



Avaya Solution & Interoperability Test Lab

Application Notes for MTS Allstream SIP Trunking Service with Avaya Communication Server 1000 Release 7.5, Avaya Aura® Session Manager Release 6.2 and Avaya Session Border Controller for Enterprise Release 4.0.5 – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between MTS Allstream SIP Trunking Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Communication Server 1000 7.5, Avaya Aura® Session Manager 6.2, Avaya Session Border Controller for Enterprise 4.0.5 and various Avaya endpoints. This documented solution does not extend to configurations without Avaya Aura® Session Manager and Avaya Session Border Controller for Enterprise.

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

Note: These Application Notes are applicable with Avaya Aura® 6.2 which is currently in Controlled Introduction. Avaya Aura® 6.2 will be Generally Available in Summer 2012.

Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing	4
2.2.	Test Results	5
2.3.	Support.....	6
3.	Reference Configuration	7
4.	Equipment and Software Validated	9
5.	Avaya Communication Server 1000 Configuration	10
5.1.	Log into CS1000.....	11
5.1.1.	Log into Unified Communications Management (UCM) and Element Manager (EM).....	11
5.1.2.	Log into Call Server Command Line Interface (CLI)	12
5.2.	Administer a Node IP Telephony	12
5.2.1.	Obtain Node IP address	12
5.2.2.	Administer Quality of Service (QoS)	14
5.2.3.	Synchronize the new configuration	14
5.3.	Administer Voice Codec.....	14
5.3.1.	Enable Voice Codec, Node IP Telephony	14
5.3.2.	Administer Voice Codec on Media Gateways.....	16
5.4.	Administer Zones and Bandwidth	17
5.4.1.	Create a zone for IP phones	17
5.4.2.	Create a zone for virtual SIP trunk	18
5.5.	Administer SIP Trunk Gateway.....	19
5.5.1.	Integrated Services Digital Network (ISDN).....	19
5.5.2.	Administer SIP Trunk Gateway to Session Manager	19
5.5.3.	Administer Virtual D-Channel.....	21
5.5.4.	Administer Virtual Super-Loop	23
5.5.5.	Enable Music for Customer Data Block	24
5.5.6.	Administer Virtual SIP Routes	25
5.5.7.	Administer Virtual Trunks.....	29
5.5.8.	Administer Calling Line Identification Entries.....	30
5.5.9.	Enable External Trunk to Trunk Transferring	31
5.6.	Administer Dialing Plans.....	32
5.6.1.	Define ESN Access Codes and Parameters (ESN)	32
5.6.2.	Associate NPA and SPN call to ESN Access Code 1.....	33
5.6.3.	Digit Manipulation Block (DMI).....	34
5.6.4.	Route List Block (RLB).....	35
5.6.5.	Incoming Digit Translation (IDC)	36
5.6.6.	Outbound Call - Special Number Configuration	36
5.6.7.	Outbound Call - Numbering Plan Area (NPA).....	38
6.	Configure Avaya Aura® Session Manager	39
6.1.	System Manager Login and Navigation	39
6.2.	Specify SIP Domain.....	40
6.3.	Add Location	41
6.4.	Add Adaptation Module	41

6.5.	Add SIP Entities.....	43
6.6.	Add Entity Links.....	45
6.7.	Add Routing Policies	46
6.8.	Add Dial Patterns.....	47
6.9.	Add/View Session Manager	49
7.	Configure Avaya Session Border Controller for Enterprise	51
7.1.	Avaya Session Border Controller for Enterprise Login.....	52
7.2.	Global Profiles	54
7.2.1.	Uniform Resource Identifier (URI) Groups.....	54
7.2.2.	Routing Profiles	55
7.2.3.	Topology Hiding.....	56
7.2.4.	Server Interworking	59
7.2.5.	Signaling Manipulation.....	62
7.2.6.	Server Configuration.....	64
7.3.	Domain Policies	68
7.3.1.	Application Rules.....	68
7.3.2.	Media Rules	69
7.3.3.	Signaling Rules	71
7.3.4.	Endpoint Policy Groups.....	76
7.3.5.	Session Policy	78
7.4.	Device Specific Settings	80
7.4.1.	Network Management.....	80
7.4.2.	Media Interface	81
7.4.3.	Signaling Interface.....	81
7.4.4.	End Point Flows - Server Flow	82
7.4.5.	Session Flows.....	84
8.	MTS Allstream SIP Trunking Service Configuration	85
9.	Verification and Troubleshooting	86
9.1.	Verification Steps.....	86
9.2.	Protocol Traces	86
9.3.	Troubleshooting	87
10.	Conclusion	91
11.	References	92

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between MTS Allstream SIP Trunking Service (from this point it will be referred as MTS Allstream for brevity) and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Communication Server 1000 (CS1000) 7.5, Avaya Aura® Session Manager 6.2, Avaya SBC for Enterprise (Avaya SBCE) 4.0.5 and various Avaya endpoints.

Customers using this Avaya SIP-enabled enterprise solution with MTS Allstream are able to place and receive PSTN calls via a broadband connection. This converged network solution is an alternative to traditional PSTN trunk such as analog and/or ISDN-PRI.

2. General Test Approach and Test Results

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

MTS Allstream is a member of the Avaya DevConnect Service Provider program. The general test approach is to connect a simulated enterprise to MTS Allstream via the public internet and exercise the features and functionality listed in **Section 2.1**.

2.1. Interoperability Compliance Testing

To verify MTS Allstream SIP Trunking Service interoperability, the following features and functionalities were covered during the compliance test:

- Response to SIP OPTIONS queries.
- Incoming PSTN call to various phone types including SIP, UNISTim, PC2050 softphone, digital and analog telephone at the enterprise. All inbound calls from PSTN are routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN call from various phone types including SIP, UNISTim, PC2050 softphone, digital and analog telephone at the enterprise. All outbound calls to PSTN are routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya one-X® Communicator (1XC) soft phone. Only the 1XC Computer Mode (where 1XC is used for call control as well as audio path) is tested. The 1XC support both SIP and H.323 protocol but only SIP protocol is tested because CS1000 does not support H.323 protocol.
- Dialing plans including local, long distance, international, outbound toll-free, operator assisted calls, local directory assistance (411)... etc.
- Proper codec negotiation with G.729 and G.711MU codecs.
- DTMF tone transmissions as out-of-band RTP events as per RFC 2833.
- Caller ID presentation and Caller ID restriction.

- Response to incomplete call attempts and trunk errors.
- Voicemail navigation for inbound and outbound calls.
- Incoming and outgoing fax over IP with G.711MU codec.
- User features such as hold and resume, transfer and conference.
- Off-net call forwarding with SIP Diversion method.
- Session Timers implementation from both ends of the enterprise and the service provider.

Items are not supported or not tested including the following:

- Inbound toll-free and outbound emergency calls (911) are supported but are not tested as part of the compliance test because MTS Allstream does not provide the necessary configuration.
- T.38 fax is not supported.
- Off-net call forwarding using History-Info method is not supported.

2.2. Test Results

Interoperability testing of MTS Allstream SIP Trunking Service with the Avaya SIP-enabled enterprise solution is completed with successful results for all test cases with the exception of the observations/limitations described below.

1. **The untrusted Calling Party Name (CPN) from CS1000 is not examined.** In an outbound call scenario, PSTN displays the original untrusted CPN from CS1000. MTS Allstream does not examine the CPN before sending to PSTN. This is a known issue on MTS Allstream SIP Trunking Service and there is no available resolution at this time.
2. **The CPN for outbound call is not being displayed by PSTN.** In an outbound call scenario, CS1000 sends both calling party name and number to PSTN. But in some cases, PSTN phone displays the calling party number only and no calling party name. In other cases, PSTN phone displays both calling party name and number. The calling party name may be overridden by MTS Allstream or by intermediate service providers that route the call through PSTN. This issue has low user impact and is listed here simply as an observation.
3. **In an inbound call scenario, MTS Allstream does not refresh the Session Timer.** MTS Allstream sends an initial INVITE with *Session-Expires: 3600; refresher: uac Min-SE: 600*. It means, as a user agent client, MTS Allstream should refresh the Session Timer every 300 seconds by a reINVITE or UPDATE method. In the compliance test, CS1000 did not receive any Session Timer refresh signaling. This is a known issue on MTS Allstream SIP Trunking Service and there is no available resolution at this time.
4. **Off-net call transfer, the calling party name and number is not updated to calling PSTN party** When CS1000 transfers off-net of an incoming call to PSTN, it sends 200OK with true connected calling party name and number in PAI header to the calling PTSN. However, the calling party name and number have not been updated; the calling PTSN party still displays calling party number of CS1000. This is a known issue on MTS Allstream SIP Trunking Service. It is recommended that MTS Allstream should support the calling party information update. This feature also needs to be supported by the

service provider hosting the calling PSTN party. This issue has low user impact, it is listed here simply as an observation.

5. **CS1000 SIP phone transfers off-net to PSTN is not successful if Music On Hold is enabled.** In an inbound or outbound call between CS1000 SIP phone and PSTN_1, CS1000 SIP phone performs an off-net transferring back to PSTN_2. The transfer fails. PSTN_1 still hear the ringback tone when the call is already answered by PSTN_2. The same call scenario is successful when SIP phone is replaced by other endpoints .e.g. UNISTim or digital phones. The issue does not happen when Music On Hold is disabled. A product defect was reported to Avaya team for an investigation and therefore it is listed here as a limitation.
6. **CS1000 phone holds and retrieves an outbound call causing the CPN to be changed.** After retrieving the call, the calling party number previously displayed on CS1000 phone will be unavailable and replaced by Route ACOD – Trunk Channel ID. This is a known on CS1000 and there is no resolution available at this time. This issue has low user impact and is listed here simply as an observation.
7. **CS1000 SIP phone calls a local UNISTim phone then blind transfers to PSTN causing the CPN to be changed.** The call is successfully transfer. However, the UNISTim phone displays Route ACOD – Trunk Channel ID instead of displaying PSTN calling party name and number. This is a known on CS1000 and there is no resolution available at this time. This issue has low user impact and is listed here simply as an observation.
8. **Performing an “Application Restart” or editing the SigMa script on Ayaya SBCE causes the SigMa script not working.** There is no resolution currently. If the SigMa script does not work after an “Application Restart” or editing, please contact Avaya SBCE support by telephone number 1-866-861-3113 or 1-214-269-2424.

2.3. Support

For technical support on the Avaya products described in these Application Notes visit <http://support.avaya.com>.

For technical support on MTS Allstream SIP Trunking Service, please contact MTS Allstream technical support at:

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

3. Reference Configuration

Figure 1 illustrates the sample Avaya SIP-enabled enterprise solution connected to the MTS Allstream SIP Trunking Service (Vendor Validation circuit) through a public Internet WAN connection.

For security purposes, the real public IP addresses and PSTN routable phone numbers used in the compliance test are not shown in these Application Notes.

Located at the edge of the enterprise network is Avaya SBCE. It has a public side that connects to MTS Allstream via internet and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise network flows through the Avaya SBCE which can protect the enterprise against any outside SIP-based attacks. Avaya SBCE provides network address translation at both the IP and SIP layers. The transport protocol between the Avaya SBCE and MTS Allstream across the public network is UDP; the transport protocol between the Avaya SBCE and Session Manager across the enterprise network is TCP.

In the compliance testing, the Avaya CPE environment was configured with SIP domain **avaya.com** for the enterprise. Avaya SBCE is used to adapt the enterprise SIP domain to the IP address based URI-Host known to MTS Allstream. **Figure 1** below illustrates the network diagram for the enterprise. All voice application elements are connected to internal trusted LAN.

