes
ITEM cls nama ddga
...
```

5.7.3. Enable Call Forward for Phone

In this section, it shows how to configure Call Forward feature at the system level and phone level.

a) Select **Customer > 04 > Call Redirection**. The Call Redirection page is shown as **Figure 45**.

- **Total redirection count limit: 7**
- **Call Forward: Originating**
- **Number of normal ring cycle of CFNA: 4**

AVAYA CS1000 Element Manager Help | Logout

UCM Network Services

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

Redirection Holidays

Do not disturb hunting: ☐

Total redirection count limit: **7**

Options:

- ☐ Call forward reminder tone for 500/2500 sets
- ☐ CFNA treatment for call waiting calls on a DN
- ☐ DID call to second degree busy treatment
- ☒ Message center
- ☒ Prevention of reciprocal call forward

Call forward: **Originating**

☐ Forwarding

Number of normal ringing cycles for CFNA

Option 0: **4**

Option 1: **4**

Option 2: **4**

Number of distinctive ringing cycles for CFNA

Option 0: **4**

Option 1: **4**

Option 2: **4**

Calls routed to message center

No answer DID calls: ☐

No answer non-DID calls: ☐

DID calls to busy telephones: ☐

Save **Cancel**

Figure 44 – Call Redirection

b) To enable **Call Forward All Call (CFAC)** for phone over trunk by using LD 11, change its CLS to **CXFA**, **SFA** then program the forward number on the phone set. The following is the configuration of a phone with CFAC enabled and forwarding number is 66139675279.

```
REQ: prt
TYPE: 2002p2
TN 108 0 0 15
DATE
PAGE
DES
MODEL_NAME
EMULATED

DES MTS
TN 108 0 00 15 VIRTUAL
TYPE 2002P2
...
CLS UNR FBA WTA LPR MTD FNA HTA TDD HFD CRPD
MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
POD SLKD CCSD SWD LNA CNDA
CFTD SFA MRD DDV CNID CDCA MSID DAPA BFED RCBF
ICDA CDMA LLCN MCTD CLBD AUTU
GPUD DPUD DNDD CFXA ARHD CLTD ASCD
...
19 CFW 16 66139675279
...
```

c) To enable **Call Forward Busy (CFB)** for phone over trunk by using LD 11, change its CLS to **FBA**, **HTA**, **SFA** then program the forward number as **HUNT**. The following is the configuration of a phone with CFB enabled and forward number 66139675279.

```
REQ: prt
TYPE: 2002p2
TN 108 0 0 15
DATE
PAGE
DES
MODEL_NAME
EMULATED

DES MTS
TN 108 0 00 15 VIRTUAL
TYPE 2002P2
...
CLS UNR FBA WTA LPR MTD FNA HTA TDD HFD CRPD
MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
POD SLKD CCSD SWD LNA CNDA
CFTD SFA MRD DDV CNID CDCA MSID DAPA BFED RCBF
...
HUNT 66139675279
...
```

d) To enable **Call Forward No Answer (CFNA)** for phone over trunk by using LD 11, change its CLS to **FNA**, **SFA** then program the forward number as **FDN**. The following is the configuration of a phone with CFNA enabled and forward number 66139675279.

```
REQ: prt
TYPE: 2002p2
TN 108 0 0 15
DATE
PAGE
DES
MODEL_NAME
EMULATED

DES MTS
TN 108 0 00 15 VIRTUAL
TYPE 2002P2
...
FDN 66139675279
...
CLS UNR FBA WTA LPR MTD FNA HTA TDD HFD CRPD
MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
POD SLKD CCSD SWD LNA CNDA
CFTD SFA MRD DDV CNID CDCA MSID DAPA BFED RCBF
...
```

5.7.4. Enable Call Waiting for Phone

In this section, it shows how to configure Call Waiting feature at phone level.

- a) Login Call Server CLI (please refer to **Section 5.1.2** for more detail).
- b) Configure Call Waiting feature for phone by using LD 11 to change CLS to **HTD**, **SWA** and adding a **CWT** key.