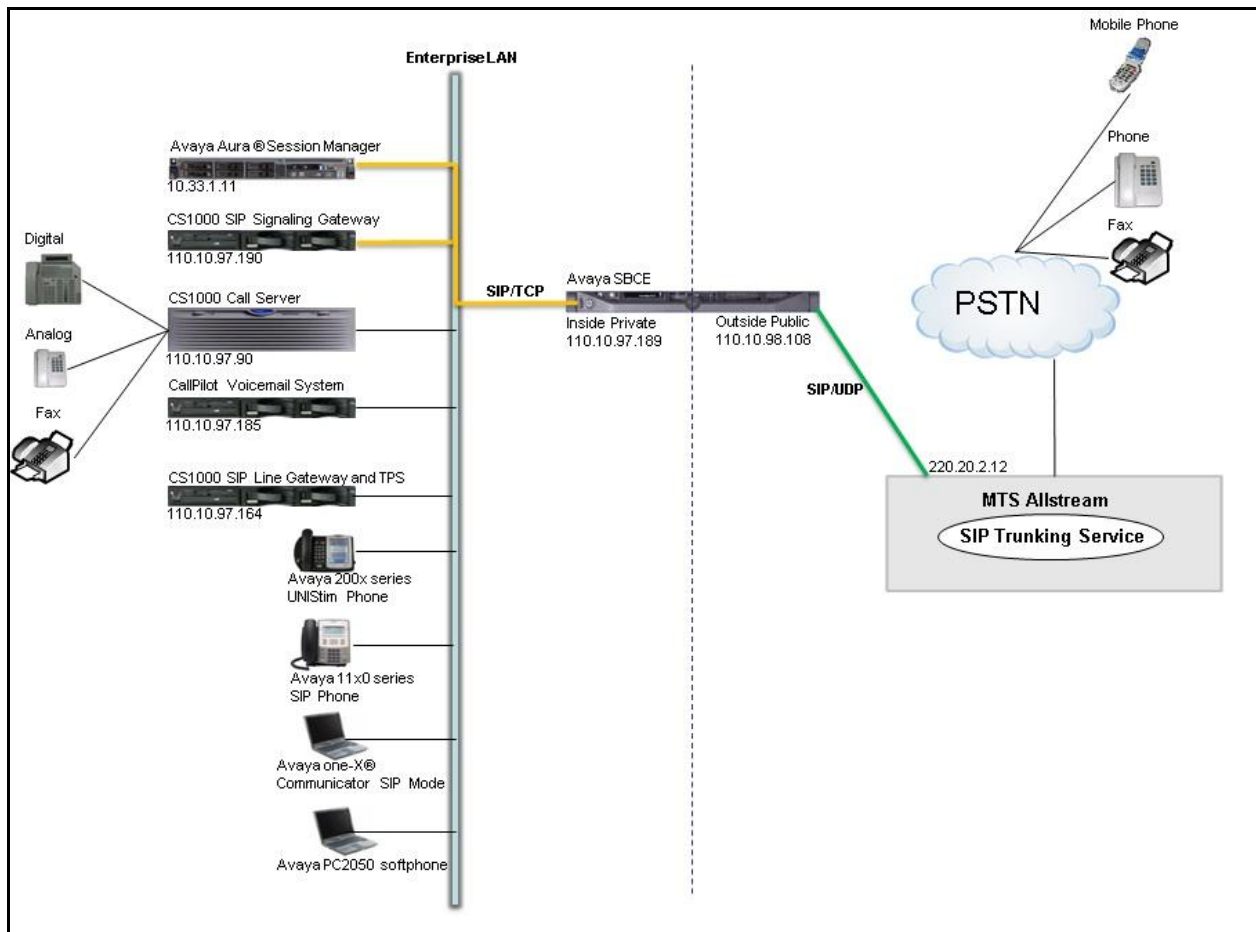


Figure 1: Avaya IP Telephony Network connecting to MTS Allstream SIP Trunking Service

4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Component	Release
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, 2012-05-16 12:51:18 (est) • SSG Server: 7.50.17 GA plus latest Service_Pack_Linux_7.50_17_20120516.ntl • SLG Server: 7.50.17 GA plus latest Service_Pack_Linux_7.50_17_20120516.ntl
Avaya IP Telephone	<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 CallPilot	05.00.41.141
Avaya Session Border Controller for Enterprise	4.0.5 Q09
Avaya 2050PC softphone	3.4
Avaya one-X Communicator (SIP)	6.1.3.08-SP3-Patch2-35791
Avaya Digital Telephone	n/a
Avaya Analog Telephone	n/a
MTS Allstream SIP Trunking Service Components	
Component	Release
Genband S3	5.2.2.12
CS2K	CVM13

Table 1: Equipment and Software Tested

Following screen shows the output of “dstat” command on Call Server:

```
pdt> dstat
Call Server:
-----
DepList name: core
  Filename: /var/opt/nortel/cs/fs/u/patch/deplist/mcore_01.cpl
  Issue   : 01
  Release : x2107.50
  Created : 2012-05-16 12:51:18 (est)
  Number of patches: 215
  Patches Loaded: 215
  Patches In-service: 215
pdt>
```

Following screen shows the output of “spstat” command on SSG Server:

```
[admin@car2-mas ~]$ spstat
There is no SP in loaded status.
The last applied SP: Service_Pack_Linux_7.50_17_20120516.ntl
It is a STANDARD SP.
Has been applied by user nortel on Mon May 28 09:13:19 2012.
spins command completed with no errors detected.
```

5. Avaya Communication Server 1000 Configuration

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

A two-way SIP trunk is created between CS1000 and Session Manager to carry traffic to and from service provider respectively. For inbound call, the call flows from the MTS Allstream to Avaya SBCE to CS1000 via Session Manager. Once the call arrives at CS1000, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed. Outbound call to PSTN is first processed by CS1000 for outbound feature treatment such as route selection and class of service restrictions. Once CS1000 selected the proper SIP trunk, the call is routed to Session Manager toward Avaya SBCE for egress to the MTS Allstream.

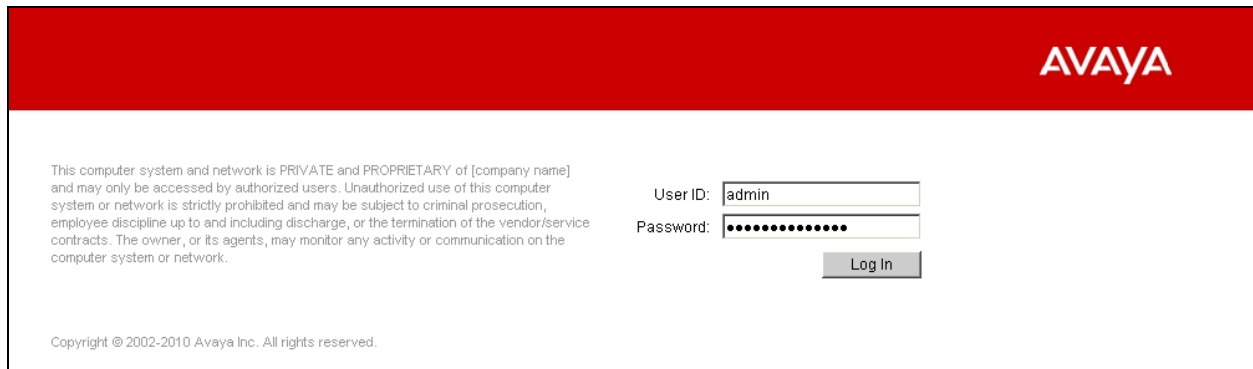
For the compliance test, CS1000 sent 11 digits in the destination headers (e.g., Request-URI and To) and sent 10 digit in the source headers (e.g., From, Contact, and P-Asserted-Identity (PAI)). MTS Allstream sent 10 digits in destination headers and sent 11 digits in source headers.

These Application Notes assume the basic configuration has already been administered and is not discussed here. For further information on CS1000, please consult references in **Section 11**.

5.1. Log into CS1000

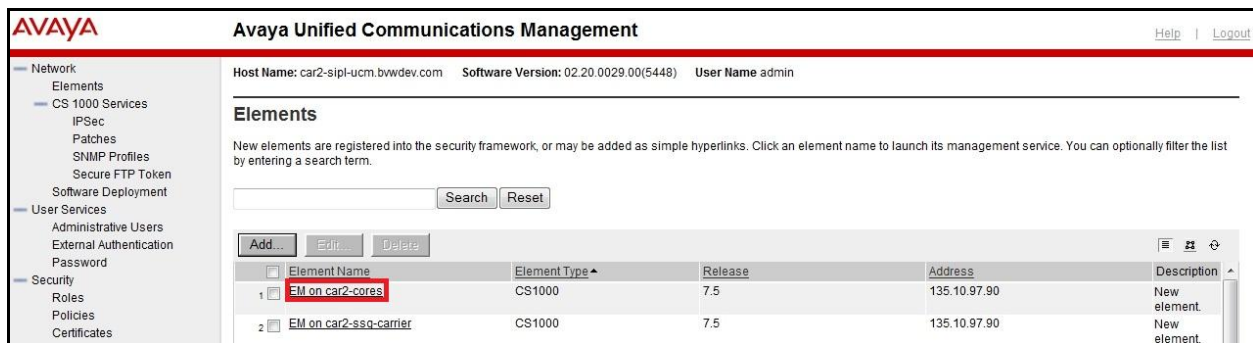
5.1.1. Log into Unified Communications Management (UCM) and Element Manager (EM)

a) Open web browser and connect to the UCM GUI <https://<UCM IP address>> as shown in the screenshot below then log in using an appropriate username and password.



The screenshot shows the Avaya login page. At the top right is the Avaya logo. Below it, a disclaimer states: "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." To the right of the disclaimer are input fields for "User ID:" (containing "admin") and "Password:" (containing "*****"). Below these fields is a "Log In" button. At the bottom left, the copyright notice reads: "Copyright © 2002-2010 Avaya Inc. All rights reserved."

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



The screenshot shows the Avaya Unified Communications Management interface. The top header includes the Avaya logo, the title "Avaya Unified Communications Management", and links for "Help" and "Logout". Below the header, the "Host Name" is "car2-sipl-ucm.bvwdev.com", "Software Version" is "02.20.0029.00(5448)", and "User Name" is "admin". The main content area is titled "Elements" and contains a search bar with "Search" and "Reset" buttons. Below the search bar are "Add...", "Edit...", and "Delete" buttons. A table lists elements with columns: "Element Name", "Element Type", "Release", "Address", and "Description". The first row is highlighted with a red box around the "Element Name" column header and the text "EM on car2-cores". The table data is as follows:

	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-ssg-carrier	CS1000	7.5	135.10.97.90	New element.

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



The screenshot shows the CS1000 Element Manager System Overview page. The top header includes the Avaya logo, the title "CS1000 Element Manager", and links for "Help" and "Logout". Below the header, the "Managing" IP address is "110.10.97.90" and the "Username" is "admin". The main content area is titled "System Overview" and contains a large box with the following information:

IP Address: 110.10.97.90
Type: Avaya Communication Server 1000E CPPM Linux
Version: 4121
Release: 750 Q +

5.1.2. Log into 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@110.10.97.190's password:
Last login: Thu Mar 10 17:38:16 2011 from 110.10.97.172
[admin@car2-ssg-carrier ~]$ cslogin
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 the basic configuration has already been administered and that a Node has already been created. This section describes configuration steps for Node ID 2004.

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

AVAYA **CS1000 Element Manager**

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.

Node ID	Components	Enabled Applications	ELAN IP	Node/TLAN IPv4	Node/TLAN IPv6	Status
2000	1	LTPS, Gateway (SIPGw)	-	110.10.97.168		Synchronized
2001	1	LTPS, Gateway (SIPGw)	-	110.10.97.170		Synchronized
2003	1	LTPS, Gateway (SIPGw)	-	110.10.97.158		Synchronized
2004	1	SIP Line, LTPS, PD, Gateway (SIPGw)	-	110.10.97.190		Synchronized
2005	1	LTPS, Gateway (SIPGw)	-	110.10.97.188		Synchronized

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

b) The **Node Details** page is shown in the screenshot below with the IP address of the Node ID 2004. The SIP Signaling Gateway uses the **Node IP Address** to connect to Session Manager for the SIP Trunk to MTS Allstream.

AVAYA **CS1000 Element Manager**

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

Node Details (ID: 2004) SIP Line, LTPS, PD, 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.

5.2.2. Administer Quality of Service (QoS)

Continued from Section 5.2.1. On the **Node Details** page, select the **Quality of Service (QoS)** link. The default Diffserv values are shown in the screenshot below. Then click the **Save** button.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation tree with the following items: UCM Network Services, Home, Links, Virtual Terminals, System, Alarms, Maintenance, Core Equipment, Peripheral Equipment, IP Network, Nodes: Servers, Media Cards (highlighted), Maintenance and Reports, Media Gateways, Zones, Host and Route Tables, Network Address Translation, 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, and Dialing and Numbering Plans. The main content area is titled 'Managing: 110.10.97.90 Username: admin' and shows the 'Node ID: 2004 - Quality of Service (QoS)' configuration page. The page includes a 'Diffserv Codepoint (DSCP)' section with the following settings: 'Enable Avaya automatic QoS' (checked), 'Control packets: 40' (range 0-63), 'Voice packets: 46' (range 0-63), 'VLAN tagging' (checked), '802.1Q support' (checked), and '802.1Q bits value (802.1P): 6' (range 0-7). A 'Save' button is highlighted at the bottom right. A note at the bottom states: 'Note: Changes made on this page will NOT be transmitted until the Node is also saved.'

5.2.3. Synchronize the new configuration

- Continued from Section 5.2.3, return to the **Node Details** page (not shown) and click on the **Save** button.
- The **Node Saved** screen is displayed. Click on the **Transfer Now** (not shown).
- The **Synchronize Configuration Files** screen is displayed (not shown). Check the Signaling Server checkbox and click on the **Start Sync** (not shown).
- 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

- To configure Voice Codec, select **IP Network** → **Nodes: Servers, Media Cards** from the left pane, and in the **IP Telephony Nodes** screen, select the **Node ID** of the CS1000 system. The **Node Details** screen is displayed as described in Section 5.2.1.
- On the **Node Details** page (not shown), click on **Voice Gateway (VGW) and Codec**.
- MTS Allstream supports voice codec G.729 and G.711 as fallback, payload size 20 ms, with VAD disabled. The following screenshots show appropriated 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 playback (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 playback (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

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 G729: ☒ Enabled

Voice payload size: 20 (milliseconds per frame)

Voice playback (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 playback (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

d) For Fax over IP, MTS Allstream supports G.711MU codec as default and does not support T.38. The following screenshot shows **Modem Pass Through** is selected for Node 2004; this configuration enables G.711MU codec to be used for fax calls between CS1000 and MTS Allstream. **Note:** The **V.21 Fax tone detection** should be unchecked to disable T.38 fax on the SIP Trunk.

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 (squelch DTMF from TDM to IP)
☒ Modem/Fax pass-through
☐ V.21 Fax tone detection
☐ R factor calculation

Voice Codescs

Codec G711: ☒ Enabled (required)
Voice payload size: 20 (milliseconds per frame)
Voice playout (jitter buffer) delay: 40 80 (milliseconds)
Note: Changes made on this page will NOT be transmitted until the Node is also saved.

* Required Value. **Save** Cancel

e) Click **Save**.

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

5.3.2. Administer Voice Codec on Media Gateways

CS1000 uses Media Gateways to support traditional analog and digital phone for voice calls over SIP trunk. Media Gateways are also needed to support analog terminals to send fax over IP.

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

b) The MTS Allstream supports voice codec G.729 and G.711 as fallback, payload size 20 ms, with VAD disabled. The screenshot below shows appropriated codec profile configured for Media Gateways.

AVAYA CS1000 Element Manager

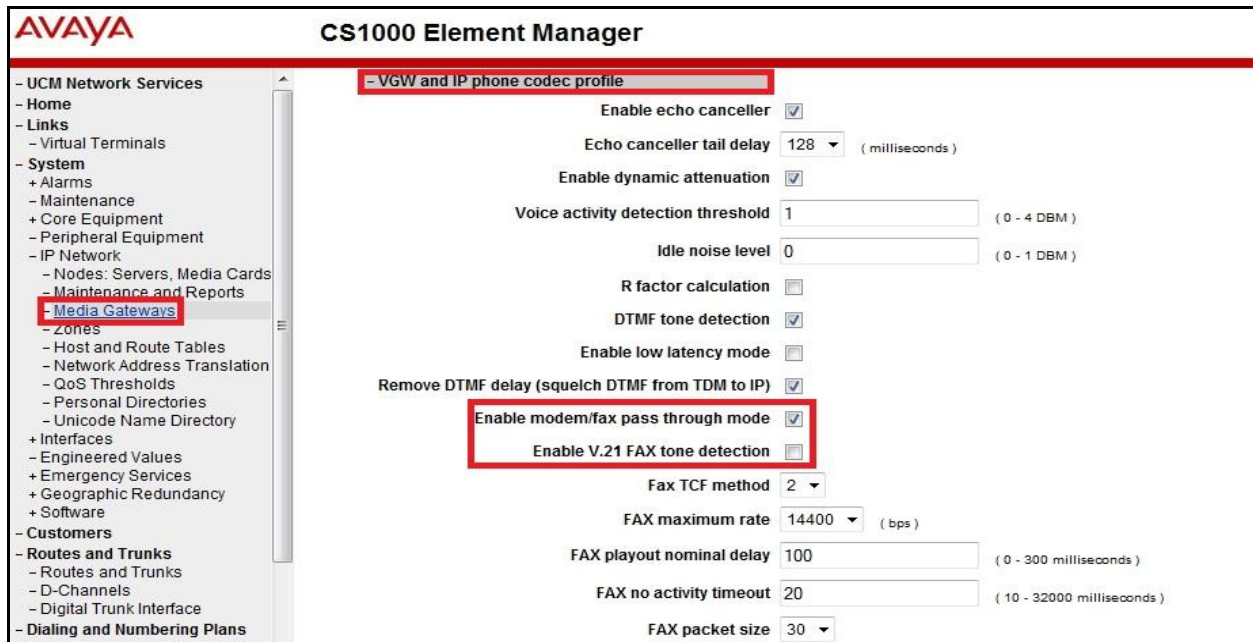
Help | Logout

Media Gateways

- Codec G711 Select ☒
Codec name G711
Voice payload size 20 (ms/frame)
Voice playout (jitter buffer) nominal delay 40
Modifications may cause changes to dependent settings
Voice playout (jitter buffer) maximum delay 80
Modifications may cause changes to dependent settings
VAD ☐

- 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 ☐

c) For Fax over IP, MTS Allstream supports G.711MU codec as default and does not support T.38. The following screenshot shows **Modem Pass Through** is selected for the Media Gateway; this configuration enables G.711MU codec to be used for fax calls between CS1000 and MTS Allstream. Note: the **V.21 Fax tone detection** should be unchecked to disable T.38 fax on the Media Gateway.



5.4. Administer Zones and Bandwidth

This section describes the steps to create 2 zones: zone 10 for VGW and IP phone and zone 255 for SIP Trunk. CS1000 uses zone configuration for bandwidth management purposes.

5.4.1. Create a zone for IP phones

- To create zone 10 for VGW and IP phone, select **IP Network** → **Zones** configuration from the left pane, click on the **Bandwidth Zones** (not shown).
- In **Bandwidth Zones** screen (not shown), click **Add** (not shown).
- 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 the screenshot below and click on the **Submit** button.

- **INTRA_STGY**: bandwidth configuration for local calls
- **INTER_STGY**: bandwidth configuration for the calls over trunk
- **BQ**: G.711 is first choice and G.729 is second choice
- **BB**: G.729 is first choice and G.711 is second choice
- **MO**: the zone type which is used for IP phones and Voice Gateway (VGW)
- **VTRK**: the zone type which is used for SIP trunk

AVAYA CS1000 Element Manager Help | Logout

Managing: 110.10.97.90 Username: admin
System » IP Network » **Zones** » Bandwidth Zones » Bandwidth Zones 10 » Edit Bandwidth Zone » Zone Basic Property and Bandwidth Management

Zone Basic Property and Bandwidth Management

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

Submit Refresh Cancel

MTS Allstream supports G.729 as the first choice, G.711 as fall-back. In the sample configuration, the **MO** Zone 10 is configured with **Strategy Best Quality (BQ)** to allow CS1000 select G.711MU as a first choice and G.729 as the second choice for both voice and fax calls. **Note:** In fax call scenario, the call has to be established with G.711MU otherwise it will fail because CS1000 cannot switch the codec to G.711MU.

5.4.2. Create a zone for virtual SIP trunk

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 and then click on the **Submit** button as shown in the screenshot below.

AVAYA CS1000 Element Manager Help | Logout

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 Quality (BQ)
Interzone Bandwidth (INTER_BW):	1000000 (0 - 10000000)
Interzone Strategy (INTER_STGY):	Best Quality (BQ)
Resource Type (RES_TYPE):	Shared (SHARED)
Zone Intent (ZBRN):	VTRK (VTRK)
Description (ZDES):	

Submit Refresh Cancel

MTS Allstream supports G.729 as the first choice, G.711 as fall-back. In the sample configuration, the **MO** Zone 255 is configured with **Strategy Best Quality (BQ)** to allow CS1000 select G.711MU as a first choice and G.729 as the second choice for both voice and fax calls. **Note:** In fax call scenario, the call has to be established with G.711MU otherwise it will fail because CS1000 cannot switch the codec to G.711MU.

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) To configure ISDN, select **Customers** in the left pane. The **Customers** screen is displayed (not shown). Click on the link associated with the appropriate customer, in this case is 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 (not shown).

b) The screen is populated with a list of **Feature Packages**. Select **Integrated Services Digital Network** to edit its parameters. The screen is populated with **Integrated Services Digital Network** parameters. Retain the default values for all remaining fields. Scroll down to the bottom of the screen, and click on the **Save** button (not shown)

The screenshot shows the AVAYA CS1000 Element Manager interface. On the left, a navigation pane lists various configuration categories, with 'Customers' highlighted. The main content area is titled 'Integrated Services Digital Network' and 'Package: 145'. It includes a checkbox for 'Integrated Services Digital Network' which is checked. Below this, there are input fields for 'Virtual private network identifier' (value: 4), 'Private network identifier' (value: 4), and 'Node DN' (value: 2004). Further down, there are fields for 'Multi-location business group' (value: 0) and 'Business sub group consult-only' (value: 65535). At the bottom, there is a 'Prefix 1' field.

5.5.2. Administer SIP Trunk Gateway to Session Manager

a) To configure SIP Trunk Gateway, select **IP Network → Nodes: Servers, Media Cards** configuration from the left pane, and in the **IP Telephony Nodes** screen, select the **Node ID** 2004. The **Node Details** screen is displayed as shown in **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 values which are highlighted in red boxes as shown in screenshot below. These configuration are obtained when user creates a SIP Entity on the Session Manager, these are shown in **Section 6.5**. Retain the default values for the remaining fields.

- **Vtrk gateway application: SIP Gateway (SIPGw)**
- **SIP domain name: avaya.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: avaya.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

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 as shown in the screenshot below, and retain the default values for the remaining fields.

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: 10.33.1.11
The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"

Port: 5060 (1 - 65535)

Transport protocol: TCP

Options: ☐ Support registration ☒ Primary CDS proxy

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

Port: 5060 (1 - 65535)

Transport protocol: TCP

Options: ☐ Support registration

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

e) On the same page, scroll down to the **SIP URI Map** section as shown in the screenshot below.

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

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: Used for making VTRK call from agent.

Converged telephone call forward DN:

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

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

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

Save Cancel

f) Then click on the **Save** button.

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

5.5.3. Administer Virtual D-Channel

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

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

- **D channel Card Type (CTYP): D-Channel is over IP (DCIP)**
- **Designator (DES):** A descriptive name

- **Interface type for D-channel (IFC): Meridian Meridian1 (SL1)**
- **Meridian 1 node type: Slave to the controller (USR)**
- **Release ID of the switch at the far end (RLS): 25**
- **Advanced options (ADVOPT):** check on **Network Attendant Service Allowed**

AVAYA CS1000 Element Manager Help | Logout

- Basic Configuration

Input Description	Input Value
Action Device And Number (ADAN):	DCH
D channel Card Type:	DCIP
Designator:	MTSAllStream
Recovery to Primary:	<input type="checkbox"/>
PRI loop number for Backup D-channel:	
User:	Integrated Services Signaling Link Dedicated (ISLD) *
Interface type for D-channel:	Meridian Meridian1 (SL1)
Country:	ETS 300 =102 basic protocol (ETSI)
D-Channel PRI loop number:	
Primary Rate Interface:	<input type="button" value="more PRI"/>
Secondary PRI2 loops:	
Meridian 1 node type:	Slave to the controller (USR)
Release ID of the switch at the far end:	25
Central Office switch type:	100% compatible with Bellcore standard (STD)
Integrated Services Signaling Link Maximum:	4000 Range: 1 - 4000
Signalling server resource capacity:	3700 Range: 0 - 3700

+ Basic options (BSCOPT)

- Advanced options (ADVOPT)

- 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:

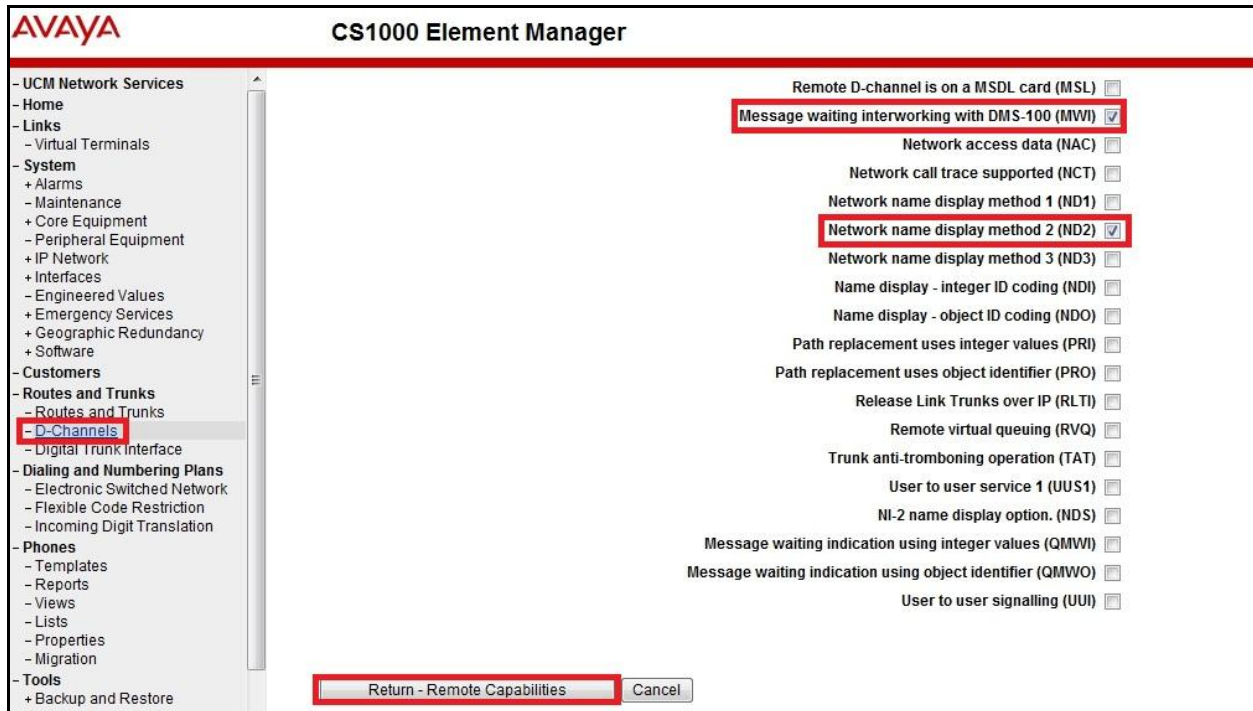
- Multilocation Business Group Allowed: ☐

- Network Attendant Service Allowed: ☒

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

+ Feature Packages

c) Click on the **Basic Options** and click on the **Edit** button at the **Remote Capabilities (RCAP)** attribute (not shown). The **Remote Capabilities Configuration** page will appear. Then verify the **ND2** and the **MWI** checkboxes as shown in the screenshot below.