```
REQ: prt
TYPE: 2002p2

TN 108 0 0 15
DATE
PAGE
DES
MODEL_NAME
EMULATED
KEM_RANGE

DES MTS
TN 108 0 00 15 VIRTUAL
TYPE 2002P2
...
CLS UNR FBD WTA LPR MTD FNA HTD TDD HFD CRPD
MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
POD SLKD CCSD SWA LNA CNDA
...
KEY 00 SCR 1223 0 MARP
CPND
CPND_LANG ROMAN
NAME MTS i2002p2
XPLN 13
DISPLAY_FMT FIRST, LAST
01 CWT
...
```

5.8. Administer Avaya Aura® Session Manager

In this section, it shows how to configure the routing on Session Manager. It is assumed that Session Manager has been successfully deployed and connected to System Manager. System Manager is the web interface to configure the Session Manager.

5.8.1. Create a SIP domain name

This section shows how to create a new SIP domain name for this test configuration. Session Manager uses this domain name to route calls from Bell Canada to enterprise CS1000 and vice versa.

a) Login to System Manager. Open a web browser, https://<SMGR_IP_Address> then login with user “admin” and appropriate password as shown in **Figure 45**.

AVAYA Avaya Aura® System Manager 6.1

Home / Log On

Log On

Recommended access to System Manager is via FQDN.
[Go to central login for Single Sign-On](#)

If IP address access is your only option, then note that authentication will fail in the following cases:

- First time login with "admin" account
- Expired/Reset passwords

Use the "Change Password" hyperlink on this page to change the password manually, and then login.

Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.

This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use, or modification of this system is strictly prohibited.

Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal, or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

User ID:

Password:

[Change Password](#)

Figure 45: Login to System Manager

b) The System Manager home page displays as shown in **Figure 46**. Select **Routing** to configure the **Network Routing Policy**.

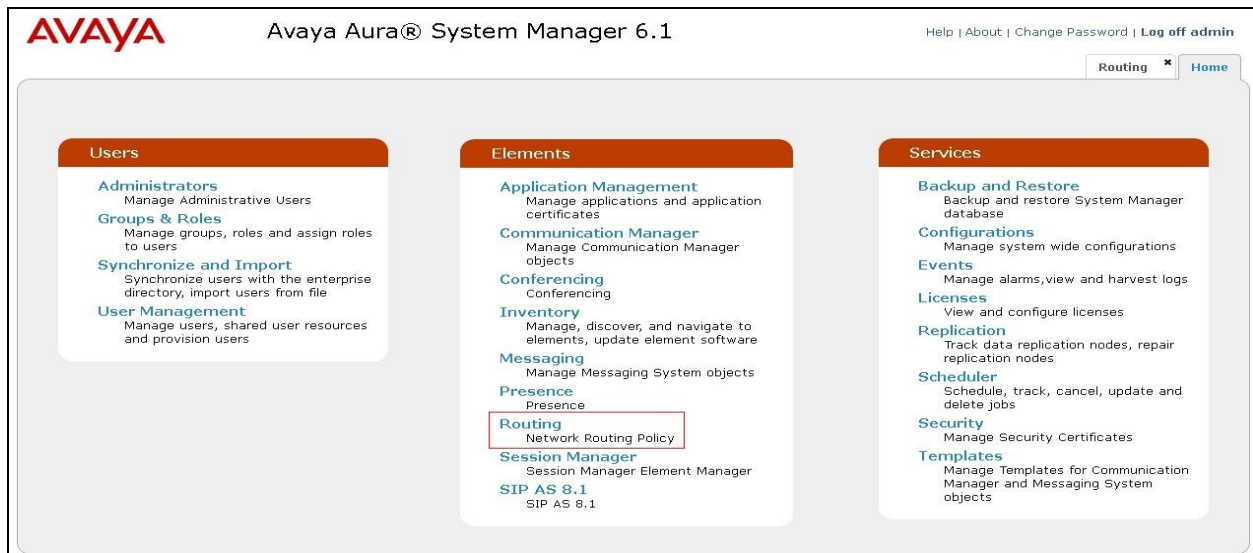


Figure 46 – Select Routing to configure Network Routing Policy

c) In the **Introduction to Network Routing Policy** page (not shown), click **Domains** link on the left menu to open **Domains - Domain Management** page. Then click button **New** (not shown) to add a new test domain. **Figure 47** shows domain **mtsallstream.com** was successfully added.

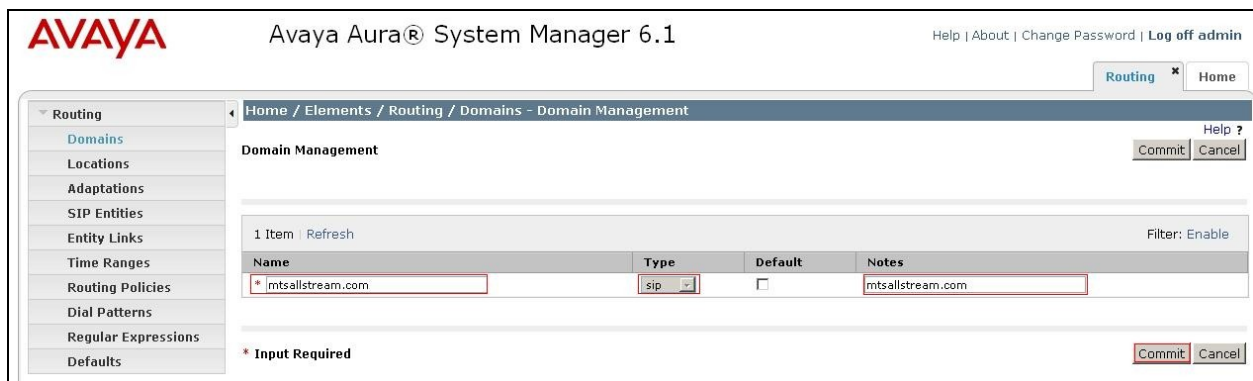


Figure 47 – Adding SIP domain mtsallstream.com

d) Click **Commit**.

5.8.2. Create a Location

Other than domain name, Session Manager binds a SIP Entity to a Location to for bandwidth and location management purposes. It inserts SIP header “P-Location” tell the Far End Gateway (Service Provider) where the call is made from.

The procedure to configure a location is as follows.

a) In the **Introduction to Network Routing Policy** page (not shown), click **Locations** link on the left menu to open **Locations - Location** page. Then click button **New** (not shown) to add a new test location. **Figure 48** shows location **Belleville,Ont,Ca** was successfully added with default settings in the red boxes.

The screenshot displays the Avaya Aura System Manager 6.1 web interface. The top navigation bar includes the Avaya logo, the title 'Avaya Aura® System Manager 6.1', and links for 'Help | About | Change Password | Log off admin'. The left sidebar shows a menu with 'Routing' selected, and sub-items like 'Domains', 'Locations', 'Adaptations', 'SIP Entities', 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Regular Expressions', and 'Defaults'. The main content area is titled 'Location Details' and contains the following sections:

- General**: A text box for '* Name:' containing 'Belleville,Ont,Ca'. Below it is a 'Notes:' text box.
- Overall Managed Bandwidth**: A dropdown for 'Managed Bandwidth Units' set to 'Kbit/sec'. Below it, a 'Total Bandwidth:' text box contains '1000000'.
- Per-Call Bandwidth Parameters**: A text box for '* Default Audio Bandwidth:' set to '80 Kbit/sec'.
- Location Pattern**: Includes 'Add' and 'Remove' buttons, a table with 0 items, and a 'Filter: Enable' option.

At the bottom, there is a '* Input Required' message and 'Commit' and 'Cancel' buttons.

Figure 48 – Adding a Location

b) Click **Commit**.

5.8.3. Create SIP Entity for Session Manager

This section shows how to configure System Manager to add a **SIP Entity** for Session Manager as a static gateway.

a) In the **Introduction to Network Routing Policy** page (not shown), click **SIP Entities** link on the left menu to open **SIP Entities – SIP Entities** page. Then click button **New** (not shown) to add a new entity for Session Manager. **Figure 49** shows entity **DevASM** was successfully added. Session Manager was configured to use transport protocol UDP with port 5060.

- **Name:** DevASM
- **FQDN or IP Address:** 110.10.97.198
- **Type:** Session Manager
- **Location:** Belleville,Ont,Ca
- **Port:** 5060, **Protocol:** UDP
- **SIP Link Monitoring:** Use Session Manager Configuration

SIP Entity Details

General

* Name: DevASM

* FQDN or IP Address: 110.10.97.198

Type: Session Manager

Notes: For Session Manager

Location: Belleville,Ont,Ca

Outbound Proxy:

Time Zone: America/Toronto

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Entity Links

Add Remove

19 Items Refresh Filter: Enable

	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
<input type="checkbox"/>	DevASM	UDP	* 5060	car3-ssg-carrier	* 5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	DevASM	UDP	* 5060	CS1K60	* 5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	DevASM	UDP	* 5060	AA-SBC3	* 5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	DevASM	UDP	* 5060	AASBCMTSAllStream	* 5060	<input checked="" type="checkbox"/>
<input type="checkbox"/>	DevASM	UDP	* 5060	ACME	* 5060	<input checked="" type="checkbox"/>

Select : All, None < Previous | Page 1 of 4 | Next >

Port

Add Remove

4 Items Refresh Filter: Enable

	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	UDP		

Figure 49 – Adding SIP Entity for Session Manager

b) Click **Commit**.

Note: The IP Address used for SIP Entity - Session Manager has to be different than the IP address used for management interface of Session Manager. The management IP was associated to physical interface eth0 and was defined during software installation. While the IP for SIP Entity was associated to physical interface eth2.

5.8.4. Create SIP Entity for CS1000 SIP Gateway

This section shows how to configure System Manager to add a SIP Entity for CS1000 SIP Gateway.

a) In the **Introduction to Network Routing Policy** page (not shown), click **SIP Entities** link on the left menu to open **SIP Entities – SIP Entities** page. Then click button **New** (not shown) to add a new entity for CS1000 SIP Gateway.

The **Entity Links** configuration is to define the network connection between Session Manager and CS1000 SIP Gateway. In this testing, the trusted link was configured with protocol UDP and port 5060. **Figure 50** shows SIP Entity **car2-ssg-mtsallstream** was successfully added.

- **Name:** car2-ssg-mtsallstream
- **FQDN or IP Address:** 110.10.97.190
- **Type:** Other
- **Location:** Belleville,Ont,Ca
- **SIP Link Monitoring:** Use Session Manager Configuration

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / SIP Entities - SIP Entity Details

SIP Entity Details

Commit Cancel

Help ?

General

* Name: car2-ssg-mtsallstream

* FQDN or IP Address: 110.10.97.190

Type: Other

Notes:

Adaptation:

Location: Belleville, Ont, Ca

Time Zone: America/New_York

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Entity Links

Add Remove

1 Item | Refresh Filter: Enable

<input type="checkbox"/>	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
<input type="checkbox"/>	DevASM	UDP	* 5060	car2-ssg-mtsallstream	* 5060	<input checked="" type="checkbox"/>

Select : All, None

* Input Required

Commit Cancel

Figure 50 – Adding SIP Entity for CS1000 SIP Gateway

b) Click **Commit**.

Note: In the **Entity Links** configuration, the option “**Trusted**” is mandatory.

5.8.5. Create SIP Entity for Avaya Aura SBC

This section shows how to configure System Manager to add a SIP Entity for Avaya Aura SBC (hereafter referred to as AA-SBC).

a) In the **Introduction to Network Routing Policy** page (not shown), click **SIP Entities** link on the left menu to open **SIP Entities – SIP Entities** page. Then click button **New** (not shown) to add a new entity for AA-SBC.

The **Entity Links** configuration is to define the network connection between Session Manager and AA-SBC. In this testing, the trusted link was configured with protocol UDP and port 5060. **Figure 51** shows SIP Entity AA-SBCMTSAllStream was successfully added.

- **Name:** AA-SBCMTSAllStream
- **FQDN or IP Address:** 110.10.97.216
- **Type:** Other
- **Location:** Belleville,Ont,Ca
- **SIP Link Monitoring:** Use Session Manager Configuration
- **SIP Entity Link:** Trusted

AVAYA Avaya Aura® System Manager 6.1 Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / SIP Entities - SIP Entity Details

SIP Entity Details Help ? Commit Cancel

General

* Name: AASBCMTSAllStream

* FQDN or IP Address: 110.10.97.216

Type: Other

Notes:

Adaptation:

Location: Belleville,Ont,Ca

Time Zone: America/New_York

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

Entity Links Add Remove

1 Item | Refresh Filter: Enable

<input type="checkbox"/>	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted
<input type="checkbox"/>	DevASM	UDP	* 5060	AASBCMTSAllStream	* 5060	<input checked="" type="checkbox"/>

Select : All, None

* Input Required Commit Cancel

Figure 51 – Adding SIP Entity for Acme Packet SBC

b) Click **Commit**.

Note: In the **Entity Links** configuration, the option “**Trusted**” is mandatory.

5.8.6. Create Routing Policy for inbound call

This section shows how to configure Session Manager to add a **Routing Policy** for inbound call from MTS Allstream to CS1000. As part of the dialing plan configuration, the **Routing Policy** instructs Session Manager to route SIP calls from PSTN to the CS1000 SIP Gateway to terminate.

The “**Time of Day**” setting defines the range to apply the **Routing Policy** during the day. In this testing, just simply select the default name **24/7**. It means the **Routing Policy** is always in effect.

Figure 52 shows policy **MTSAllStream_To_CS1K** was created.

- Name: MTSAllStream_To_CS1K
- SIP Entity as Destination: car2-ssg-mtsallstream
- Time of Day: 24/7

The screenshot displays the Avaya Aura System Manager 6.1 web interface. The left sidebar shows a navigation menu with 'Routing Policies' selected. The main content area is titled 'Routing Policy Details' and contains several sections:

- General:** The 'Name' field is set to 'MTSAllStream_To_CS1K'. The 'Disabled' checkbox is unchecked. The 'Notes' field is empty.
- SIP Entity as Destination:** A table lists the destination entity.
- Time of Day:** A table lists the time ranges for the policy.
- Dial Patterns:** A table lists the dial patterns associated with the policy.
- Regular Expressions:** A table for regular expressions, currently empty.

At the bottom of the form, there are 'Commit' and 'Cancel' buttons, and a note that says '* Input Required'.

Name	FQDN or IP Address	Type	Notes
car2-ssg-mtsallstream	110.10.97.190	Other	

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Pattern	Min	Max	Emergency Call	SIP Domain	Originating Location	Notes
647776	10	36	<input type="checkbox"/>	mtsallstream.com	Belleville,Ont,Ca	

Pattern	Rank Order	Deny	Notes
---------	------------	------	-------

Figure 52 – Adding Routing Policy for inbound call

5.8.7. Create Routing Policy for outbound calls

Please refer to **Section 5.8.6** to create a **Routing Policy** for outbound calls. Based on the policy, Session Manager routes calls from CS1000 to SIP Entity AA-SBC (created in **Section 5.8.5**) as destination, then AA-SBC sends the request to Bell Canada.

Figure 53 shows policy **CS1K_To_MTSAllStream** was created.

- Name: CS1K_To_MTSAllStream
- SIP Entity as Destination: AA-SBCMTSAllStream
- Time of Day: 24/7