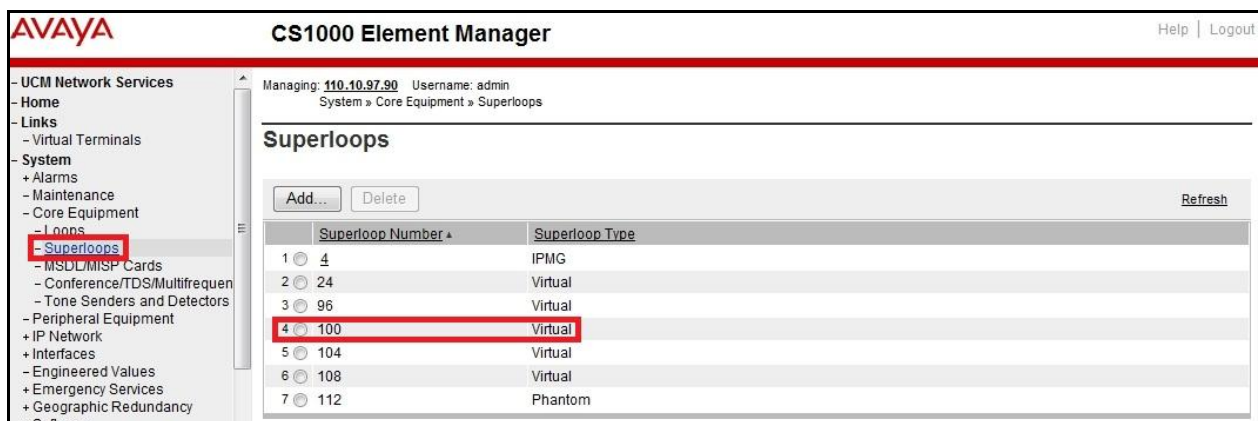


d) Click on the **Return – Remote Capabilities** button.

e) Click on the **Submit** button (not shown).

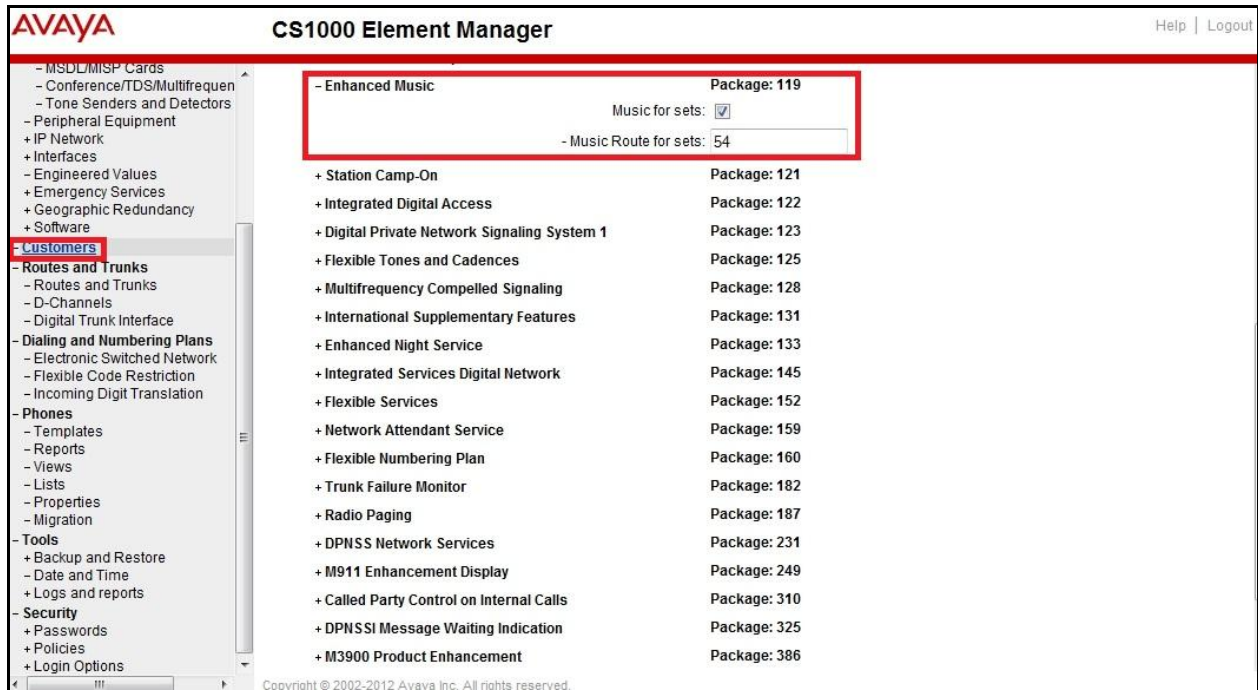
5.5.4. Administer Virtual Super-Loop

To add a virtual 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 the screenshot below. In this example, Superloop 100 is added and used.



5.5.5. Enable Music for Customer Data Block

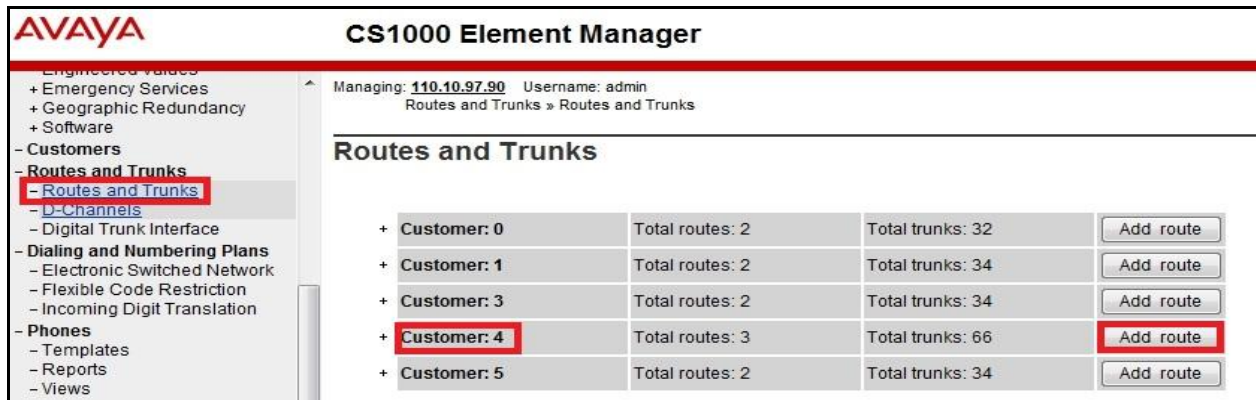
- a) To enable music for a customer, select **Customers** in the left pane. The **Customers** screen is displayed (not shown). Click on the link associated with the appropriate customer, in this case is 04. The **Customer 04 Edit** page will appear (not shown). Select the **Feature Packages** option from this page (not shown).
- b) The screen is populated with a list of **Feature Packages**. Select **Enhanced Music** to edit its parameters. Check to enable music for Customer 04, define music route 54 as shown in the red box of screenshot below. The CS1000 has been pre-configured with music route 54.



- c) Scroll down to the bottom of the screen, and click on the **Save** button at the bottom of the page (not shown).

5.5.6. Administer Virtual SIP Routes

a) To create a SIP Route, select **Routes and Trunks** → **Routes and Trunks** from the left pane to display the **Routes and Trunks** screen. In this example, **Customer 04** is being used. Click on the **Add route** button as shown in the screenshot below.



b) The **Customer 4, New Route Configuration** screen is displayed (not shown). Scroll down to the **Basic Configuration** section and enter the following values for the specified fields. Retain the default values for the remaining fields as shown in the screenshot below.

- **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 signalling 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
 - **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):** Checked
 - **Network call redirection (NCRD):** Checked
 - **Insert ESN access code (INAC):** Checked

AVAYA

CS1000 Element Manager

Help | Logout

UCM Network Services

Home

Links

Virtual Terminals

System

Alarms

Maintenance

Core Equipment

Loops

Superloops

MSDL/MISP Cards

Conference/TDS/Multifrequency

Tone Senders and Detectors

Peripheral Equipment

IP Network

Interfaces

Engineered Values

Emergency Services

Geographic Redundancy

Software

Customers

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

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):

☐

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

☒

Zone for codec selection and bandwidth management (ZONE):

00255

(0 - 8000)

Node ID of signaling server of this route (NODE):

2004

(0 - 9999)

Protocol ID for the route (PCID):

SIP (SIP)

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

☐

Integrated services digital network option (ISDN):

☒

Mode of operation (MODE):

Route uses ISDN Signaling 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):

☒

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)

TD; Reviewed:
SPOC 8/21/2012

Solution & Interoperability Test Lab Application Notes
©2012 Avaya Inc. All Rights Reserved.

26 of 93
MTSCS1KSMSBCE

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

AVAYA **CS1000 Element Manager** Help | Logout

Managing: **10.10.97.90** Username: admin
Routes and Trunks » **Routes and Trunks** » Customer 4, Route 104 Property Configuration

Customer 4, Route 104 Property Configuration

- + Basic Configuration**
 - Basic Route Options**

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

Billing number required (BLN): ☐

Call detail recording (CDR): ☒

- CDR records generated on incoming calls (INC): ☒

- CDR record printing content option for redirected calls (LAST): ☐

- Time to answer output in CDR (TTA): ☐

- CDR ACD Q initial connection records to be generated (QREC): ☐

- CDR on outgoing calls (OAL): ☒

- CDR on outgoing toll calls (OTL): ☐

- Answered call identification allowed (AIA): ☐

- CDR timing starts on answer supervision of outgoing calls (OAN): ☒

- outpulsed digits in CDR (OPD): ☒

- Number of digits printed (NDP): EXC 0

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**

- Click on **Advance Configurations**; check **Music-on-hold (MUS)** to enable music on hold on the route. Input music route 54 to the boxes as shown in the screenshot below. The CS1000 has been pre-configured with route 54 as a music route.

AVAYA CS1000 Element Manager Help | Logout

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
- + Basic Route Options
- + Network Options
- + General Options
- + Advanced Configurations**

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

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

ANI identifier number (ANTK):

AC15 timed reminder recall (ATRR): ☐

Auto terminate (AUTO): ☐

Collect call blocking allowed (CCBA): ☐

Call forward restriction (CFWR): ☐

Maximum number of CNI 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 (DCTI): 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): ☐

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

5.5.7. Administer Virtual Trunks

a) Continued from **Section 5.5.6**, the **Routes and Trunks** screen is displayed and updated with the newly added route (not shown). In the compliance test, route 104 was added. Click on the **Add trunk** button next to the newly added route 104 as shown in the screenshot below.

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	Actions	
+ Customer: 0	2	32	Add route	
+ Customer: 1	2	34	Add route	
+ Customer: 3	2	34	Add route	
- Customer: 4	3	66	Add route	
+ Route: 54 Type: MUS Description: MUSIC Edit Add trunk				
+ Route: 104 Type: TIE Description: MTSALLSTREAM Edit Add trunk				
+ Route: 114 Type: TIE Description: SIPL Edit Add trunk				
+ Customer: 5	2	34	Add route	

b) The **Customer 4, Route 104, Trunk 1 Property Configuration** is shown in the screenshot below. Enter **The Multiple trunk input number (MTINPUT)** field to add multiple trunks in a single operation, or repeat the operation for each trunk. In the certification test, 32 trunks are created (not shown). The following values are entered for specified fields and retain the default values for the remaining fields.

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

Terminal number: 100 1 01 00

Designator field for trunk: MTSALLSTREAM

Extended trunk: VTRK

Member number: 1 *

Level 3 Signaling: 8D

Card density: 8D

Start arrangement Incoming: Immediate (IMM)

Start arrangement Outgoing: Immediate (IMM)

Trunk group access restriction: 1

Channel ID for this trunk: 3

Class of Service: Edit

+ Advanced Trunk Configurations

Save
Delete
Cancel

c) 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. For **Media Security**, select **Media Security Never (MSNV)**. Enter the remaining values for the specified fields as shown in the screenshot below. 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 Help | Logout

Manual Incoming: Manual Incoming Denied (MID)

Media Security: Media Security Never (MSNV)

-Network Hook Flash Over M911P: 8D

- Polarity: 8D

- Priority: Low Priority (LPR)

Restriction level: Unrestricted (UNR)

- Reversed Ear Piece: Reversed Ear Piece denied (XREP)

- Short or long line: 8D

- Transmission Class of Service: Non-Transmission Compensated (NTC)

- Warning Tone: Warning Tone Allowed (WTA)

- Reversed Ear Piece: Reversed Ear Piece denied (XREP)

- ARF Supervised COT: 8D

Return Class of Service
Cancel

5.5.8. Administer Calling Line Identification Entries

a) To create a Calling Line Identification Entry, select **Customers > 04 > ISDN and ESN Networking**. Click on **Calling Line Identification Entries** link at the bottom of the page (not shown).

b) On the Calling Line Identification Entries page (not shown), click **Add**.

c) Add entry **0** as shown in the screenshot below.