The screenshot shows the Avaya Aura System Manager 6.1 interface. The left sidebar contains a navigation menu with options: Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies (highlighted), Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Routing Policy Details' and shows the configuration for the policy 'CS1K_To_MTSAllStream'. The 'General' tab is active, displaying the policy name, a 'Disabled' checkbox, and a 'Notes' field. The 'SIP Entity as Destination' section shows a table with one entry: 'AASBCMTSAllStream' with FQDN or IP Address '110.10.97.216' and Type 'Other'. The 'Time of Day' section shows a table with one entry: '24/7' with Start Time '00:00' and End Time '23:59'.

Name	FQDN or IP Address	Type	Notes
AASBCMTSAllStream	110.10.97.216	Other	

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	00:00	23:59	Time Range 24/7

Figure 53 – Adding Routing Policy for outbound call

5.8.8. Create Dial Pattern for inbound call

In this testing, MTS Allstream assigns DID numbers with prefix **647** to CS1000. The DIDs are in 10 digits format. The Dial Pattern **647** on Session Manager is configured as an entry of Routing Policy MTSAllStream_To_CS1K (created in **Section 5.8.6**). It means when Session Manager receives inbound calls with prefix **647**, it routes calls to the CS1000 SIP Gateway car2-ssg-mtsallstream as the destination. **Figure 54** shows policy **Dial Pattern 647** was created.

a) In the **Introduction to Network Routing Policy** page (not shown), click **Dial Patterns** link on the left menu to open **Dial Patterns – Dial Pattern Details** page. Then click button **New** (not shown) to add a new Dial Pattern for inbound calls with prefix **647**.

b) Under **Originating Locations and Routing Policy**, click **Add** (not shown). In the **Dial Patterns – Originating Locations and Routing Policy List** page (not shown), select

Originating Location entry **Belleville,Ont,Ca** (created in **Section 5.8.2**) and **Routing Policies** entry **MTSAllStream_To_CS1K** (created in **Section 5.8.6**).

- Pattern: **647**
- Min: 10 (digits)
- Max: 36 (default)
- SIP Domain: mtsallstream.com
- Originating Location Name: Belleville,Ont,Ca
- Routing Policy Name: MTSAllstream_To_CS1K
- Routing Policy Destination: car2-ssg-mtsallstream

AVAYA Avaya Aura® System Manager 6.1 Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Dial Patterns - Dial Pattern Details

Dial Pattern Details Help ? Commit Cancel

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

SIP Domain:

Notes:

Originating Locations and Routing Policies

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Belleville,Ont,Ca		MTSAllStream_To_CS1K	0	<input type="checkbox"/>	car2-ssg-mtsallstream	

Select : All, None

Denied Originating Locations

0 Items Refresh Filter: Enable

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

* Input Required Commit Cancel

Figure 54 – Adding Dial Pattern for inbound call

c) Click **Commit**.

5.8.9. Create Dial Pattern for outbound calls

The **Dial Pattern** for outbound calls is associated to the **Routing Policy** **CS1K_To_MTSAllStream** (created in **Section 5.8.7**). The **Dial Pattern** configuration on Session Manager has to match the dialing plan configure on CS1000 (**Section 5.6**).

a) Dial Pattern with prefix **1**. For long distance calls, CS1000 sends 11 digits with prefix **1** to MTS Allstream via AA-SBC. Please refer to **Section 5.8.8** to create a Dial Pattern. The detail configuration of **Dial Pattern 1** is shown in **Figure 55**.

- Pattern: **1**
- Min: 11 (digits)
- Max: 36 (default)
- SIP Domain: mtsallstream.com
- Originating Location Name: Belleville,Ont,Ca
- Routing Policy Name: CS1K_To_MTSAllstream
- Routing Policy Destination: AA-SBCMTSAllStream

AVAYA Avaya Aura® System Manager 6.1 Help | About | Change Password | Log off admin

[Routing](#) [Home](#)

Dial Pattern Details Commit Cancel

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

SIP Domain:

Notes:

Originating Locations and Routing Policies

[Add](#) [Remove](#)

1 Item [Refresh](#) Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Belleville,Ont,Ca		CS1K_To_MTSAllStream	0	<input type="checkbox"/>	AASBCMTSAllStream	

Select : All, None

Denied Originating Locations

[Add](#) [Remove](#)

0 Items [Refresh](#) Filter: Enable

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

* Input Required Commit Cancel

Figure 55 – Adding Dial Pattern for outbound long distance call with prefix 1

b) Dial Pattern with prefix **0**. CS1000 sends **0** or **0+10** digits to reach operator at MTS Allstream. MTS Allstream also uses the same prefix **011** for outbound international calls. Thus, the Dial Pattern **0** should have flexible length. Please refer to **Section 5.8.8** to create a Dial Pattern. The detail configuration of **Dial Pattern 0** is shown in **Figure 56**.

- Pattern: **0**
- Min: 1 (digits)
- Max: 36 (default)
- SIP Domain: mtsallstream.com
- Originating Location Name: Belleville,Ont,Ca
- Routing Policy Name: CS1K_To_MTSAllstream
- Routing Policy Destination: AA-SBCMTSAllStream

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing x Home

Home / Elements / Routing / Dial Patterns - Dial Pattern Details

Dial Pattern Details

General

* Pattern: 0

* Min: 1

* Max: 36

Emergency Call: ☐

SIP Domain: mtsallstream.com

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Belleville,Ont,Ca		CS1K_To_MTSAllStream	0	<input type="checkbox"/>	AASBCMTSAllStream	

Select : All, None

Denied Originating Locations

Add Remove

0 Items Refresh Filter: Enable

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

* Input Required

Commit Cancel

Figure 56 – Adding Dial Pattern for outbound special call with prefix 0

c) Dial Pattern with prefix **411**. As a part of the dialing plan, the **Dial Pattern 411** routes calls from CS1000 to 411 services hosted on MTS Allstream. Please refer to **Section 5.8.8** to create a Dial Pattern. The detail configuration of **Dial Pattern 411** is shown in **Figure 57**.

- Pattern: **411**
- Min: 3 (digits)
- Max: 36 (default)
- SIP Domain: mtsallstream.com
- Originating Location Name: Belleville,Ont,Ca
- Routing Policy Name: CS1K_To_MTSAllstream
- Routing Policy Destination: AA-SBCMTSAllStream

AVAYA Avaya Aura® System Manager 6.1 Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Dial Patterns - Dial Pattern Details

Dial Pattern Details Help ? Commit Cancel

General

* Pattern: 411

* Min: 3

* Max: 36

Emergency Call: ☐

SIP Domain: mtsallstream.com

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Belleville,Ont,Ca		CS1K_To_MTSAllStream	0	<input type="checkbox"/>	AASBCMTSAllStream	

Select : All, None

Denied Originating Locations

Add Remove

0 Items Refresh Filter: Enable

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

* Input Required Commit Cancel

Figure 57 – Adding Dial Pattern for outbound 411 calls

e) Dial Pattern with prefix **911**. As a part of the dialing plan, the **Dial Pattern 911** routes calls from CS1000 to 911 emergency services hosted on MTS Allstream. Please refer to **Section 5.8.8** to create a Dial Pattern. The detail configuration of **Dial Pattern 911** is shown in **Figure 58**.

- Pattern: **911**
- Min: 3 (digits)
- Max: 36 (default)
- SIP Domain: siptrunking.bell.ca
- Originating Location Name: Belleville,Ont,Ca
- Routing Policy Name: **CS1K75_TO_BELLCANADA**
- Routing Policy Destination: ACME

Home / Elements / Routing / Dial Patterns - Dial Pattern Details

Dial Pattern Details

General

* Pattern: 911

* Min: 3

* Max: 36

Emergency Call: ☐

SIP Domain: siptrunking.bell.ca

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Belleville,Ont,Ca		CS1K75_TO_BELLCANADA	0	<input type="checkbox"/>	ACME	CS1K75_TO_BELLCANADA

Select : All, None

Denied Originating Locations

Add Remove

0 Items Refresh Filter: Enable

<input type="checkbox"/>	Originating Location	Notes
--------------------------	----------------------	-------

* Input Required

Commit Cancel

Figure 58 – Adding Dial Pattern for outbound 911 calls

6. Configure Avaya Aura® Session Border Controller

This section describes the configuration of the Avaya Aura® Session Border Controllers necessary for interoperability with the CS1000 and MTS Allstream systems.

This section will not attempt to describe each component in its entirety but instead will highlight critical fields in each component which relates to the functionality in these Application Notes and the direct connection to CS1000. The remaining fields are generally the default/standard value used by the AA-SBC for that field.

In this testing, according to the configuration reference **Figure 1**, the Avaya elements reside on the Private side and the MTS Allstream system reside on the Public side of the network.

6.1. Service Provider Pre-installation Wizard

Service Provider Pre-installation Wizard is a tool distributed along with SBC release 6.0 installation packages. This wizard collects network configuration information relevant to MTS Allstream, and generates template file with extension EPW. Later on, EPW file is uploaded to the wizard during SBC installation.

Run **SP_Pre-Installation_Wizard_5273.exe** to install the **Service Provider Pre-installation Wizard** on a Window based PC. After the installation is complete, invoke the wizard from **Start > All Programs > SP Pre-installation Wizard > Run SP Pre-installation Wizard**.

a) The **SP Pre-installation Wizard** will be run in a web browser. Under **Select a template**, select **SBCT** from the drop down list, and then click **Next Step** as shown in **Figure 60**.

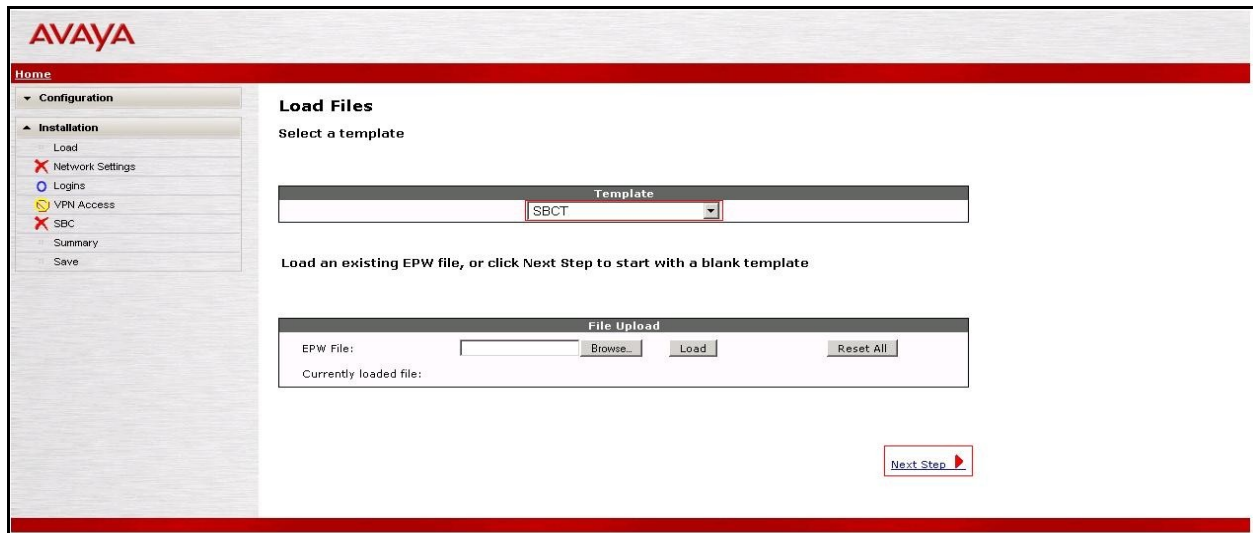


Figure 59: SP Pre-installation Wizard; Select a template

b) **Network Settings** is to configure internal interface of the AA-SBC to connect to the enterprise CS1000 network as shown in **Figure 60**.

- **Domain0 IP Address:** IP address of System Platform system domain 0, e.g. 110.10.97.214
- **CDom IP Address:** IP address of System Platform console domain, e.g. 110.10.97.215
- **Gateway IP Address:** 110.10.97.193
- **Network Mask:** 255.255.255.192
- **SBC:** IP address of SBC internal interface, e.g. 110.10.97.216
- **Hostname:** AA-SBC
- **Domain:** bvwddev.com

AVAYA

Home

Configuration

Installation

Load

Network Settings

Logins

VPN Access

SBC

Summary

Save

Network Settings

Enter network settings

Domain-0 IP Address: 110.10.97.214

CDom IP Address: 110.10.97.215

Gateway IP Address: 110.10.97.193

Network Mask: 255.255.255.192

Primary DNS:

Secondary DNS (Optional):

Default Search List (Optional):

HTTPS Proxy (Optional) [IP Address:Port Number]:

Virtual Machine	IP Address	Hostname	Domain
SBC	110.10.97.216	AASBC	bvwddev.com (Optional)

Default Domain: (Optional)

Apply to all VMs

Previous Step

Next Step

Figure 60: SP Pre-installation Wizard; Network Settings

c) The **Service logins for SBC (optional)** is to define password for account **craft**, **init** and **dadmin** as shown in **Figure 61**.

Login name	Password	Re-type password
craft
init
dadmin

Figure 61: SP Pre-installation Wizard; Services logins for SBC (optional)

d) Next step is the **VPN Access**. The SIP Trunk connect to MTS Allstream is not behind the VPN, so select **No** (VPN mode is disabled) and click **Next Step**.

Would you like to configure the VPN remote access parameters for System Platform?

☐ Yes ☒ No

VPN Access Configuration

VPN Router IP Address (Optional)

Remote Access Network

Remote Access Network Subnet Mask

The data on this page is used to configure static routes on System Platform to enable remote VPN access to the component applications and the Avaya Aura™ System Platform Web Console.

Once the template has been installed, the user must access the Avaya Aura™ System Platform Web Console and check the "Server Management -> Static Route Configuration" page to verify that the static routes configured by the Wizard are suitable for the intended remote access application.

If in doubt, please refer to the documentation.

Figure 62: SP Pre-installation Wizard; VPN Access

e) **Session Border Controller Data** is to define IP address of MTS Allstream SBC used for SIP signaling and for RTP as shown in **Figure 63**.

SIP Service Provider Data:

- **Service Provider:** Generic
- **Port:** 5060
- **IP Address1:** IP address of MTS Allstream SBC used for SIP signaling, e.g. 220.20.1.12