- **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** is 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** is 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** is to be used for call display purpose for Call Type = Local Subscriber (NXX)
- **Calling Party Name Display:** Uncheck Roman characters

AVAYA CS1000 Element Manager

Managing: 110.10.97.90 Username: admin

Customers » Customer 04 » Customer Details » ISDN and ESN Networking » Calling Line Identification Entries » Edit Calling Line Identification 0

Edit Calling Line Identification 0

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

Save Cancel

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

AVAYA CS1000 Element Manager

Managing: **110.10.97.90** Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN)

Electronic Switched Network (ESN)

- + Customer 00
- + Customer 01
- + Customer 03
- **Customer 04**
 - Network Control & Services
 - Network Control Parameters (NCTL)
 - **ESN Access Codes and Parameters (ESN)**
 - **Digit Manipulation Block (DGT)**
 - Home Area Code (HNP)
 - Flexible CLID Manipulation Block (CMDB)
 - Free Calling Area Screening (FCAS)
 - Free Special Number Screening (FSNS)
 - **Route List Block (RLB)**
 - Incoming Trunk Group Exclusion (ITGE)
 - Network Attendant Services (NAS)
 - Coordinated Dialing Plan (CDP)
 - Local Steering Code (LSC)
 - Distant Steering Code (DSC)
 - Trunk Steering Code (TSC)
 - Numbering Plan (NET)
 - Access Code 1
 - Home Location Code (HLOC)
 - Location Code (LOC)
 - **Numbering Plan Area Code (NPA)**
 - Exchange (Central Office) Code (NXX)
 - **Special Number (SPN)**
 - Network Speed Call Access Code (NSCL)
 - Access Code 2
 - Home Location Code (HLOC)
 - Location Code (LOC)
 - Numbering Plan Area Code (NPA)
 - Exchange (Central Office) Code (NXX)
 - Special Number (SPN)
 - Network Speed Call Access Code (NSCL)

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

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: 6

NARS Access Code 2: 9

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

Expensive Route Warning Tone: ☒

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

Coordinated Dialing Plan feature for this customer: ☒

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

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

Routing Controls: ☐

Check for Trunk Group Access Restrictions: ☐

Limits

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

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

a) Login Call Server CLI (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)

- To create a DMI, select **Dialing and Numbering Plans** → **Electronic Switched Network** from the left pane to display the **Electronic Switched Network** (ESN) screen (not shown).
- Select **Digit Manipulation Block** (DGT) (not shown).
- In the **Choose a DMI Number** field, select an available DMI from the drop-down list and click to **Add** (not shown).
- The screenshot below shows DMI 1 is created with following values.
 - Number of leading digits to be Deleted** (Del): 0
 - Insert**: 11129
 - Call Type to be used by the manipulated digits** (CTYP): NPA

The screenshot displays the AVAYA CS1000 Element Manager web interface. The left-hand navigation pane shows a tree structure with categories like UCM Network Services, System, IP Network, and Customers. Under 'Dialing and Numbering Plans', the 'Electronic Switched Network' option is highlighted. The main content area is titled 'Digit Manipulation Block' and contains the following configuration fields:

- Digit Manipulation Index numbers:** 1
- Number of leading digits to be deleted:** 0 (with a range of 0 - 19)
- Insert:** 11129
- IP Special Number:** ☐
- Call Type to be used by the manipulated digits:** NPA (NPA) (selected from a dropdown menu)

At the bottom right of the configuration area, there are four buttons: **Submit**, **Refresh**, **Delete**, and **Cancel**.

Note: This DMI will add a prefix 11129 to URI-User of Request Line for outbound call. This prefix is defined by MTS Allstream. MTS Allstream requires different prefix per SIP Trunk group. This configuration is to meet the SIP specification of MTS Allstream. The prefix will be automatically deleted by MTS Allstream and not to be sent to PSTN.

d) Click Submit.

5.6.4. Route List Block (RLB)

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

a) To create RLB 104, 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 **Section 5.6.1**.

b) Select an available value (e.g. 104) in the textbox for the **route list index** and click on the “**to Add**” button (not shown).

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

- **Route number (ROUT):** 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. The left sidebar shows a navigation tree with 'Electronic Switched Network' highlighted under 'Dialing and Numbering Plans'. The main content area is titled 'Data Entry of a Route List Block'. At the top, it shows 'Route List Block Index: 104'. Below this, the 'General Properties' section includes 'Entry Number for the Route List: 0'. The 'Indexes' section contains several dropdown menus and text boxes: 'Time of Day Schedule: 0', 'Facility Restriction Level: 0 (0 - 7)', 'Digit Manipulation Index: 1' (highlighted with a red box), 'ISL D-Channel Down Digit Manipulation Index: 0 (0 - 1999)', 'Free Calling Area Screening Index: 0', 'Free Special Number Screening Index: 0', 'Business Network Extension Route: [checkbox]', and 'Incoming CLID Table: 0 (0 - 256)'. The 'Options' section at the bottom includes 'Local Termination entry: [checkbox]', 'Route Number: 104' (highlighted with a red box), and 'Skip Conventional Signaling: [checkbox]'. The top of the interface shows the AVAYA logo, 'CS1000 Element Manager', and user information: 'Managing: 110.10.97.90 Username: admin'.

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

5.6.5. Incoming Digit Translation (IDC)

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

a) To create an IDC, 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 (not shown).

b) Click on **New DCNO** to create a digit translation entry. In this example, Digit Conversion Tree Number (**DCNO**) **0** is created. Detail configuration of the **DCNO** is shown in screenshot below. The **Incoming Digits** can be added to map to the **Converted Digits** which would be the CS1000 DN. This **DCNO** has been assigned to route 104 as shown in **Section 5.5.6**.

In the following configuration, incoming calls from PSTN with prefix 64777612XX will be translated to CS1000 DN 12XX. The DID 6477761233 is translated to 3111 for Voicemail accessing purpose.

AVAYA CS1000 Element Manager

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		

5.6.6. Outbound Call - Special Number Configuration

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

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

b) Enter SPN and then click on the “to Add” button (not shown). The screenshot below shows all the special numbers used for this testing.

Special Number: 0

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

Special Number: 411

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

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a tree view with the following items: UCM Network Services, Home, Links, System, Alarms, Maintenance, Core Equipment, Loops, Superloops, MSD/MISP 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** (highlighted), **Electronic Switched Network** (highlighted), Flexible Code Restriction, Incoming Digit Translation, and Phones. The main content area is titled 'Special Number List' and shows a table of special numbers. The table has three rows: Special Number -- 0, Special Number -- 1, and Special Number -- 411. Each row has an 'Edit' button. The details for each special number are as follows:

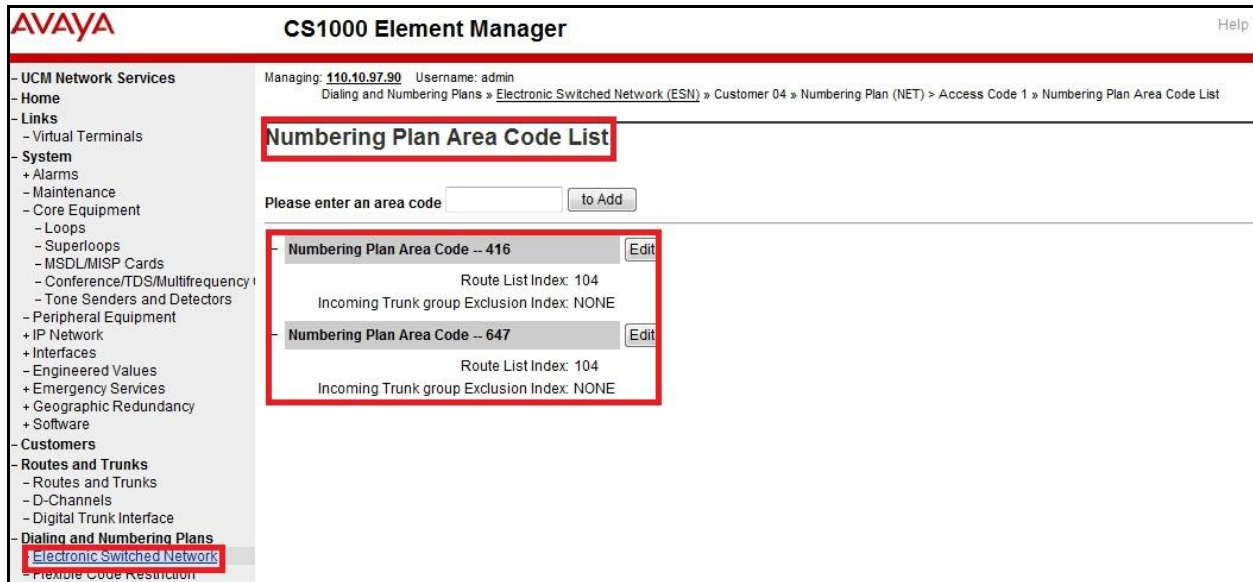
Special Number	Flexible length	International dialing plan	Type of call that is defined by the special number	Route list index
0	0	NO	NONE	104
1	11	NO	NATL	104
411	3	NO	SSER	104

5.6.7. Outbound Call - Numbering Plan Area (NPA)

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

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

b) Enter area code desired in the textbox and click on the “to Add” button (not shown). The screenshot below shows NPA numbers 416 and 647 are configured for this testing. These NPA numbers are associated to the SIP Trunk.



6. Configure Avaya Aura® Session Manager

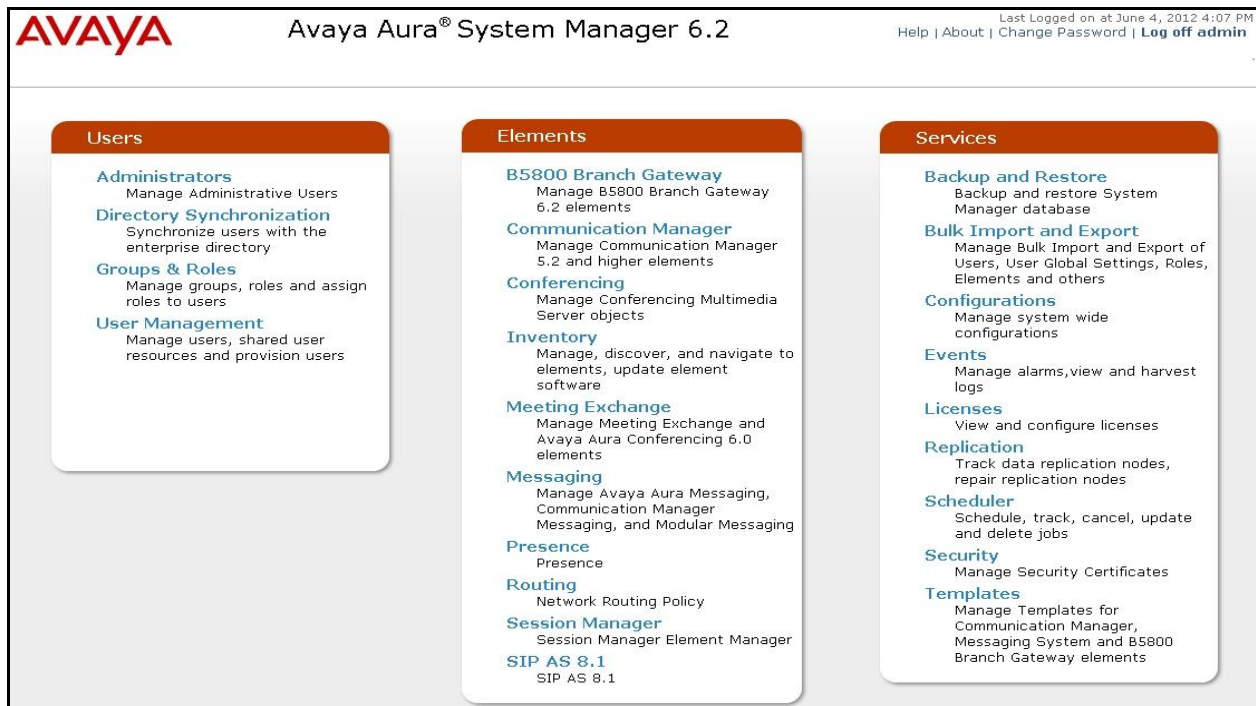
This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

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

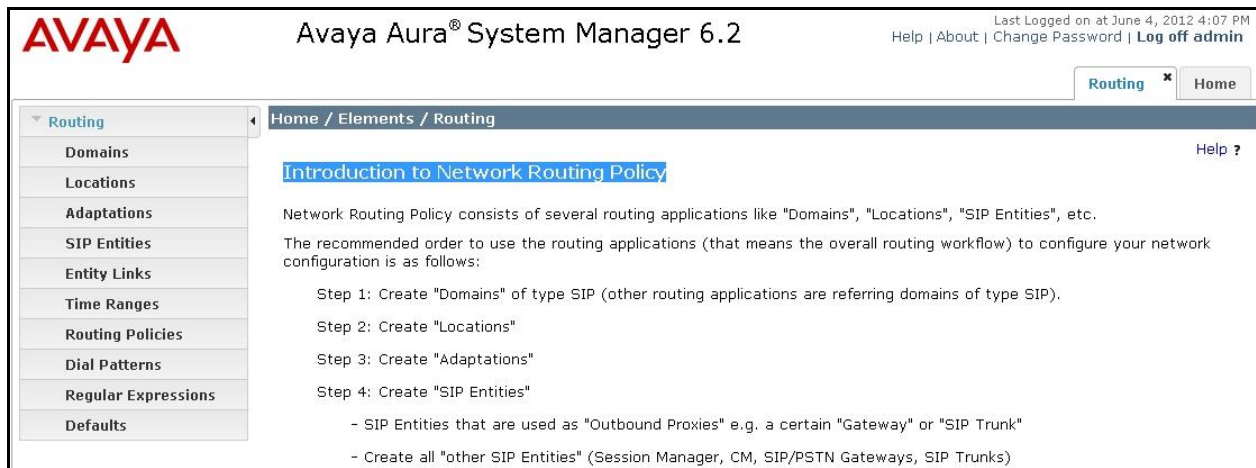
It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session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

6.1. System Manager Login and Navigation

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



Most of the configuration items are performed in the Routing element. Click on **Routing** in the **Elements** column to bring up the **Introduction to Network Routing Policy** screen as below.