- **Signalling/media network1:** network address of MTS Allstream SBC, e.g. 220.20.1.10/27

SBC Network Data:

- **Public:** IP address of AA-SBC to connect to MTS Allstream system, e.g. 110.10.98.108
- **Net Mask:** 255.255.255.224
- **Gateway:** 110.10.98.97

Enterprise SIP Server:

- **SIP Domain:** mtsallstream.com
- **IP Address1:** the IP address of Session Manager (please refer to **Section 5.8**), e.g. 110.10.97.198
- **Transport1:** UDP

The screenshot shows the Avaya SBC Pre-installation Wizard. The left sidebar contains a navigation menu with options: Home, Configuration, Installation, Load, Network Settings, Logins, VPN Access, SBC, Summary, and Save. The main content area is titled 'SBC' and 'Session Border Controller Data'. It contains three sections: 'SIP Service Provider Data', 'SBC Network Data', and 'Enterprise SIP Server'. The 'SIP Service Provider Data' section has fields for Service Provider (Generic), Port (5060), IP Address1 (220.20.2.12), Signalling/Media Network1 (220.20.2.0), Signalling/Media Netmask1 (255.255.255.224), IP Address2 (Optional), Signalling/Media Network2 (Optional), Signalling/Media Netmask2 (Optional), and Hunting (Optional). The 'SBC Network Data' section is a table with columns: Interface, IP Address, Net Mask, and Gateway. It shows Private (Management) and Public interfaces. The 'Enterprise SIP Server' section has fields for SIP Domain (mtsallstream.com), IP Address1 (110.10.97.198), Transport1 (UDP), IP Address2 (Optional), Transport2 (Optional), and Hunting (Optional). At the bottom, there are 'Previous Step' and 'Next Step' buttons.

Interface	IP Address	Net Mask	Gateway
Private (Management)	110.10.97.216	255.255.255.192	110.10.97.193
Public	110.10.98.108	255.255.255.224	110.10.98.97

Figure 63: SP Pre-installation Wizard; Session Border Controller Data

f) **Summary** is to give an overview of the configuration as shown in **Figure 64**. Scroll down and click on **Next Step** (not shown).

AVAYA

Home

Configuration

Installation

- Load
- Network Settings
- Logins
- VPN Access
- SBC
- Summary
- Save

Summary

Network Settings	
Domain-0 Address	110.10.97.214
CDom Address	110.10.97.215
Gateway Address	110.10.97.193
Network Mask	255.255.255.192
Primary DNS	Not set
Secondary DNS	Not set
Default Search List	Not set
HTTPS Proxy	Not set

Virtual Machine	IP Address	Hostname	Domain
SBC	110.10.97.216	AASBC	bvwdev.com
Default Domain			Not set

Logins	
SBC craft Password	*****
SBC init Password	*****
SBC dadmin Password	*****

VPN Access	
VPN Access	Not Configured

SBC	
Service Provider	generic
Service Provider Port	5060
Service Provider IP Address	220.20.2.12
Service Provider Signalling/Media Network1	220.20.2.0
Service Provider Signalling/Media Netmask1	255.255.255.224
Service Provider IP Address2	Not set
Service Provider Signalling/Media Network2	Not set
Service Provider Signalling/Media Netmask2	Not set
Service Provider Hunting	Not set

Figure 64: SP Pre-installation Wizard; Summary

g) **Save** is to give an option to save the configuration as an EPW file. Click **Accept** then **Save EPW file** as shown in **Figure 65**.

AVAYA

Home

Configuration

Installation

- Load
- Network Settings
- Logins
- VPN Access
- SBC
- Summary
- Save

Save

The following required fields have not been set

[Primary DNS](#)

The following optional fields have not been set

- [Default Search List](#)
- [Secondary DNS](#)
- [HTTPS Proxy](#)
- [Default Domain](#)
- [SBC Service Provider IP Address 2](#)
- [SBC Service Provider Hunting](#)
- [SBC Service Provider Media Netmask2](#)
- [SBC Service Provider Media Network2](#)
- [SBC Enterprise SIP Server IP2](#)
- [SBC Enterprise SIP Server Transport2](#)
- [SBC Enterprise SIP Server Hunting](#)

WARNING - the country specific values configured by the installation wizard are based upon those that have typically been used, in similar installations, in those countries in the past. Due to the many different ways in which systems may be configured, even within the same country, it is your responsibility to verify (after installation) that all parameters are consistent with those required by local and national laws and that the system has been correctly configured to guard against toll fraud and other security vulnerabilities, see *Avaya Toll Fraud and Security Handbook*, 555-025-600.

This is particularly important for emergency service numbers. **Avaya is not responsible or liable for any damages resulting from toll fraud, or failure to configure the system to comply with local or national laws or from misplaced emergency calls made from an Avaya endpoint.**

Figure 65: SP Pre-installation Wizard; Save

h) Download and save the EPW file.

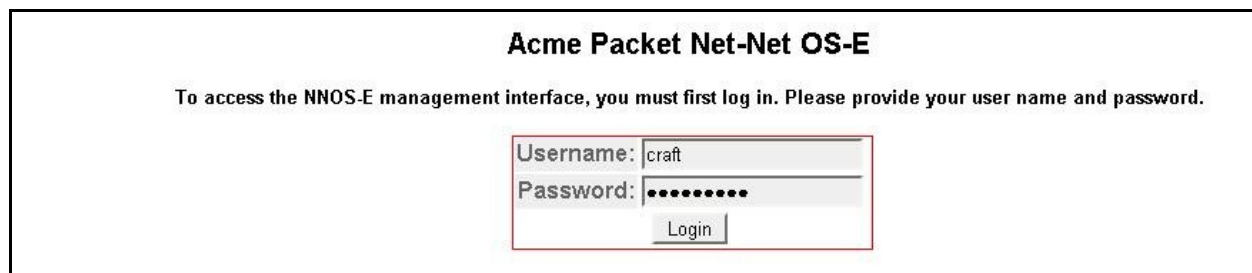
6.2. AA-SBC Installation

To install Avaya Aura SBC, follow installation guide provided on <http://support.avaya.com>. The installation wizard (not shown) is an automation tool.

During installation, EPW file is needed. Please use EPW file created in **Section 6.1** to upload to the wizard. After the installation is complete, continue to configure the SBC as described in **Section 6.3**.

6.3. Administer Enterprise Servers

To login to AA-SBC, go to <https://SBCIPAddress/> and enter username as craft and appropriate password.



Acme Packet Net-Net OS-E

To access the NNOS-E management interface, you must first log in. Please provide your user name and password.

Username: craft

Password:

Login

Figure 66: Login to AA-SBC

During installation, the information in the EPW file was used to populate the entry “**server Telco1**”, which is the information of MTS Allstream SBC for SIP Trunking and the entry “**server PBX1**” which is the information of Session Manager.

6.3.1. Configuration of “server Telco1”

Select **Configuration > vsp > enterprise > servers > sip-gateway Telco**. Figure 67 shows detail configuration of IP connectivity of entry **Telco1**. Verify IP address, transportation protocol, and port as defined in step e of Section 6.1.

Under **Policy** setting, configure **outbound-session-config-pool-entry** to associate to **vsp\session-config-pool\entry ToTelco**.

The screenshot shows the Avaya Aura Configuration interface. The left sidebar shows the navigation tree with 'Configuration: all' expanded, and 'vsp' > 'enterprise' > 'servers' > 'sip-gateway Telco' selected. The main content area is titled 'Configure vsp\enterprise\servers\sip-gateway Telco'. It includes tabs for 'Set', 'Reset', 'Back', 'Copy', and 'Delete'. Below the tabs are links for 'Manage connections', 'Log instant messages', 'Record media', 'Record files', 'Set up accounting', 'Change "from" URI', and 'Change "to" URI'. The 'general' section contains fields for 'name' (Telco), 'admin' (enabled), 'domain', and 'failover-detection' (ping). The 'servers' section shows a table with columns for 'server', 'admin', 'host', 'transport', 'port', 'outbound-normalization', 'inbound-normalization', and 'admission-control'. The table has one row for 'server Telco1' with values: enabled, 220.20.2.12, UDP, 5060, Configure, Configure, disabled. Below the table are links for 'Add server' and 'Add handle-response'. The 'policy' section has dropdowns for 'inbound-session-config-pool-entry' and 'outbound-session-config-pool-entry' (vsp\session-config-pool\entry ToTelco). The 'other properties' section has fields for 'carrier' (default) and 'routing-tag'. At the bottom are 'Set', 'Reset', 'Back', and 'Copy' buttons.

server	admin	host	transport	port	outbound-normalization	inbound-normalization	admission-control
server Telco1	enabled	220.20.2.12	UDP	5060	Configure	Configure	disabled

Figure 67: server-Telco1 Configuration

6.3.2. Configuration of “server PBX1”

Select **Configuration > vsp > enterprise > servers > sip-gateway PBX**. **Figure 68** shows detail configuration of IP connectivity of entry **PBX1**. Verify IP address, transportation protocol, and port as defined in step b of **Section 6.1**.

Under **Policy** setting, configure **outbound-session-config-pool-entry** to associate to **vsp\session-config-pool\entry ToPBX**.

The screenshot displays the Avaya Aura Configuration web interface. The left sidebar shows a navigation tree with 'Configuration' selected. The main content area is titled 'Configure vsp\enterprise\servers\sip-gateway PBX'. It includes a 'general' section with fields for name (PBX), admin (enabled), domain (mtsallstream.com), and failover-detection (ping). Below this is a 'servers' section with a table listing server configurations. The table has columns for server, admin, host, transport, port, outbound-normalization, and inbound-normalization. A row for 'server PBX1' is highlighted, showing an enabled admin, host 10.10.97.198, transport UDP, and port 5060. The 'policy' section shows 'inbound-session-config-pool-entry' set to a default value and 'outbound-session-config-pool-entry' set to 'vsp\session-config-pool\entry ToPBX'. The 'other properties' section includes fields for carrier (default) and routing-tag.

server	admin	host	transport	port	outbound-normalization	inbound-normalization
server PBX1	enabled	10.10.97.198	UDP	5060	Configure	Configure

Figure 68: server-PBX1 Configuration.

6.4. Administer Heartbeat

AA-SBC was configured to send OPTION/ping to MTS Allstream and Session Manager for keep alive purpose.

To send OPTION/ping to MTS Allstream, select **Configuration > vsp > enterprise > servers > sip-gateway Telco** then select “ping” for “failover-detection” as shown in **Figure 69**.

The screenshot shows the Avaya Aura Configuration interface. The top navigation bar includes 'Home', 'Configuration', 'Status', 'Call Logs', 'Event Logs', 'Actions', 'Services', 'Keys', 'Access', and 'Tools'. The left sidebar shows a tree view with 'Configuration: all' expanded, and 'servers' under 'enterprise' selected. The main content area is titled 'Configure vspenterprise\servers\sip-gateway Telco'. It includes buttons for 'Set', 'Reset', 'Back', 'Copy', and 'Delete'. Below these are links for 'Manage connections', 'Log instant messages', 'Record media', 'Record files', 'Set up accounting', 'Change "from:" URI', and 'Change "to:" URI'. The 'general:' section contains fields for '* name' (Telco), 'admin' (enabled), 'domain', and 'failover-detection' (ping). The 'servers:' section shows a 'server-pool' button and a 'Delete' button.

Figure 69: KeepAlive Configuration for sip-gateway Telco

To send OPTION/ping to the Session Manager, select **Configuration > vsp > enterprise > servers > sip-gateway PBX** then select “ping” for “failover-detection” as shown in **Figure 70**.

The screenshot shows the Avaya Aura Configuration interface. The left sidebar displays a tree view under 'Configuration: all' with the path 'cluster > vsp > enterprise > servers > sip-gateway PBX' selected. The main content area is titled 'Configure vspenterprise\servers\sip-gateway PBX' and includes a 'Show advanced' link. Below the title are buttons for 'Set', 'Reset', 'Back', 'Copy', and 'Delete'. A link for 'Help' and 'Index' is also present. The 'general:' section contains the following fields:

* name	PBX
admin	enabled (Resource is active)
domain	mtsallstream.com
failover-detection	ping (Use OPTIONS to detect failures)

The 'servers:' section shows a 'server-pool' entry with a 'Delete' link.

Figure 70: KeepAlive Configuration for sip-gateway PBX

6.5. Administer dial-plan

AA-SBC was pre-configured with typical dial-plans to route SIP calls from CS1000 to MTS Allstream and vice versa.

6.5.1. The entry “source-route FromPBX”

The entry “source-route FromPBX” as shown in **Figure 71** below is to route SIP calls from CS1000 to MTS Allstream.

- **source-server:** vsp\enterprise\servers\sip-gateway **PBX**
- **peer server:** vsp\enterprise\servers\sip-gateway **Telco**
- **location-match-preferred:** up-to-outbound-peer
- **priority:** 100 (default)
- **condition-list-match-secondary:** false
- **other properties:**
 - o **admin:** enabled
 - o **action:** forward
 - o **apply-to-methods:** Select All

The screenshot displays the Avaya Aura Configuration web interface. The left sidebar shows a tree view of the configuration hierarchy, with 'Configuration: all' expanded. The main content area is titled 'Configure vsp\dial-plan\source-route FromPBX'. It includes a 'general' section with fields for name, description, source-match, peer, location-match-preferred, priority, condition-list, and condition-list-match-secondary. The 'other properties' section includes fields for admin, action, and apply-to-methods. The 'apply-to-methods' field is set to 'Select All'.