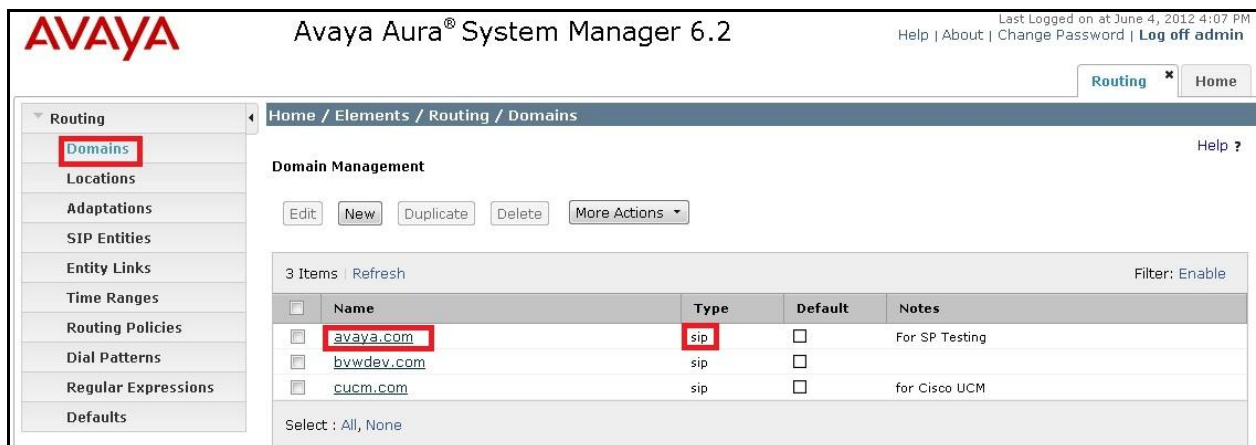


The navigation tree displayed in the left pane will be referenced in subsequent sections to navigate to items requiring configuration.

6.2. Specify SIP Domain

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

The following screenshot shows the list of configured SIP domains. The domain **avaya.com** is already being used for communication among a number of Avaya systems and applications with SIP integration to Session Manager. The domain **avaya.com** is not known to the MTS Allstream. Later on, it will be adapted by Avaya SBCE to IP address based URI-Host to meet the SIP specification of MTS Allstream.



6.3. Add Location

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

To add a location, navigate to **Routing → Locations** in the left-hand navigation pane and click the **New** button in the right pane (not shown).

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

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

In the **Location Pattern** section (not shown), click **Add** and enter the following values:

- **IP Address Pattern:** Enter two subnets 110.10.x.x and 10.33.x.x which are an IP address patterns used to identify the location including CS1000, Session Manager and Avaya SBCE
- **Notes:** Add a brief description (optional)

The screenshot displays the Avaya Aura System Manager 6.2 web interface. On the left, a navigation menu lists various configuration areas, with 'Locations' under the 'Routing' section highlighted. The main content area is titled 'Home / Elements / Routing / Locations'. It features a 'Location Details' section with a 'General' tab. In the 'General' tab, the 'Name' field is populated with 'Belleville'. Below this, the 'Notes' field is empty. Further down, the 'Overall Managed Bandwidth' section shows 'Managed Bandwidth Units' set to 'kbit/sec', 'Total Bandwidth' set to 100000, 'Multimedia Bandwidth' set to 100000, and a checkbox for 'Audio Calls Can Take Multimedia Bandwidth' which is checked. At the top right of the main area, there are 'Commit' and 'Cancel' buttons, along with a 'Help ?' link. The top of the page shows the Avaya logo, the title 'Avaya Aura® System Manager 6.2', and a status bar indicating the user is logged in as 'admin'.

6.4. Add Adaptation Module

Session Manager can be configured with Adaptation module that modifies SIP messages before or after routing decisions have been made.

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

The following screen shows adaptations named CS1000 and Diversion were configured and used in the compliance test.

AVAYA Avaya Aura® System Manager 6.2 Last Logged on at June 4, 2012 4:07 PM
Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Adaptations

Adaptations Help ?

Edit New Duplicate Delete More Actions

3 Items Refresh Filter: Enable

Name	Module name	Egress URI Parameters	Notes
Cisco UCMZ	CiscoAdapter iosrcd=bvwdev.com odstd=135.10.97.249		
CS1000	CS1000Adapter fromto=true		
Diversion	DiversionTypeAdapter MIME=no		

Select : All, None

The CS1000 adaptation will later be assigned to the CS1000 SIP Entity. This adaptation uses the CS1000Adapter to normalize the SIP traffic exchange between CS1000 and Session Manager. The parameter is set to **fromto=true** to allow Session Manager to normalize From and To headers. The screen below shows the CS1000 adaptation configured for the testing associated with these Application Notes:

AVAYA Avaya Aura® System Manager 6.2 Last Logged on at June 4, 2012 4:07 PM
Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Adaptations

Adaptation Details Commit Cancel

General

* Adaptation name: CS1000

Module name: CS1000Adapter

Module parameter: fromto=true

Egress URI Parameters:

Notes:

The adaptation named Diversion shown below will later be assigned to the Avaya SBCE SIP Entity. As a requirement of MTS Allstream, only Diversion header is supported on the SIP Trunk. Session Manager uses the DiversionTypeAdapter to convert the History-Info to Diversion header on the egress traffic to MTS Allstream. The parameter is set to **MIME=no** to allow Session Manager to send only SDP in SIP message body, other part will be deleted.

AVAYA Avaya Aura® System Manager 6.2 Last Logged on at June 4, 2012 4:07 PM
Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Adaptations

Adaptation Details Commit Cancel

General

* Adaptation name: Diversion

Module name: DiversionTypeAdapter

Module parameter: MIME=no

Egress URI Parameters:

Notes:

6.5. Add SIP Entities

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

To add a new SIP Entity, navigate to **Routing → SIP Entities** in the left navigation pane and click on the **New** button in the right pane (not shown).

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

- **Name:** Enter a descriptive name
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling
- **Type:** Select **Session Manager** for Session Manager and select **Other** for CS1000 and Avaya SBCE
- **Adaptation:** Select the CS1000 adaptation for SIP Entity for CS1000 and select Diversion adaptation for SIP Entity for Avaya SBCE. The adaptations are created in **Section 6.4**. The Adaptation is not available for Session Manager type
- **Location:** Select one of the locations defined previously in **Section 6.3**
- **Time Zone:** Select the time zone for the location above

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

The screenshot displays the Avaya Aura System Manager 6.2 web interface. The left-hand navigation pane shows a tree structure with 'Routing' expanded and 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and 'General'. The form contains the following fields: 'Name' with the value 'InteropSM', 'FQDN or IP Address' with the value '10.33.1.11', 'Type' set to 'Session Manager', 'Notes' with the text 'Interop Session Manager', 'Location' set to 'Belleville', 'Outbound Proxy' (empty), 'Time Zone' set to 'America/Toronto', and 'Credential name' (empty). At the bottom, the 'SIP Link Monitoring' section shows 'Use Session Manager Configuration'. The top right of the interface indicates the user is logged in as 'admin' and shows a 'Log off' button.

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

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

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

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

The compliance test used **Port** 5060 with TCP for connecting to CS1000 and Avaya SBCE. It is shown in the screenshot below.

Port

TCP Failover port:

TLS Failover port:

4 Items | Refresh Filter: Enable

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	TCP	avaya.com	<input type="text"/>
<input type="checkbox"/>	5060	UDP	bwdev.com	<input type="text"/>
<input type="checkbox"/>	5061	TLS	bwdev.com	<input type="text"/>
<input type="checkbox"/>	5070	UDP	bwdev.com	<input type="text"/>

The following screen shows the addition of CS1000 SIP Entities. In order for Session Manager to send SIP traffic to CS1000, it is necessary to create a SIP Entity for CS1000. The **FQDN or IP Address** field is set to the IP address of CS1000. Select **Type** is **Other**. Select Adaptation CS1000 created in **Section 6.4**.

AVAYA Avaya Aura® System Manager 6.2 Last Logged on at June 4, 2012 4:07 PM
Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / SIP Entities

SIP Entity Details Help ?

General

* Name: CS1KR75_MTS

* FQDN or IP Address: 110.10.97.190

Type: Other

Notes: CS1KR75_MTS

Adaptation: CS1000

Location: Belleville

Time Zone: America/Toronto

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

CommProfile Type Preference:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

The following screen shows the addition of the SIP Entity for Avaya SBCE. The **FQDN or IP Address** field is set to the IP address of its private network interface (see **Figure 1**). Select **Type** is **Other**. Select Adaptation Diversion created in **Section 6.4**.

The screenshot shows the Avaya Aura System Manager 6.2 web interface. The left navigation pane has 'SIP Entities' selected under the 'Routing' section. The main content area is titled 'SIP Entity Details' and 'General'. The form contains the following fields:

- Name:** AvayaSBCE
- FQDN or IP Address:** 110.10.97.189
- Type:** Other
- Notes:** AvayaSBCE
- Adaptation:** Diversion
- Location:** Belleville
- Time Zone:** America/Toronto
- Override Port & Transport with DNS SRV:** ☐
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty field)
- Call Detail Recording:** none
- CommProfile Type Preference:** (empty dropdown)
- SIP Link Monitoring:** Use Session Manager Configuration

Buttons for 'Commit' and 'Cancel' are visible in the top right corner of the form area.

6.6. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links are created for CS1000 and for Avaya SBCE. To add an Entity Link, navigate to **Routing → Entity Links** in the left navigation pane and click on the **New** button in the right pane (not shown).

Fill in the following fields in the new row that is displayed:

- **Name:** Enter a descriptive name
- **SIP Entity 1:** Select the Session Manager
- **Protocol:** Select the transport protocol used for this link
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For CS1000, this must match the port of **Proxy Server Route 1** which defined in **Section 5.5.2** step d)
- **SIP Entity 2:** Select the name of the other system. For CS1000, select the CS1000 SIP Entity; for Avaya SBCE, select the Avaya SBCE SIP Entity. The SIP Entities are defined in **Section 6.5**
- **Port:** Port number on which the other system receives SIP requests from the Session Manager. For CS1000, this must match the **Local SIP Port** defined in **Section 5.5.2** step c)
- **Connection Policy:** Select **Trusted**. Note: If this is not selected, calls from the associated SIP Entity specified in **Section 6.5** will be denied
- Click **Commit** to save

The following screens illustrate the Entity Links to CS1000 and Avaya SBCE. For the compliance test, transport protocol TCP and port 5060 were used to match the values of **Proxy Server Route 1** defined in **Section 5.5.2** step d) and in **Figure 1**.

Entity Link to CS1000:

Entity Links

Add Remove

1 Item | Refresh Filter: Enable

<input type="checkbox"/>	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
<input type="checkbox"/>	InteropSM	TCP	* 5060	CS1KR75_MTS	* 5060	Trusted

Select : All, None

Entity Link to Avaya SBCE:

Entity Links

Add Remove

1 Item | Refresh Filter: Enable

<input type="checkbox"/>	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
<input type="checkbox"/>	InteropSM	TCP	* 5060	AvayaSBCE	* 5060	Trusted

Select : All, None

6.7. Add Routing Policies

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

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

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

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

The following screens show the Routing Policies **To_CS1K** for CS1000.

Avaya Aura® System Manager 6.2

Home / Elements / Routing / Routing Policies

Routing Policy Details

General

* Name: To_CS1K

Disabled: ☐

* Retries: 0

Notes: To_CS1K

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
CS1KR75_MTS	110.10.97.190	Other	CS1KR75_MTS

The following screens show the Routing Policies **To_MTSAllstream** for the Avaya SBCE.

Avaya Aura® System Manager 6.2

Home / Elements / Routing / Routing Policies

Routing Policy Details

General

* Name: To_MTSAllstream

Disabled: ☐

* Retries: 0

Notes: To_MTSAllstream

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
AvayaSBCE	110.10.97.189	Other	AvayaSBCE

6.8. Add Dial Patterns

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

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

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

In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating

location for use in the match criteria. Lastly, select the routing policy from the list that will be used to route all calls that match the specified criteria. Click **Select**.

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

Two examples of the dial patterns used for the compliance test are shown below, one for outbound calls from the enterprise to the PSTN and one for inbound calls from the PSTN to the enterprise.

The first example shows dial pattern for outbound call. The dialed numbers has to begin with prefix **11129** and has a destination domain of **avaya.com** uses route policy **To_MTSAllstream** as defined in **Section 6.6**.

The screenshot shows the Avaya Aura System Manager 6.2 web interface. The left sidebar contains a navigation menu with options: Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, **Dial Patterns** (highlighted with a red box), Regular Expressions, and Defaults. The main content area is titled 'Dial Pattern Details' and includes a 'General' tab. The 'General' tab contains the following fields:

- * Pattern: 11129 (highlighted with a red box)
- * Min: 5 (highlighted with a red box)
- * Max: 36 (highlighted with a red box)
- Emergency Call: ☐
- Emergency Priority: 1
- Emergency Type:
- SIP Domain: avaya.com (highlighted with a red box)
- Notes:

 At the top right of the main area are 'Commit' and 'Cancel' buttons (both highlighted with red boxes). Below the 'General' tab is a section titled 'Originating Locations and Routing Policies' which includes 'Add' and 'Remove' buttons. Below this is a table with 1 item. The table has columns: Originating Location Name, Originating Location Notes, Routing Policy Name, Rank, Routing Policy Disabled, Routing Policy Destination, and Routing Policy Notes. The single row in the table is:

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
Belleville		To_MTSAllstream	0	<input type="checkbox"/>	AvayaSBCE	To_MTSAllstream

 The row is highlighted with a red box. At the bottom of the table area is a 'Select' dropdown menu with options 'All, None'.