general:	
* name	FromPBX
description	
* source-match	
* type	server
* source-server	vsp\enterprise\servers\sip-gateway PBX
peer	
type	server (Peer is a SIP server)
server	vsp\enterprise\servers\sip-gateway Telco
location-match-preferred	up-to-outbound-peer (Outbound peer determines whether preferred)
priority	100 (from 0 to 999,999, default=100)
condition-list	Configure
condition-list-match-secondary	false

other properties:	
admin	enabled (Resource is active)
action	forward (forward the INVITE to the server specified in the header)
apply-to-methods	INVITE REFER MESSAGE INFO Select All Unselect All

Figure 71: dial-plan “source-route FromPBX”

6.5.2. The entry “source-route FromTelco”

The entry “source-route FromTelco” as shown in **Figure 72** below is to route SIP calls from MTS Allstream to CS1000.

- **source-server:** vsp\enterprise\servers\sip-gateway Telco
- **peer server:** vsp\enterprise\servers\sip-gateway PBX
- **location-match-preferred:** up-to-outbound-peer
- **priority:** 100 (default)
- **condition-list-match-secondary:** false
- **other properties:**
 - o **admin:** enabled
 - o **action:** forward
 - o **apply-to-methods:** Select All

The screenshot displays the Avaya Aura Configuration web interface. The top navigation bar includes tabs for Home, Configuration, Status, Call Logs, Event Logs, Actions, Services, Keys, Access, and Tools. The left sidebar shows a tree view of the configuration hierarchy, with 'source-route FromTelco' selected under the 'dial-plan' section. The main content area is titled 'Configure vsp\dial-plan\source-route FromTelco' and contains several sections: 'general' and 'other properties'. The 'general' section includes fields for name, description, source-match, type, source-server, peer, type, server, location-match-preferred, priority, condition-list, and condition-list-match-secondary. The 'other properties' section includes fields for admin, action, and apply-to-methods. The configuration is set to route SIP calls from MTS Allstream to CS1000.

general:	
* name	FromTelco
description	
* source-match	
* type	server
* source-server	vsp\enterprise\servers\sip-gateway Telco
peer	
type	server (Peer is a SIP server)
server	vsp\enterprise\servers\sip-gateway PBX
location-match-preferred	up-to-outbound-peer (Outbound peer determines whether preferred)
priority	100 (from 0 to 999,999, default=100)
condition-list	Configure
condition-list-match-secondary	false

other properties:	
admin	enabled (Resource is active)
action	forward (forward the INVITE to the server specified in the header)
apply-to-methods	INVITE REFER MESSAGE INFO

Figure 72: dial-plan “source-route Telco”

6.6. Administer session-config-pool “entry ToTelco”

6.6.1. Administer sip-settings

AA-SBC has a feature to re-transmit IP packets to prevent packet lost when travel over internet. By default, **max-retransmissions** value is set to 1. To increase **max-retransmissions**, select **Configuration vsp\session-config-pool\entry ToTelco\sip-settings\other properties**, and change the value of **max-retransmissions** from 1 to 5 as shown in **Figure 73**.

The screenshot displays the Avaya Aura Configuration web interface. The left sidebar shows a tree view of the configuration hierarchy, with 'entry ToTelco' selected under 'session-config-pool'. The main content area is divided into two sections: 'session-options' and 'other properties'. In the 'other properties' section, the 'max-retransmissions' field is highlighted with a red box and set to the value '5'. Other fields like 'route-hdr-add-register-msg' and 'route-hdr-preprocess-strip' are set to 'disabled'. The 'session-timeout' is set to '300' seconds, and 'session-duration-max' is set to '0' seconds. The 'enum-fail-response' section shows 'enum-lookup-failed-action' set to 'ignore'. The 'dns-fail-response-code' is set to '404', and 'dns-fail-response-string' is set to 'Not Found'. The 'supported-inleg' and 'supported-outleg' fields are empty. The 'persistent-destination-address' is set to 'true', and 'loop-detection-threshold' is set to '2'. The 'sip-signaling-encryption' is set to 'unspecified', and 'share-transport-connection' is set to 'remoteAddr'. At the bottom of the configuration area, there are 'Set', 'Reset', and 'Back' buttons.

session-options:	
session-timeout	300 seconds (from 1 to 1,000,000, default=300)
session-duration-max	0 seconds (from 0 to 1,000,000, default=0)

other properties:	
max-retransmissions	5 (from 0 to 32, default=1)
symmetric-signaling	disabled (Resource is inactive)
redirect-preserve-session-config	disabled (Resource is inactive)
max-forwards	70
enum-fail-response	* enum-lookup-failed-action ignore (ignore failed lookup)
dns-fail-response-code	404 (from 0 to 65,535)
dns-fail-response-string	Not Found
supported-inleg	
supported-outleg	
persistent-destination-address	true
loop-detection-threshold	2 (from 1 to 256, default=2)
sip-signaling-encryption	unspecified (TLS is allowed, but not required)
share-transport-connection	remoteAddr (reuse the connection when both the remote ip and port match)

Figure 73: Increase the max- retransmissions

AA-SBC can **overwrite** the Quality of Service (DSCP) value for SIP packets. This value can be set at **Configuration vsp\session-config-pool\entry ToTelco\sip-settings\message options\outleg-tos**. Figure 74 shows **outleg-tos** was set to **overwrite** with DSCP 20.

The screenshot displays the Avaya Aura Configuration web interface. On the left, a navigation tree shows the path: Configuration > vsp > session-config-pool > entry ToTelco > sip-settings. The 'outleg-tos' setting is highlighted. The main panel shows the configuration for 'message-options' and 'header-options'. The 'outleg-tos' setting is configured with 'mode' set to 'overwrite' and 'value' set to '20' (from 0 to 255).

message-options:	
preserve-call-id	disabled (Resource is inactive)
handle-3xx-locally	disabled (Resource is inactive)
handle-3xx-locally-server-arbitration	disabled (Resource is inactive)
handle-3xx-locally-lookup-original-invoke	disabled (Resource is inactive)
inleg-tos	mode: preserve
outleg-tos	mode: overwrite value: 20 (from 0 to 255)
auto-accept-reinvite-with-no-sdp-on-in-leg	disabled (Resource is inactive)
auto-accept-reinvite-with-no-sdp-on-out-leg	disabled (Resource is inactive)

header-options:	
strip-route-header	disabled (Resource is inactive)
route-hdr	none (No RecordRoute headers added)
route-hdr-use-fqdn	disabled (Resource is inactive)
route-hdr-uri-host	
route-hdr-add-register-msg	disabled (Resource is inactive)
route-hdr-preprocess-strip	disabled (Resource is inactive)

Figure 74: DSCP setting for SIP message

By default AA-SBC does not forward PRACK from CS1000 to MTS Allstream. It causes issue with ringback tone cannot be sent to PSTN in case of offnet call forward no answer. To enable PRACK forwarding, go to **Configuration vsp\session-config-pool\entry ToTelco\sip-settings** click “**Show advance**” (not shown), then under “**message-options**” set “**forward-provisional-ack**” to **enable** (as shown in **Figure 75**).

The screenshot displays the Avaya Aura Configuration web interface. The left sidebar shows a tree view of the configuration hierarchy, with 'sip-settings' selected under 'session-config-pool' > 'entry ToTelco'. The main content area shows the 'message-options' configuration table.

message-options:	
compress-signaling	disabled (Resource is inactive)
preserve-call-id	disabled (Resource is inactive)
proxy-generate-100-trying	INVITE REFER MESSAGE INFO
handle-3xx-locally	disabled (Resource is inactive)
handle-3xx-locally-server-arbitration	disabled (Resource is inactive)
handle-3xx-locally-lookup-original-invite	disabled (Resource is inactive)
preserve-session-config-on-3xx	disabled (Resource is inactive)
ignore-provisional-tag	enabled (Resource is active)
strip-authint-qop	disabled (Resource is inactive)
preserve-cseq	disabled (Resource is inactive)
forward-provisional-ack	enabled (Resource is active)
terminate-transaction-on-bye	enabled (Resource is active)

Figure 75: Enable PRACK forwarding

6.6.2. Manipulate From, To, Request-URI, and P-Asserted-Identity headers.

The CS1000 SIP gateway was configured with domain name mtsallstream.com (please refer to **Section 5.5**). However, MTS Allstream expects to receive IP address instead of a domain name.

This section shows the configuration on AA-SBC to change domain name mtsallstream.com to an IP address. The change is applied to SIP headers From, To, Request-URI and P-Asserted-Identity.

a) Manipulate **From** header.

Select **Configuration vsp\session-config-pool\entry ToTelco\from-uri-specification**. Then change **host** to send **local-ip** as shown in **Figure 76**. AA-SBC presents its public IP address in the **From** header.

The screenshot displays the Avaya Aura Configuration web interface. The left sidebar shows a tree view of the configuration hierarchy: Configuration > vsp > session-config-pool > entry ToTelco > from-uri-specification. The main panel is titled 'Configure vsp\session-config-pool\entry ToTelco\from-uri-specification'. It contains several configuration fields:

Field	Value	Notes
user	from-uri	(Net-Net OS-E uses the value from the incoming FROM URI.)
host	local-ip	(Net-Net OS-E uses the local ip for the next-hop server.)
port	from-uri	(Net-Net OS-E uses the value from the incoming FROM URI.)
display	from-uri	(Net-Net OS-E uses the value from the incoming FROM URI.)
user-agent-aware-display-translation	disabled	(Resource is inactive)
transport	from-uri	(Net-Net OS-E uses the value from the incoming FROM URI.)
user-param	omit	
user-truncate-non-digits	disabled	(Resource is inactive)

Figure 76: Manipulate From header of session-config-pool “entryToTelco”

b) Manipulate **To** header.

Select **Configuration vsp\session-config-pool\entry ToTelco\to-uri-specification**. Then change **host** to send **next-hop** as shown in **Figure 77**. AA-SBC presents MTS Allstream SBC IP address in the **To** header.

The screenshot shows the Avaya Aura Configuration interface. The left sidebar displays a tree view of the configuration hierarchy, with 'to-uri-specification' selected under 'entry ToTelco'. The main panel is titled 'Configure vsp\session-config-pool\entry ToTelco\to-uri-specification'. It contains a table of configuration parameters:

Parameter	Value	Description
user	to-uri	(Net-Net OS-E uses the value from the incoming TO URI.)
host	next-hop	(Net-Net OS-E uses the IP address of the next-hop server.)
port	to-uri	(Net-Net OS-E uses the value from the incoming TO URI.)
display	to-uri	(Net-Net OS-E uses the value from the incoming TO URI.)
transport	to-uri	(Net-Net OS-E uses the value from the incoming TO URI.)
user-param	omit	
user-truncate-non-digits	disabled	(Resource is inactive)

Figure 77: Manipulate To header of session-config-pool “entryToTelco”

c) Manipulate **Request-URI** header.

Select **Configuration vsp\session-config-pool\entry ToTelco\request-uri-specification**. Then change **host** to send **next-hop** as shown in **Figure 78**. AA-SBC presents MTS Allstream SBC IP address in the **Request-URI** header.

The screenshot shows the Avaya Aura Configuration interface. The left sidebar displays a tree view of the configuration hierarchy, with 'request-uri-specification' selected under 'entry ToTelco'. The main panel is titled 'Configure vsp\session-config-pool\entry ToTelco\request-uri-specification'. It contains a table of configuration parameters:

Parameter	Value	Description
user	request-uri	(Net-Net OS-E uses the value from the incoming REQUEST URI.)
host	next-hop	(Net-Net OS-E uses the IP address of the next-hop server.)
port	request-uri	(Net-Net OS-E uses the value from the incoming REQUEST URI.)
transport	request-uri	(Net-Net OS-E uses the value from the incoming REQUEST URI.)
user-param	omit	
user-truncate-non-digits	disabled	(Resource is inactive)

Figure 78: Manipulate Request-URI header of session-config-pool “entryToTelco”

d) Manipulate **P-Asserted-Identity** header.