Note: This is a requirement of MTS Allstream. The prefix 11129 will be automatically deleted by MTS Allstream and not to be sent to PSTN. For example, if a CS1000 phone dials 11 digits to make a long distance call to PTSN, the DMI 1 configured in **Section 5.6.3** will insert prefix 11129 before sending to Session Manager, the Dial Pattern 11129 configured on Session Manager then routes the call to MTS Allstream. Because the prefix 11129 applies to all outbound calls from CS1000 as described in **Section 5.6.6 and 5.6.7**, Session Manager just needs to use only Dial Pattern 11129 for all outbound calls. As a result, the length of Dial Pattern 11129 should be flexible but cannot exceed 36 digits as it is a maximum dial digits allowed by Session Manager.

The second example shows that inbound 10-digit numbers that start with **647776** to domain **avaya.com** uses route policy **To_CS1000** as defined in **Section 6.6**. These are the DID numbers assigned to the enterprise by MTS Allstream.

AVAYA

Avaya Aura® System Manager 6.2

Last Logged on at June 4, 2012 10:00 PM

[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing

Home

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

General

* Pattern: 647776

* Min: 10

* Max: 10

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: avaya.com

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh

Filter: Enable

	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		To_CS1K	0	<input type="checkbox"/>	CS1KR75_MTS	To_CS1K

Select : All, None

6.9. Add/View Session Manager

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

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

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

The screen below shows the Session Manager values used for the compliance test.

Avaya Aura® System Manager 6.2

Last Logged on at June 4, 2012 10:00 PM
Help | About | Change Password | Log off admin

Session Manager x Routing x Home

Home / Elements / Session Manager

Edit Session Manager

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

General

SIP Entity Name: InteropSM

Description:

*Management Access Point Host Name/IP: 10.33.1.10

*Direct Routing to Endpoints: Enable

Commit Cancel

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

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

Use default values for the remaining fields. Click **Save** (not shown) to add this Session Manager. The screen below shows the remaining Session Manager values used for the compliance test.

Security Module

SIP Entity IP Address: 10.33.1.11

*Network Mask: 255.255.255.192

*Default Gateway: 10.33.1.1

*Call Control PHB: 46

*QOS Priority: 6

*Speed & Duplex: Auto

VLAN ID:

7. Configure Avaya Session Border Controller for Enterprise

This section covers the configuration of Avaya Session Border Controller for Enterprise (Avaya SBCE). It is assumed that the software has already been installed. For additional information on these configuration tasks, see Reference [14] and [15].

The compliance test comprises of configuration for two major components, trunk server for service provider and call server for the enterprise. Each component consists of a set of Global Profiles, Domain Policies and Device Specific Settings. The configuration is performed using the Avaya SBCE web user interface as described in the following sections.

Trunk server configuration elements for service provider MTS Allstream:

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

Call server configuration elements at the enterprise for Session Manager:


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

- Device Specific Settings:
 - o Network Management
 - o Media Interface
 - o Signaling Interface
 - o End Point Flows → Server Flows
 - o Session Flows

7.1. Avaya Session Border Controller for Enterprise Login

Use a Web browser to access the Unify Communication Security (UC-Sec) web interface, enter `https://<ip-addr>/ucsec` in the address field of the web browser (not shown), where <ip-addr> is the management LAN IP address of UC-Sec.

Enter appropriate credentials and click **Sign In**.

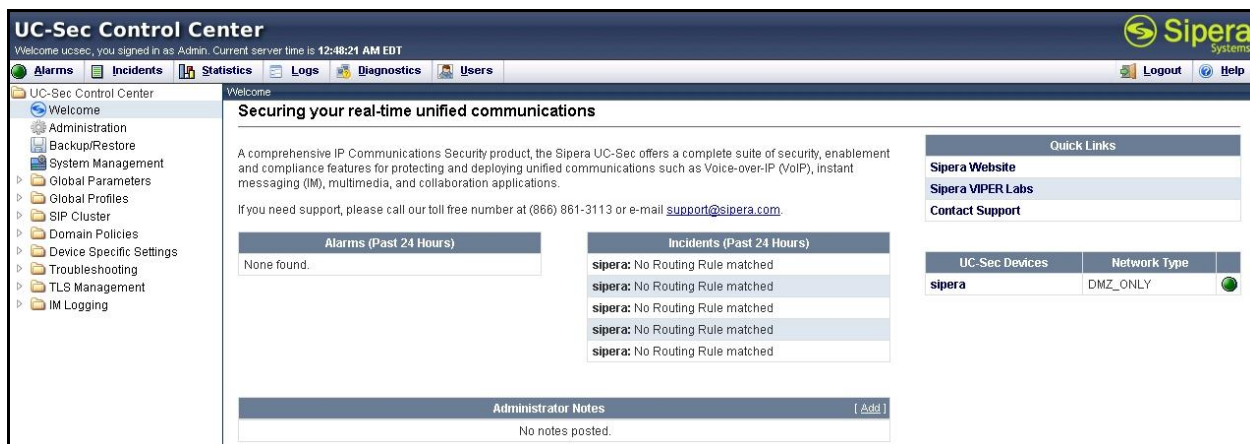


The UC-Sec™ family of products from Siper Systems delivers comprehensive VoIP security by adapting the best practices of internet security and by using unique, sophisticated techniques such as VoIP protocol misuse & anomaly detection, behavioral learning based anomaly detection and voice spam detection to protect VoIP networks.

[Visit the Siper Systems website to learn more.](#)

NOTICE TO USERS: This system is for authorized use only. Unauthorized use of this system is strictly prohibited. Unauthorized or improper use of this system may result in civil and/or criminal penalties. Use of this system constitutes consent to security monitoring. All activity is logged with login info, host name and IP address.

The main page of the **UC-Sec Control Center** will appear as shown below.



To view system information that has been configured during installation, navigate to **UC-Sec Control Center → System Management**. A list of installed devices is shown in the right pane. In the compliance test, a single device named **sipera** is added. To view the configuration of this device, click the **View Config** icon (the third icon from the right) as shown below.



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

System Information: sipera				
Network Configuration				
General Settings		Device Settings		
Appliance Name	sipera		HA Mode	No
Box Type	SIP		Secure Channel Mode	None
Deployment Mode	Proxy		Two Bypass Mode	No
Network Settings				
IP	Public IP	Netmask	Gateway	Interface
110.10.97.189	110.10.97.189	255.255.255.192	110.10.97.129	A1
110.10.98.112	110.10.98.112	255.255.255.224	110.10.98.97	B1
110.10.98.108	110.10.98.108	255.255.255.224	110.10.98.97	B1
DNS Configuration		Management IP(s)		
Primary DNS	110.10.98.60		IP	110.10.98.85
Secondary DNS				
DNS Location	DMZ			
DNS Client IP	110.10.97.189			

7.2. Global Profiles

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

7.2.1. Uniform Resource Identifier (URI) Groups

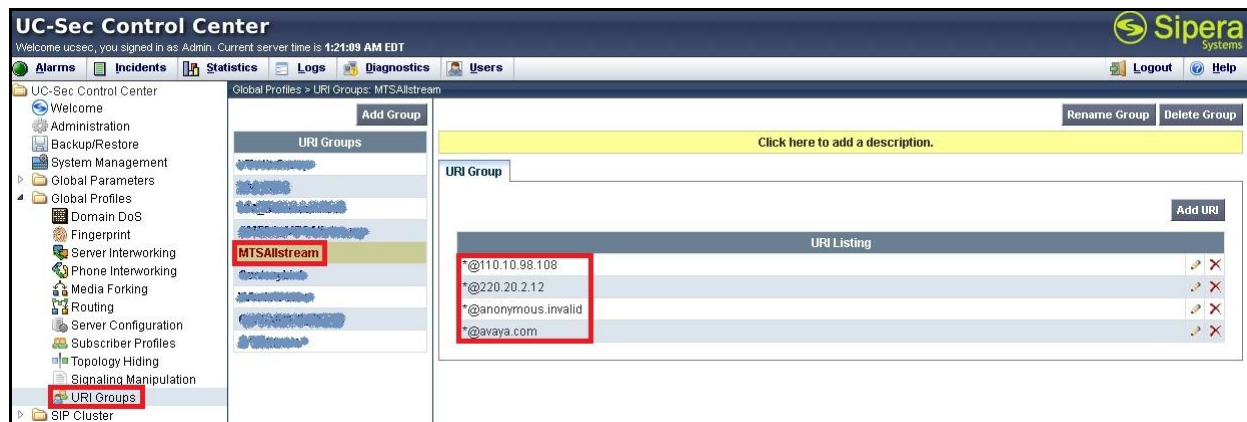
The **URI Group** feature allows user to create any number of logical URI groups that are comprised of individual SIP subscribers located in that particular domain or group. These groups are used by the various domain policies to determine which actions (Allow, Block, or Apply Policy) should be used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

To add an **URI Group**, select **UC-Sec Control Center → Global Profiles → URI Groups**. Click on **Add Group** (not shown).

In the compliance test, a URI Group named **MTSAllstream** was added with URI type **Plain** (not shown) and consists of four domain [*@anonymous.invalid](#), [*@avaya.com](#), [*@110.10.98.108](#) and [*@220.20.2.12](#). Domain **anonymous.invalid** is defined for private calls received either from call server or trunk server had URI-Host masked by **anonymous.invalid**. The enterprise domain name **avaya.com** is for SIP Trunk domain defined in **Section 5.5.2** step c) between CS1000 and Avaya SBCE via Session Manager. For the public SIP Trunk between Avaya SBCE and MTS Allstream, the Avaya SBCE public IP address 110.10.98.108 is set as URI-Host of From, PAI and Diversion headers while the public IP address of MTS Allstream 220.20.2.12 is set as URI-Host of Request-URI and To headers.

This URI-Group is used to match the From and To headers in a SIP call dialog received from both Session Manager and MTS Allstream. If there is a match, the Avaya SBCE will apply the appropriate **Routing Profile** and **Server Flow** to route the inbound and outbound call to the right destination. The **Routing Profile** and **Server Flow** are configured in **Section 7.2.2** and **Section 7.4.4** appropriately.

The screenshot below illustrates the URI Listing for URI Group **MTSAllstream**.



7.2.2. Routing Profiles

Routing Profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by **Routing Profiles** include packet transport settings, name server addresses and resolution methods, next hop routing information and packet transport types.

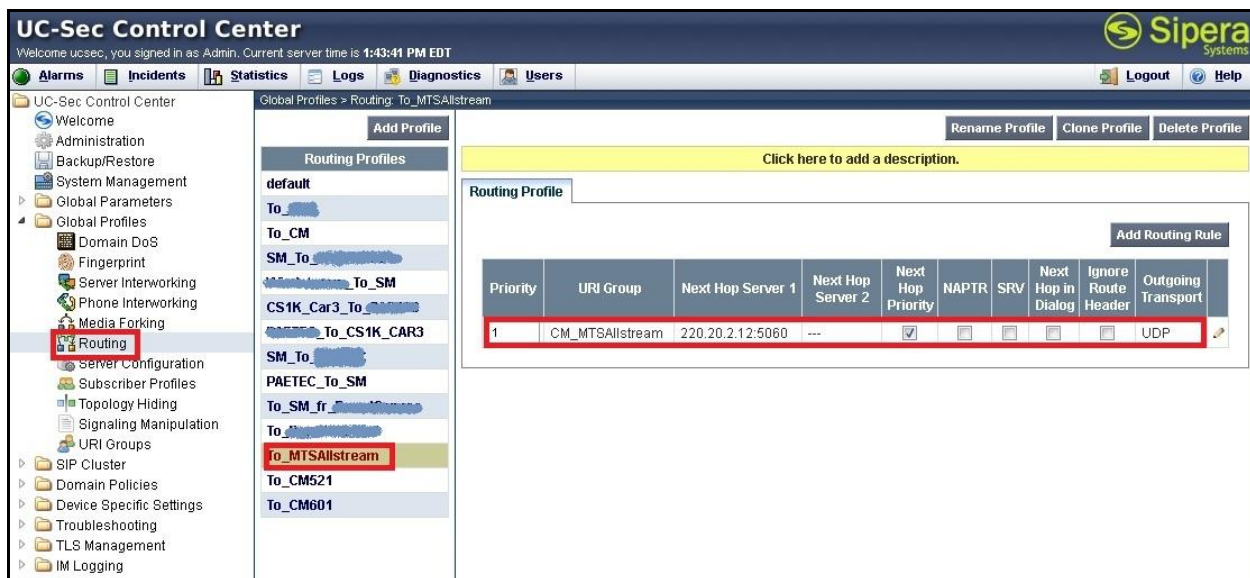
To create a **Routing Profile**, select **UC-Sec Control Center → Global Profiles → Routing**. Click on **Add Profile** (not shown).

In the compliance test, a **Routing Profile** named **To_MTSAllstream** was created to be used in conjunction with the server flow defined for Session Manager. This entry is to route the outgoing call from the enterprise to MTS Allstream.

In the opposite direction, a **Routing Profile** named **To_SM62** is created to be used in conjunction with the server flow defined for MTS Allstream. This entry is to route the incoming call from MTS Allstream to the enterprise.