Select **Configuration vsp\session-config-pool\entry ToTelco\p-asserted-identity-uri-specification**. Then change **host** to send **local-ip** as shown in **Figure 79**. AA-SBC presents its public IP address in the **P-Asserted-Identity** header.

The screenshot shows the Avaya Aura Configuration interface. The left sidebar displays a tree view of the configuration hierarchy, with 'p-asserted-identity-uri-specification' selected under 'entry ToTelco'. The main panel shows the configuration for 'Configure vsp\session-config-pool\entry ToTelco\p-asserted-identity-uri-specification'. The configuration fields are as follows:

Field	Value	Notes
user	same-uri	(Net-Net OS-E uses the value from the uri being altered)
host	local-ip	(Net-Net OS-E uses the local ip for the next-hop server.)
port	same-uri	(Net-Net OS-E uses the value from the incoming uri being altered.)
display	same-uri	(Net-Net OS-E uses the value from the uri being altered)
transport	same-uri	(Net-Net OS-E uses the value from the incoming uri being altered.)
user-param	omit	
uri-parameter		Add uri-parameter

Figure 79: Manipulate P-Asserted-Identity header of session-config-pool “entryToTelco”

6.6.3. Administer media

This session shows the configuration to enable media anchoring on AA-SBC and set DSCP value for RTP.

To enable media anchoring, select **Configuration vsp\session-config-pool\entry ToTelco\media**. Then change **anchor** to **enable** as shown in **Figure 80**.

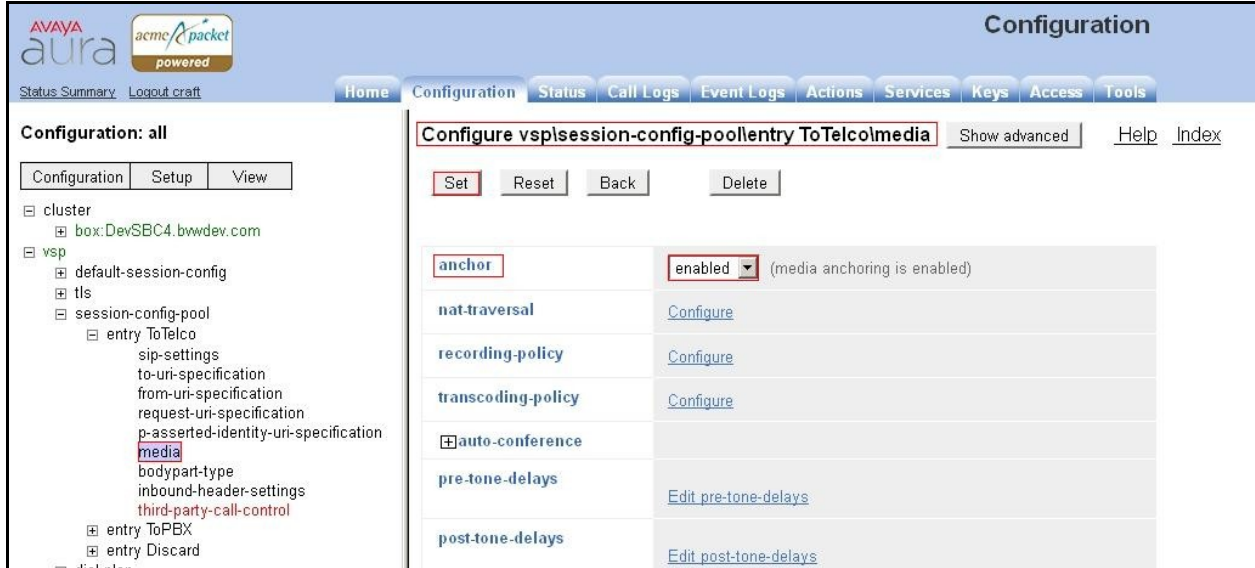


Figure 80: Enable media anchoring

AA-SBC can **overwrite** the Quality of Service (DSCP) value for RTP packets. This value can be set at **Configuration vsp\session-config-pool\entry ToTelco\media**. **Figure 81** shows **packet-marking** was set to **tos** with DSCP 60.

The screenshot displays the Avaya Aura Configuration web interface. The left sidebar shows a tree view of the configuration hierarchy, with 'media' selected under 'session-config-pool' > 'entry ToTelco'. The main panel shows the configuration for 'packet-marking'.

Configuration	Setup	View
cluster		
box: DevSBC4.bwwdev.com		
vsp		
default-session-config		
tls		
session-config-pool		
entry ToTelco		
sip-settings		
to-uri-specification		
from-uri-specification		
request-uri-specification		
p-asserted-identity-uri-specification		
media		
bodypart-type		
inbound-header-settings		
third-party-call-control		
entry ToPBX		
entry Discard		
dial-plan		
enterprise		
dns		
settings		

Configuration	Setup	View
pre-tone-delays		Edit pre-tone-delays
post-tone-delays		Edit post-tone-delays
introduction		Browse System Files
stop-introduction-after-180	<input type="checkbox"/>	
periodic-announcement		Configure
music-on-hold		Browse System Files
inactivity-timeout	<input type="checkbox"/> admin disabled (inactivity timer is disabled)	
inactivity-style	session (inactivity is determined across the entire session)	
monitor	<input type="checkbox"/> Create	
media-verify-config		Configure
packet-marking	* mode <input type="text" value="tos"/> (Specify TOS value to mark packets with) value <input type="text" value="60"/> (from 0 to 255)	
rtp-stats	<input type="checkbox"/> disabled (Resource is inactive)	
rtcp		
call-monitoring		Configure
mirror	<input type="checkbox"/> enabled (Resource is active)	
answer-media-loopback	<input type="checkbox"/> disabled (Resource is inactive)	
tag-routing	<input type="checkbox"/> enabled (Resource is active)	

Set Reset Back

Figure 81: Define DSCP value for RTP

6.6.4. Administer bodypart-type to delete MIME/multiple parts in SIP message body

This section shows the configuration for **bodypart-type** of “entry ToTelco” to send only SDP part to MTS Allstream.

a) Add SDP to allowed-body-part.

Select **Configuration > vsp > session-config-pool > entry ToTelco > bodypart-type**. Click on link **Add allowed-body-part** as shown in **Figure 82**.

The screenshot shows the Avaya Aura Configuration interface. The left sidebar contains a tree view of the configuration hierarchy, with 'bodypart-type' selected under 'entry ToTelco'. The main area displays the configuration for 'Configure vsp\session-config-pool\entry ToTelco\bodypart-type'. It includes buttons for 'Set', 'Reset', 'Back', and 'Delete'. The 'allowed-body-part' section shows a table with 'bodypart-type' and 'application sdp', with an 'Add allowed-body-part' link. The 'blocked-body-part' section shows a table with 'bodypart-type' and 'application any', with an 'Add blocked-body-part' link. The 'move-bp-headers' section shows a dropdown set to 'disabled' with the note '(Resource is inactive)'. There are also 'Set', 'Reset', and 'Back' buttons at the bottom of the main area, along with 'Help' and 'Index' links.

Figure 82: Add an allowed-body-part entry

b) Create a new entry to allow SDP body part. Select **bodypart-type** as **application**; **application sub-type** as **sdp** then click “Create” as shown in **Figure 83**.

The screenshot shows the Avaya Aura Configuration interface. On the left is a navigation tree with 'bodypart-type' selected under 'entry ToTelco'. The main panel displays a form titled 'Create vsplsession-config-poolentry ToTelco/bodypart-type/allowed-body-part - Step 1 of 1: Edit allowed-body-part'. The form contains two dropdown menus: '* bodypart-type' with 'application' selected, and '* application-sub-type' with 'sdp' selected. At the bottom of the form are three buttons: 'Create', 'Reset', and 'Cancel'.

Figure 83: Create an entry to allow SDP body part

c) Configure AA-SBC to block all body parts other than SDP. Select **Configuration > vsp > session-config-pool > entry ToTelco > bodypart-type**. Click on link **Add blocked-body-part** as shown in **Figure 84**.

The screenshot shows the Avaya Aura Configuration interface. On the left, the navigation tree has 'bodypart-type' selected. The main panel displays the 'Configure vsplsession-config-poolentry ToTelco/bodypart-type' page. At the top, there are buttons for 'Set', 'Reset', 'Back', and 'Delete'. Below these are two tables. The first table, 'allowed-body-part', has a header 'bodypart-type' and a row with 'application sdp' and links 'Edit' and 'Delete'. Below this table is a link 'Add allowed-body-part'. The second table, 'blocked-body-part', has a header 'bodypart-type' and a row with 'application any' and links 'Edit' and 'Delete'. Below this table is a link 'Add blocked-body-part' which is highlighted with a red border. At the bottom, there is a section 'move-bp-headers' with a dropdown set to 'disabled' and the text '(Resource is inactive)'. At the very bottom are buttons for 'Set', 'Reset', and 'Back', along with 'Help' and 'Index' links.

Figure 84: Add a blocked-body-part entry

d) Create a new entry to block other body parts. Select **bodypart-type** as **application**; **application sub-type** as **any** then click “Create” as shown in **Figure 85**.

The screenshot displays the Avaya Aura Configuration web interface. The top navigation bar includes 'Home', 'Configuration', 'Status', 'Call Logs', 'Event Logs', 'Actions', 'Services', 'Keys', 'Access', and 'Tools'. The left sidebar shows a tree view of configuration objects, with 'bodypart-type' highlighted under 'session-config-pool'. The main content area is titled 'Create vspsession-config-poolentry ToTelco/bodypart-type/blocked-body-part - Step 1 of 1: Edit blocked-body-part'. It contains a form with two dropdown menus: 'bodypart-type' set to 'application' and 'application-sub-type' set to 'any'. Below the form are 'Create', 'Reset', and 'Cancel' buttons.

Configuration: all

Configuration Setup View

cluster

box: DevSBC4.bwwdev.com

vsp

default-session-config

tls

session-config-pool

entry ToTelco

sip-settings

to-uri-specification

from-uri-specification

request-uri-specification

p-asserted-identity-uri-specification

media

bodypart-type

inbound-header-settings

third-party-call-control

entry ToPBX

entry Discard

Create vspsession-config-poolentry ToTelco/bodypart-type/blocked-body-part - Step 1 of 1: Edit blocked-body-part

Please provide some basic information for blocked-body-part. Then press "Create".

* bodypart-type application

* application-sub-type any

Create Reset Cancel

Figure 85: Create an entry to block body parts other than SDP

6.6.5. Administer inbound-header-setting to block X-nt-e164-clid, Alert-Info Request and P-Location headers

MTS Allstream SIP Trunking does not support X-nt-e164-clid, Alert-Info, Request and P-Location in SIP message headers for outbound calls. This section shows the configuration for **inbound-header-setting** of “**entry ToTelco**” to block mentioned headers to be sent to MTS Allstream.

Select **Configuration > vsp > session-config-pool > entry ToTelco > inbound-header-settings**. Click on link **Edit blocked-header** to add X-nt-e164-clid; Alert-Info; Request and P-Location to blocked headers as shown in **Figure 86**.

The screenshot displays the Avaya Aura Configuration interface. The left sidebar shows the navigation tree with 'inbound-header-settings' selected under 'entry ToTelco'. The main content area is titled 'Configure vsp|session-config-pool|entry ToTelco|inbound-header-settings'. It features a 'blocked-header' table with the following entries:

blocked-header
X-nt-e164-clid
Alert-Info
P-Location
Request

Below the table, there are dropdown menus for 'apply-allow-block-to' (set to 'requests-and-responses') and 'apply-to-allow-block-to-dialog' (set to 'both').

Figure 86: Edit blocked-header in inbound-header-settings

6.6.6. Administer sip-session-timers-setting

By default the **sip-session-timers-setting** was disabled on AA-SBC. The session timers should be turned on to let AA-SBC terminate the unsuccessfully call attempts to PSTN.

In order to support Session Timer, CS1000 system has to send header “Supported: timer” to MTS Allstream. But CS1000 does not send this header by nature. The following configuration in **Figure 87a**, shows how to configure AA-SBC **Configuration vsp\session-config-pool\entry ToTelco\header-setting\reg-ex-header20** to insert “Supported: timer”.

- destination: Supported
- source: Supported
- expression: .*
- replacement: 100rel,timer
- apply-to-method: Select All
- apply-to-responses: both
- apply-to-dialog: both

The screenshot displays the Avaya Aura Configuration web interface. The left sidebar shows a tree view of the configuration hierarchy: **Configuration: all** > **vsp** > **session-config-pool** > **entry ToTelco** > **header-setting** > **reg-ex-header 20**. The main panel is titled "Configure vspsession-config-poolentry ToTelcoheader-settingreg-ex-header 20". It contains several sections for configuration:

- admin**: A dropdown menu set to "enabled" with a note "(Resource is active)".
- * number**: A text input field containing "20".
- * destination**: A text input field containing "Supported" and a dropdown menu also set to "Supported".
- create**: A section with three fields:
 - * source**: A text input field containing "Supported" and a dropdown menu set to "Supported".
 - * expression**: A text input field containing ".*" with a note "(regular expression)".
 - * replacement**: A text input field containing "100rel,timer".
- append**: A link labeled "Add append".
- apply-to-methods**: A dropdown menu showing "INVITE", "REFER", "MESSAGE", and "INFO". Below it are "Select All" and "Unselect All" buttons.
- apply-to-responses**:
 - * type**: A dropdown menu set to "both" with a note "(Apply to responses and requests)".
 - * response-code**: A text input field containing "0" with a note "(from 0 to 65,535)".
- apply-to-dialog**: A dropdown menu set to "both" with a note "(Apply to both inbound and outbound dialogs.)".
- session-persistent**: A dropdown menu set to "disabled" with a note "(Resource is inactive)".

At the bottom of the main panel are buttons for "Set", "Reset", "Back", and "Copy".

Figure 87a: Configure the regular expression to insert header “Supported: timer”

To enable **sip-session-timers-setting**, select **Configuration vsp\session-config-pool\entry ToTelco\ sip-session-timers-setting**. Then change **admin** state to **enable** as shown in **Figure 87b**. The refresher was configured to **UAS** to let MTS Allstream in charge of refreshing the session timer. MTA Allstream sets Min-SE 600 for SIP Trunk, so the Session-Expires has to be set 600 or greater. In this testing Session-Expires was set to 600, it means every 300 seconds the session refresher (MTA Allstream) will send UPDATE.

The screenshot shows the Avaya Aura Configuration web interface. The left sidebar displays a tree view of the configuration hierarchy, with 'sip-session-timers-setting' selected under 'entry ToTelco'. The main content area is titled 'Configure vsp\session-config-pool\entry ToTelco\ sip-session-timers-setting'. It contains a table of configuration parameters with the following values:

Parameter	Value	Description
admin	enabled	(Resource is active)
preferred-refresher	UAS	(UAS of the session will perform the session refresh)
session-expires	600	seconds(from 90 to 1,000,000,default=1800)
min-se	90	seconds(from 90 to 1,000,000,default=90)
action	Terminate	(Cleanup the session state and related resources)

Buttons for 'Set', 'Reset', 'Back', and 'Delete' are located at the top of the configuration area. At the bottom, there are 'Set', 'Reset', and 'Back' buttons, along with 'Help' and 'Index' links.

Figure 87b: Enable SIP session timers

6.6.7. Disable third-party-call-control

The **third-party-call-control** should be disabled on AA-SBC to interwork with MTS Allstream.

To disable **third-party-call-control**, select **Configuration > vsp > session-config-pool > entry ToTelco > third-party-call-control**. Then change the **admin** state to **disabled** as shown in **Figure 88**.

The screenshot displays the Avaya Aura Configuration web interface. The left sidebar shows a tree view of the configuration hierarchy: **Configuration: all** > **vsp** > **session-config-pool** > **entry ToTelco** > **third-party-call-control**. The main content area is titled **Configure vspsession-config-poolentry ToTelcothird-party-call-control**. It features a table of configuration parameters for this entry. The **admin** parameter is set to **disabled**, with a note "(Resource is inactive)". Other parameters include **status-events** (both), **handle-refer-locally** (enabled), **refer-maintain-identity** (false), **ringback-file**, **busy-file**, **pre-call-announcement**, and **terminate-after-pre-call-announcement** (disabled).

Parameter	Value	Notes
admin	disabled	(Resource is inactive)
status-events	both	(both call-legs)
handle-refer-locally	enabled	(Resource is active)
refer-maintain-identity	false	
ringback-file		Browse System Files
busy-file		Browse System Files
pre-call-announcement		Browse System Files
terminate-after-pre-call-announcement	disabled	(Resource is inactive)

Figure 88: Disable third-party-call-control

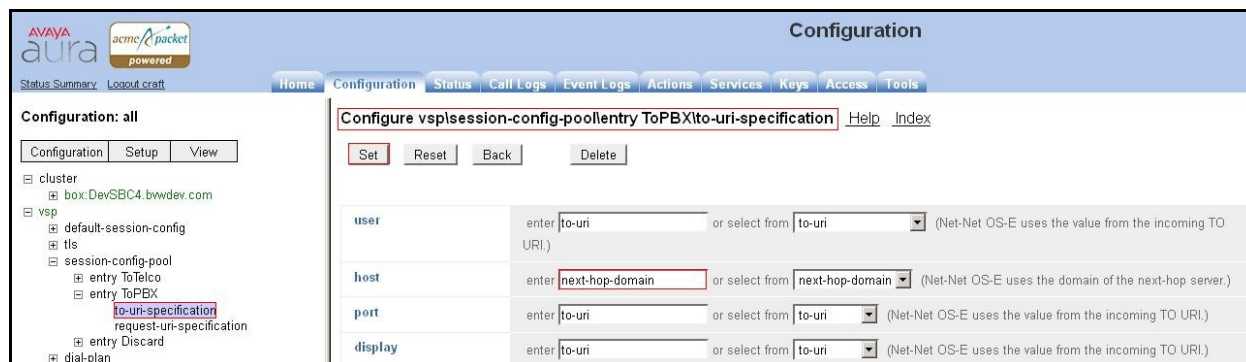
6.7. Administer session-config-pool “entry ToPBX”

6.7.1. Manipulate To, Request-URI headers.

The CS1000 SIP gateway was configured with domain name mtsallstream.com (please refer to **Section 5.5**). However, MTS Allstream prefers to IP address in SIP headers. This section shows the configuration on AA-SBC to manipulate SIP headers To and Request-URI before sending to CS1000.

a) Manipulate **To** header.

Select **Configuration vsp\session-config-pool\entry ToPBX\to-uri-specification**. Then change **host** to send **next-hop-domain** as shown in **Figure 89**. AA-SBC presents domain **mtsallstream.com** in the **To** header sent to CS1000.



The screenshot displays the Avaya Aura Configuration interface. The left sidebar shows a tree view under 'Configuration: all' with the path 'vsp > session-config-pool > entry ToPBX > to-uri-specification' highlighted. The main panel is titled 'Configure vsp\session-config-pool\entry ToPBX\to-uri-specification' and includes 'Set', 'Reset', 'Back', and 'Delete' buttons. Below these are four configuration rows:

Field	Configuration Options	Notes
user	enter to-uri or select from to-uri (dropdown)	(Net-Net OS-E uses the value from the incoming TO URI.)
host	enter next-hop-domain or select from next-hop-domain (dropdown)	(Net-Net OS-E uses the domain of the next-hop server.)
port	enter to-uri or select from to-uri (dropdown)	(Net-Net OS-E uses the value from the incoming TO URI.)
display	enter to-uri or select from to-uri (dropdown)	(Net-Net OS-E uses the value from the incoming TO URI.)

Figure 89: Manipulate To header of session-config-pool “entryToPBX”

b) Manipulate **Request-URI** header.

Select **Configuration vsp\session-config-pool\entry ToPBX\request-uri-specification**. Then change **host** to send **next-hop-domain** as shown in **Figure 90**. AA-SBC presents domain **mtsallstream.com** in the **Request-URI** header sent to CS1000.

The screenshot shows the Avaya Aura Configuration interface. The left sidebar displays a tree view of the configuration hierarchy, with 'request-uri-specification' selected under 'entry ToPBX'. The main content area is titled 'Configure vsp\session-config-pool\entry ToPBX\request-uri-specification'. It features a 'Set' button and a table with three rows: 'user', 'host', and 'port'. The 'user' row has a text input field with 'request-uri' and a dropdown menu with 'request-uri'. The 'host' row has a text input field with 'next-hop-domain' and a dropdown menu with 'next-hop-domain'. The 'port' row has a text input field with 'request-uri' and a dropdown menu with 'request-uri'. Each row has a note in parentheses: '(Net-Net OS-E uses the value from the incoming REQUEST URI.)'.

Field	Value	Notes
user	request-uri	(Net-Net OS-E uses the value from the incoming REQUEST URI.)
host	next-hop-domain	(Net-Net OS-E uses the domain of the next-hop server.)
port	request-uri	(Net-Net OS-E uses the value from the incoming REQUEST URI.)

Figure 90: Manipulate Request-URI header of session-config-pool “entryToPBX”

6.7.2. Administer media

This session shows the configuration to enable media anchoring on AA-SBC.

To enable media anchoring, select **Configuration vsp\session-config-pool\entry ToPBX\media**. Then change **anchor** to **enable** as shown in **Figure 91**.



Figure 91: Enable media anchor

6.7.3. Administer inbound-header-setting to block X-nt-e164-clid, Alert-Info Request and P-Location headers

MTS Allstream SIP Trunking does not support X-nt-e164-clid, Alert-Info, Request and P-Location in SIP message headers for outbound calls. This section shows the configuration for **inbound-header-setting** of “**entry ToPBX**” to block mentioned headers to be sent to MTS Allstream.

Select **Configuration > vsp > session-config-pool > entry ToPBX > inbound-header-settings**. Click on link **Edid blocked-header** to add X-nt-e164-clid; Alert-Info; Request and P-Location to blocked headers as shown in **Figure 92**.

The screenshot shows the Avaya Aura Configuration interface. The left sidebar displays a tree view of the configuration hierarchy, with 'entry ToPBX' > 'inbound-header-settings' selected. The main content area is titled 'Configure vspsession-config-poolentry ToPBXinbound-header-settings'. It features a 'blocked-header' section with a list of headers: 'X-nt-e164-clid', 'Alert-Info', 'P-Location', and 'Request'. Below this, there are dropdown menus for 'apply-allow-block-to' (set to 'requests-and-responses') and 'apply-to-allow-block-to-dialog' (set to 'both').

Figure 92: Edit blocked-header in inbound-header-settings

6.7.4. Administer sip-session-timers-setting

By default the **sip-session-timers-setting** was disabled on AA-SBC. The session timers should be turned on to let AA-SBC terminate the unsuccessfully call attempts to PSTN.

In order to support Session Timer, CS1000 system has to send header “Supported: timer” to MTS Allstream. But CS1000 does not send this header by nature. The following configuration in **Figure 93a**, shows how to configure AA-SBC **Configuration vsp\session-config-pool\entry ToPBX\header-setting\reg-ex-header20** to insert “Supported: timer”.

- destination: Supported
- source: Supported
- expression: .*
- replacement: 100rel,timer
- apply-to-method: Select All
- apply-to-responses: both
- apply-to-dialog: both

The screenshot displays the Avaya Aura Configuration web interface. The left sidebar shows a tree view of the configuration hierarchy: **Configuration: all** > **cluster** > **box: DevSBC4.bwwdev.com** > **vsp** > **session-config-pool** > **entry ToTelco** > **header-setting** > **reg-ex-header 20**. The main panel is titled **Configure vspsession-config-poolentry ToTelcoheader-settingreg-ex-header 20**. It contains several sections:
- **admin**: A dropdown menu set to **enabled** with the note "(Resource is active)".
- *** number**: A text field containing **20**.
- *** destination**: A text field containing **Supported** and a dropdown menu also set to **Supported**.
- **create** section:
 - *** source**: A text field containing **Supported** and a dropdown menu set to **Supported**.
 - *** expression**: A text field containing **.*** with the note "(regular expression)".
 - *** replacement**: A text field containing **100rel,timer**.
- **append**: A link labeled **Add append**.
- **apply-to-methods**: A dropdown menu showing **INVITE**, **REFER**, **MESSAGE**, and **INFO**, with **Select All** and **Unselect All** buttons below it.
- **apply-to-responses**:
 - *** type**: A dropdown menu set to **both** with the note "(Apply to responses and requests)".
 - *** response-code**: A text field containing **0** with the note "(from 0 to 65,535)".
- **apply-to-dialog**: A dropdown menu set to **both** with the note "(Apply to both inbound and outbound dialogs.)".
- **session-persistent**: A dropdown menu set to **disabled** with the note "(Resource is inactive)".
At the bottom of the main panel are buttons for **Set**, **Reset**, **Back**, and **Copy**.

Figure 93a: Configure the regular expression to insert header “Supported: timer”

To enable **sip-session-timers-setting**, select **Configuration vsp\session-config-pool\entry ToTelco\ sip-session-timers-setting**. Then change **admin** state to **enable** as shown in **Figure 93b**. The refresher was configured to **UAC** to let MTS Allstream in charge of refreshing the session timer. MTA Allstream sets Min-SE 600 for SIP Trunk, so Session-Expires has to be set 600 or greater. In this testing Session-Expires was set to 600, it means every 300 seconds the session refresher (MTA Allstream) will send UPDATE.

The screenshot shows the Avaya Aura Configuration web interface. The left sidebar displays a tree view of the configuration hierarchy, with 'sip-session-timers-settings' selected under 'entry ToPBX'. The main content area is titled 'Configure vsp\session-config-pool\entry ToPBX\ sip-session-timers-settings'. It contains a table of configuration parameters:

Parameter	Value	Description
admin	enabled	(Resource is active)
preferred-refresher	UAC	(UAC of the session will perform the session refresh)
session-expires	600	seconds(from 90 to 1,000,000,default=1800)
min-se	90	seconds(from 90 to 1,000,000,default=90)
action	Terminate	(Cleanup the session state and related resources)

Buttons for 'Set', 'Reset', 'Back', and 'Delete' are located at the top of the configuration area. Below the table, there are 'Set', 'Reset', and 'Back' buttons, along with 'Help' and 'Index' links.

Figure 93b: Enable SIP session timers

7. Verification Steps

The following steps may be used to verify the configuration.

7.1. General

Place an **inbound/ outbound** call from/ to a PSTN phone to/ from an internal CS1000 phone, answer the call, and verify that two-way speech path exists. Check call display name and number to ensure the correct information was sent/ received. Perform hold/ retrieve. Verify the call remains stable for several minutes and disconnect properly.

7.2. Verify Call Establishment on CS1000 Call Server

a) Active Call Trace (LD 80)

The following is an example of one of the commands available on CS1000 to trace the DN when the call is in progress. The call scenario involved the PSTN phone number 6139675258 calling 6477761230 on CS1000.

- Login Call Server CLI (please refer to **Section 5.1.2** for more detail).
- Login to the Overlay command prompt, issue the command **LD 80** and then **trace 4 1230**.
- After the call is released, issue the command **trac 4 1230** again to see if the DN is released back to idle state.

Below is the actual output of the Call Server Command Line mode when the 1230 is in call state:

```
>ld 80
>*ld 80
TRA000
.trac 4 1230

ACTIVE VTN 108 0 00 18

ORIG VTN 100 1 01 00 VTRK IPTI RMBR 104 1 INCOMING VOIP GW CALL
FAR-END SIP SIGNALLING IP: 207.245.2.12
FAR-END MEDIA ENDPOINT IP: 135.10.97.216 PORT: 21320
FAR-END VendorID: AVAYA-SM-6.1.1.0.611023
TERM VTN 108 0 00 18 KEY 0 SCR MARP CUST 4 DN 1230 TYPE 1140
SIGNALLING ENCRYPTION: INSEC
MEDIA ENDPOINT IP: 135.10.98.133 PORT: 5200
MEDIA PROFILE: CODEC G.729A NO-LAW PAYLOAD 20 ms VAD OFF
RFC2833: RXPT 101 TXPT 101 DIAL DN 1230
MAIN_PM ESTD
TALKSLOT ORIG 88 TERM 61
EES_DATA:
NONE
QUEU NONE
CALL ID 0 34784
```



```
---- ISDN ISL CALL (ORIG) ----  
CALL REF # = 387  
BEARER CAP = VOICE  
HLC =  
CALL STATE = 10  ACTIVE  
CALLING NO = 6139675258 NUM_PLAN:UNKNOWN TON:UNKNOWN ESN:UNKNOWN  
CALLED NO = 6477761230 NUM_PLAN:UNKNOWN TON:UNKNOWN ESN:UNKNOWN
```

And this is the example after the call on 4685 is completed.

```
.trac 4 1230
```

```
IDLE VTN 108 0 00 18  MARP
```

b) SIP Trunk monitoring (LD 32)

Place an inbound call from PSTN (6139675258) to CS1000 (9729414685). Then check the SIP Trunk status by using LD 32.

```
>ld 32  
NPR000  
.stat 100 1  
063 UNIT(S) IDLE  
001 UNIT(S) BUSY  
000 UNIT(S) DSBL  
000 UNIT(S) MBSY  
.
```

And this is the example after the call is completed; the BUSY trunk changes its state to IDLE.

```
.stat 100 1  
064 UNIT(S) IDLE  
000 UNIT(S) BUSY  
000 UNIT(S) DSBL  
000 UNIT(S) MBSY  
.
```

7.3. Protocol Traces

Below are Wireshark traces of the same call scenario that has been made in **Section 7.2**.

The following SIP headers are inspected:

- RequestURI: verify the request number and either SIP domain
- From: verify the display name and display number.
- To: verify the display name and display number.
- History-Info: verify the call forward information and reason code.
- P-Asserted-Identity: verify the display name and display number.

The following attributes in SIP message body are inspected:

- Connection Information (c): verify IP address of far end endpoint
- Time Description (t): verify session timeout of far end endpoint
- Media Description (m): verify audio port, codec, DTMF event description
- Media Attribute (a): verify specific audio port, codec,ptime, send/ receive ability, DTMF event and fax attributes.

a) Outbound calls.

The SIP/INVITE from CS1000 to MTS Allstream was captured at Avaya Aura® Session Border Controller OUTSIDE interface.

```
INVITE sip:16139675258@220.20.2.12 SIP/2.0
From: "mts 1230" <sip:6477761230@110.10.98.108>;tag=6c620a87-13c4-4e666911-3137c662-511bdc37
To: <sip:16139675258@220.20.2.12>
Call-ID: CXC-101-5c412850-6c620a87-13c4-4e666911-3137c662-2f2f46d1@110.10.98.108
CSeq: 1 INVITE
Via: SIP/2.0/UDP 135.10.98.108:5060;branch=z9hG4bK-285b1-4e666911-3137c662-4f7fb5a4
Supported: 100rel,x-nortel-sipvc,replaces
User-Agent: Nortel CS1000 SIP GW release_7.0 version_linux-6.50.00 AVAYA-SM-6.1.1.0.611023
P-Asserted-Identity: "mts 1230" <sip:6477761230@110.10.98.108>
Privacy: none
History-Info: <sip:16139675258@mtsallstream.com;user=phone>;index=1
Max-Forwards: 65
Allow:
INVITE,ACK,BYE,REGISTER,REFER,NOTIFY,CANCEL,PRACK,OPTIONS,INFO,SUBSCRIBE,UPDATE
Contact: <sip:6477761230@110.10.98.108:5060;maddr=110.10.98.108;transport=udp>
Min-SE: 90
Session-Expires: 1800
Content-Type: application/SDP
Content-Length: 263
```

v=0
o=- 79 1 IN IP4 110.10.98.108
s=-
c=IN IP4 135.10.98.108
t=0 0
m=audio 20320 RTP/AVP 18 0 8 101 111
c=IN IP4 135.10.98.108
a=rtpmap:101 telephone-event/8000
a=rtpmap:111 X-nt-inforeq/8000
a=fmtp:18 annexb=no
a=fmtp:101 0-15
a=ptime:20
a=sendrecv

The SIP/200OK MTS Allstream to CS1000 was captured at Avaya Aura® Session Border Controller OUTSIDE interface.

SIP/2.0 200 OK
Via: SIP/2.0/UDP 110.10.98.108:5060;branch=z9hG4bK-285b1-4e666911-3137c662-4f7fb5a4
To: <sip:16139675258@220.20.2.12>;tag=3524323349-604795
From: "mts 1230" <sip:6477761230@110.10.98.108>;tag=6c620a87-13c4-4e666911-3137c662-511bdc37
Call-ID: CXC-101-5c412850-6c620a87-13c4-4e666911-3137c662-2f2f46d1@135.10.98.108
CSeq: 1 INVITE
Allow: INVITE, BYE, OPTIONS, CANCEL, ACK, REGISTER, NOTIFY, INFO, REFER, SUBSCRIBE, PRACK, UPDATE, MESSAGE, PUBLISH
Contact: <sip:16139675258@220.20.2.12:5060>
Call-Info: <sip:220.20.2.12>;method="NOTIFY";Event=telephone-event;Duration=1000"
Content-Type: application/sdp
Content-Length: 227

v=0
o=nextone-msw-lab-3 529412758 529412758 IN IP4 220.20.2.12
s=sip call
c=IN IP4 220.20.2.13
t=0 0
m=audio 31964 RTP/AVP 18 0 8 101
a=ptime:20
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15

b) Inbound calls.

The SIP/INVITE from MTS Allstream to CS1000 was captured at Avaya Aura® Session Border Controller OUTSIDE interface.

INVITE sip:6477761230@110.10.98.108;user=phone SIP/2.0
Max-Forwards: 69
Session-Expires: 3600;refresher=uac
Min-SE: 600
Supported: timer, 100rel
To: <sip:6477761230@110.10.98.108;user=phone>
From: <sip:6139675258@220.20.2.12;user=phone>;tag=3524324116-575879
P-Asserted-Identity: <sip:6139675258@220.20.2.12;user=phone>
Call-ID: 118327-3524324116-575873@nextone-msw-lab-3.mtsallstream.com
CSeq: 1 INVITE
Allow: INVITE, BYE, OPTIONS, CANCEL, ACK, REGISTER, NOTIFY, INFO, REFER, SUBSCRIBE, PRACK, UPDATE, MESSAGE, PUBLISH
Via: SIP/2.0/UDP 220.20.2.12:5060;branch=z9hG4bK71df5f993f6beda8d0e8f5137d6140a3
Contact: <sip:6139675258@220.20.2.12:5060;tgrp=TOROONSBCIOT1>
Call-Info: <sip:220.20.2.12>;method="NOTIFY;Event=telephone-event;Duration=1000"
Content-Type: application/sdp
Content-Length: 227

v=0
o=nextone-msw-lab-3 537084383 537084383 IN IP4 220.20.2.12
s=sip call
c=IN IP4 220.20.2.13
t=0 0
m=audio 31986 RTP/AVP 18 0 8 101
a=ptime:20
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15

The SIP/200OK MTS Allstream to CS1000 was captured at Avaya Aura® Session Border Controller OUTSIDE interface.

SIP/2.0 200 OK
From: <sip:6139675258@220.20.2.12;user=phone>;tag=3524324116-575879
To: <sip:6477761230@110.10.98.108;user=phone>;tag=6c620a87-13c4-4e666c12-314380e5-37050cb4
Call-ID: 118327-3524324116-575873@nextone-msw-lab-3.mtsallstream.com
CSeq: 1 INVITE
Supported: 100rel,x-nortel-sipvc,replaces
Require: timer

User-Agent: Nortel CS1000 SIP GW release_7.0 version_linux-6.50.00
P-Asserted-Identity: "mts 1230" <sip:6477761230@mtsallstream.com;user=phone>
Privacy: none
Server: AVAYA-SM-6.1.1.0.611023
Request:
Allow:
INVITE,ACK,BYE,REGISTER,REFER,NOTIFY,CANCEL,PRACK,OPTIONS,INFO,SUBSCRIBE,UPDATE
Via: SIP/2.0/UDP 220.20.2.12:5060;branch=z9hG4bK71df5f993f6beda8d0e8f5137d6140a3
Contact:
<sip:6477761230@110.10.98.108:5060;user=phone;maddr=110.10.98.108;transport=udp>
Content-Type: application/sdp
Content-Length: 259

v=0
o=- 85 1 IN IP4 110.10.98.108
s=-
c=IN IP4 135.10.98.108
t=0 0
m=audio 20264 RTP/AVP 18 101 111
c=IN IP4 135.10.98.108
a=rtpmap:101 telephone-event/8000
a=rtpmap:111 X-nt-inforeq/8000
a=ptime:20
a=fmtp:18 annexb=no
a=fmtp:101 0-15
a=sendrecv

8. Conclusion

All of the test cases have been executed. Despite the number of observations seen during testing as noted in **Section 2.2**, the test result met the objectives outlined in **Section 2.1**. The MTS Allstream system is considered **compliant** with Avaya Communication Server 1000 Release 7.5.

9. Additional References

Product documentation for Avaya products may be found at:

<http://support.avaya.com/css/appmanager/public/support>

[1] *Network Routing Service Fundamentals, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-130, Revision 03.02, November 2010.*

[2] *IP Peer Networking Installation and Commissioning, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-313, Revision: 05.02, November 2010*

[3] *Communication Server 1000E Overview, Avaya Communication Server 1000, Release 7.5, Document Number NN43041-110, Revision: 05.02, January 2011*

[4] *Communication Server 1000 Unified Communications Management Common Services Fundamentals, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-116, Revision 05.08, January 2011*

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

[6] *Product Compatibility Reference, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-256, Revision 05.02, February 2011*

©2011 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.