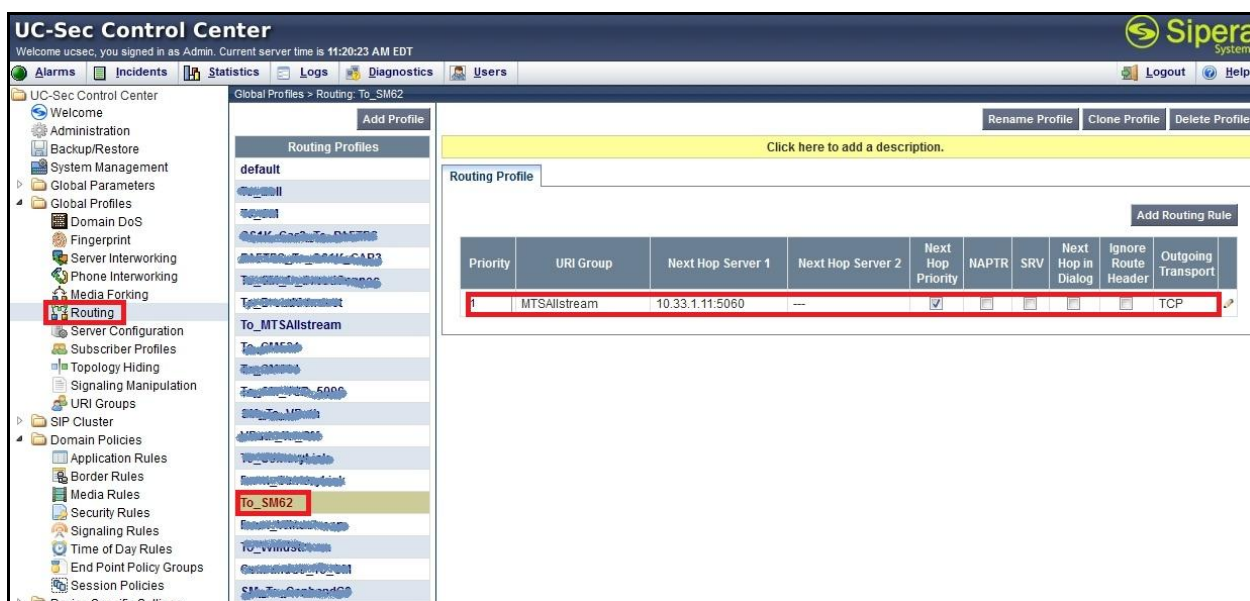
7.2.2.1 Routing Profile for MTS Allstream

The screenshot below illustrates the **UC-Sec Control Center → Global Profiles → Routing: To_MTSAllstream**. As shown in **Figure 1**, MTS Allstream SIP Trunk is connected with transportation protocol **UDP**. If there is a match in the **To** header of the **MTSAllstream** URI Group defined in **Section 7.2.1**, the call will be routed to the **Next Hop Server 1** which is the IP address of MTS Allstream SIP Trunk on port 5060.



7.2.2.2 Routing Profile for Session Manager

The routing profile **To_SM62** is defined to route calls where the **To** header matches the URI-Group **MTSAllstream**, defined in **Section 7.2.1**, to **Next Hop Server 1** which is the IP address of Session Manager, on port 5060 as a destination. As shown in **Figure 1**, SIP Trunk between Session Manager and Avaya SBCE is connected with transportation protocol **TCP**.



7.2.3. Topology Hiding

Topology Hiding is an Avaya SBCE security feature which allows changing certain key SIP message parameters to 'hide' or 'mask' how the enterprise network may appear to an unauthorized or malicious user.

To create a **Topology Hiding** profile, select **UC-Sec Control Center** → **Global Profiles** → **Topology Hiding**. Click on **Add Profile** (not shown).

In the compliance test, two Topology Hiding profiles **To_MTSAllstream** and **To_CS1K** were created.

7.2.3.1 Topology Hiding Profile for MTS Allstream

Profile **To_MTSAllstream** is defined to mask the enterprise SIP domain **avaya.com** in Request-URI and To headers to IP **220.20.2.12** (the IP address MTS Allstream uses as URI-Host portion for Request-URI and To headers to meet the SIP specification requirement of MTS Allstream); mask the enterprise SIP domain **avaya.com** in From header to IP **110.10.98.108** (Avaya SBCE public IP address); and replace Record-Route, Via headers and SDP added by CS1000 by external IP address known to MTS Allstream. It is to secure the enterprise network topology and also to meet the SIP requirement from service provider.

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

The screenshot shows the UC-Sec Control Center interface. On the left is a navigation tree with 'Topology Hiding' selected. The main area displays the configuration for the 'To_MTSAllstream' profile. A table lists the headers and their replacement values:

Header	Criteria	Replace Action	Overwrite Value
Request-Line	IP/Domain	Overwrite	220.20.2.12
Via	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
From	IP/Domain	Overwrite	110.10.98.108
To	IP/Domain	Overwrite	220.20.2.12
SDP	IP/Domain	Auto	---

Notes:

- The **Criteria** should be selected as **IP/Domain** to give the Avaya SBCE the capability to mask both domain name and IP address present in SIP URI-Host.
- The masking applied on **From** header also applies to **Referred-By** and **P-Asserted-Identity** headers.
- The masking applied on **To** header also applies to **Refer-To** header.

7.2.3.2 Topology Hiding Profile for CS1000

Profile **To_CS1K** is also needed to mask MTS Allstream URI-Host in Request-URI, From, To headers to the enterprise SIP domain **avaya.com**; replace Record-Route, Via headers and SDP added by MTS Allstream by internal IP address known to CS1000.

The screenshots below illustrate the **Topology Hiding** profile **To_CS1K**.

The screenshot shows the UC-Sec Control Center interface. On the left is a navigation tree with categories like Administration, System Management, Global Profiles, and Topology Hiding. The 'Topology Hiding' section is expanded, showing a list of profiles including 'To_CS1K', which is highlighted. The main panel displays the configuration for 'To_CS1K'. It includes a table with columns: Header, Criteria, Replace Action, and Overwrite Value. The table contains the following data:

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

Below the table is an 'Edit' button. Above the table, there are buttons for 'Rename Profile', 'Clone Profile', and 'Delete Profile', and a link to 'Click here to add a description.'

Notes:

- The **Criteria** should be **IP/Domain** to give the Avaya SBCE the capability to mask both domain name and IP address present in SIP URI-Host.
- The masking applied on **From** header also applies to **Referred-By** and **P-Asserted-Identity** headers.
- The masking applied on **To** header also applies to **Refer-To** header.

7.2.4. Server Interworking

Interworking Profile features are configured differently for Call and Trunk Servers.

To create a **Server Interworking** profile, select **UC-Sec Control Center → Global Profiles → Server Interworking**. Click on **Add Profile** (not shown).

In the compliance testing, two profiles, **MTSAllstream** and **SM**, are created for MTS Allstream and Session Manager.

7.2.4.1 Server Interworking profile for MTS Allstream

Profile **MTS Allstream** is defined to match the specification of MTS Allstream. The **General** settings are configured with following parameters while the other settings for **Timers**, **URI Manipulation**, **Header Manipulation** and **Advanced** are kept as default.

General settings:

- Hold Support = **None**. Avaya SBCE will not modify the hold/ resume signaling from CS1000 to MTS Allstream.
- 18X Handling = **None**. Avaya SBCE will not handle 18X, it will keep the 18X messages from CS1000 unchanged to MTS Allstream.
- Refer Handling = **unchecked**. Avaya SBCE will not handle Refer. It will keep the Refer message from CS1000 unchanged to MTS Allstream.
- T.38 Support = **unchecked**. MTS Allstream does not support T.38 fax in the compliance test.
- Privacy Enabled = **unchecked**. Avaya SBCE will not mask the From header with anonymous for outbound call to MTS Allstream. It depends on the CS1000 to enable/ disable privacy on individual call basis.
- DTMF Support = **None**. Avaya SBCE will send original DTMF supported by CS1000 to MTS Allstream.

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

Editing Profile: MTSAllstream

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

Next

Editing Profile: MTSAllstream

Privacy	
Privacy Enabled	<input checked="" type="checkbox"/>
User Name	<input type="text"/>
P-Asserted-Identity	<input type="checkbox"/>
P-Preferred-Identity	<input type="checkbox"/>
Privacy Header	<input type="text"/>

DTMF	
DTMF Support	<input checked="" type="radio"/> None <input type="radio"/> SIP NOTIFY <input type="radio"/> SIP INFO

Back Finish

7.2.4.2 Server Interworking profile for Session Manager

Profile **CS1K** is defined to match the specification of CS1000. The **General** settings are configured with the following parameters while the other settings for **Timers**, **URI Manipulation**, **Header Manipulation** and **Advanced** are kept as default.

General settings:

- Hold Support = **RFC2543**. CS1000 supports hold/ resume as per RFC2543.
- 18X Handling = **None**. Avaya SBCE will not handle 18X, it will keep the 18X messages from MTS Allstream to CS1000 unchanged.
- Refer Handling = **unchecked**. Avaya SBCE will not handle Refer. CS1000 does not use Refer to redirect the call over SIP Trunk.
- T.38 Support = **unchecked**. MTS Allstream does not support T.38 fax in the compliance test.
- Privacy Enabled = **unchecked**. Avaya SBCE will not mask the **From** header with anonymous for inbound call from MTS Allstream. It depends on the MTS Allstream to enable/ disable privacy on individual call basis.
- DTMF Support = **None**. Avaya SBCE will send original DTMF supported by MTS Allstream to CS1000.

The screenshots below illustrate the **Server Interworking** profile **CS1K**.

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

Next

Privacy	
Privacy Enabled	<input checked="" type="checkbox"/>
User Name	<input type="text"/>
P-Asserted-Identity	<input type="checkbox"/>
P-Preferred-Identity	<input type="checkbox"/>
Privacy Header	<input type="text"/>

DTMF	
DTMF Support	<input checked="" type="radio"/> None <input type="radio"/> SIP NOTIFY <input type="radio"/> SIP INFO

Back Finish

7.2.5. Signaling Manipulation

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

The SigMa scripting language is designed to express any of the SIP header manipulation operations to be done by the Avaya SBCE. Using this language, a script can be written and tied to a given **Server Configuration** which is configured in the next steps through the EMS GUI. The Avaya SBCE appliance then interprets this script at the given entry point or “hook point”.

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

To create a **Signaling Manipulation** script, select **UC-Sec Control Center → Global Profiles → Signaling Manipulation**. Click on **Add Script** (not shown). Separate SigMa script is created for call server and trunk server.

7.2.5.1 SigMa script for MTS Allstream

In the compliance test, a SigMa script named **MTSAllstream_To_CS1K** was created for Server Configuration MTS Allstream and described detail as following:

```

within session "ALL"
{
act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
{
%HEADERS["P-Asserted-Identity"][1].URI.HOST="110.10.98.108";
%HEADERS["Diversion"][1].URI.HOST="110.10.98.108";
remove(%HEADERS["History-Info"][1]);
remove(%HEADERS["P-Location"][1]);
remove(%HEADERS["Remote-Party-ID"][1]);
}

act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
{
%HEADERS["Request_Line"][1].regex_replace("sip:110.10.98.108","sip:avaya.com");
%HEADERS["To"][1].regex_replace("sip:110.10.98.108","sip:ping@110.10.98.108");
%HEADERS["From"][1].regex_replace("sip:220.20.2.12","sip:ping@220.20.2.12");
}
}

```

The statement **act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"** is to specify that the script will take effect on all types of SIP messages for outbound calls to MTS Allstream and the manipulation will be done after routing. The manipulation will be according to the rules contained in this statement. The **Topology-Hiding** profile **MTSAllstream** could mask URI-Host of P-Asserted-Identity and Diversion headers successfully in “request” SIP message. However, as a limitation, the P-Asserted-Identity and Diversion headers in “response” SIP message will still have the private enterprise SIP domain. Therefore, two SigMa rules are used to correct the URI-Host of P-Asserted-Identity and Diversion headers. Three SigMa rules are also added to remove History-Info, P-Location and Remote-Party-ID headers because they are not required by MTS Allstream.

The statement **act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"** is to specify that the script will take effect on all types of SIP messages for inbound calls from MTS Allstream and the manipulation will be done before routing. The manipulation will be according to the rules contained in this statement. The purpose of the SigMa script **MTAllstream** is to normalize the OPTIONS received from MTS Allstream. The header **From** and **To** need to be modified to have URI-User@URI-Host format, otherwise the OPTIONS will fail to match the URI-Group defined in **Section 7.2.1**. If unmatching happens, the **Routing Profile** and **Server Flow** (discussed in **Section 7.4.4**) will not be applied to the call, and will result in dropped packets. With the SigMa script in place, the OPTIONS heartbeat from MTS Allstream will be forwarded to Session Manager. The 200OK response from Session Manager will confirm the status of SIP Trunk as active. If there is no response, MTS Allstream will change the status of SIP Trunk to “out of service”.

7.2.5.2 SigMa script for Session Manager

In the compliance test, a SigMa script named **SM62_4_MTSAllstream** is created for Server Configuration Session Manager and described in detail as follows:

```
within session "ALL"
{
  act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"
  {
    %HEADERS["Request_Line"][1].regex_replace("sip:110.10.97.189","sip:220.20.2.12");
    %HEADERS["From"][1].regex_replace("sip:10.33.1.11","sip:ping@avaya.com");
    %HEADERS["To"][1].regex_replace("sip:110.10.97.189","sip:ping@avaya.com");
  }
}
```

The statement **act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK"** is to specify that the script will take effect on all types of SIP messages for outbound calls from Session Manager and the manipulation will be done before routing. The manipulation will be according to the rules contained in this statement. The purpose of the SigMa script **SM62_4_MTSAllstream** is to normalize the OPTIONS received from Session Manager. The header **From** and **To** need to be modified to have URI-User@URI-Host format, otherwise the OPTIONS will fail to match the URI-Group defined in **Section 7.2.1**. If unmatching happens, the **Routing Profile** and **Server Flow** (discussed in **Section 7.4.4**) will not be applied to the call, and will result in dropped packets. With the SigMa script in place, the OPTIONS heartbeat from Session Manager will be forwarded to MTS Allstream. The 200OK response from MTS Allstream will confirm the status of SIP Trunk as active. If there is no response, Session Manager will change the status of SIP Trunk to “out of service”.

7.2.6. Server Configuration

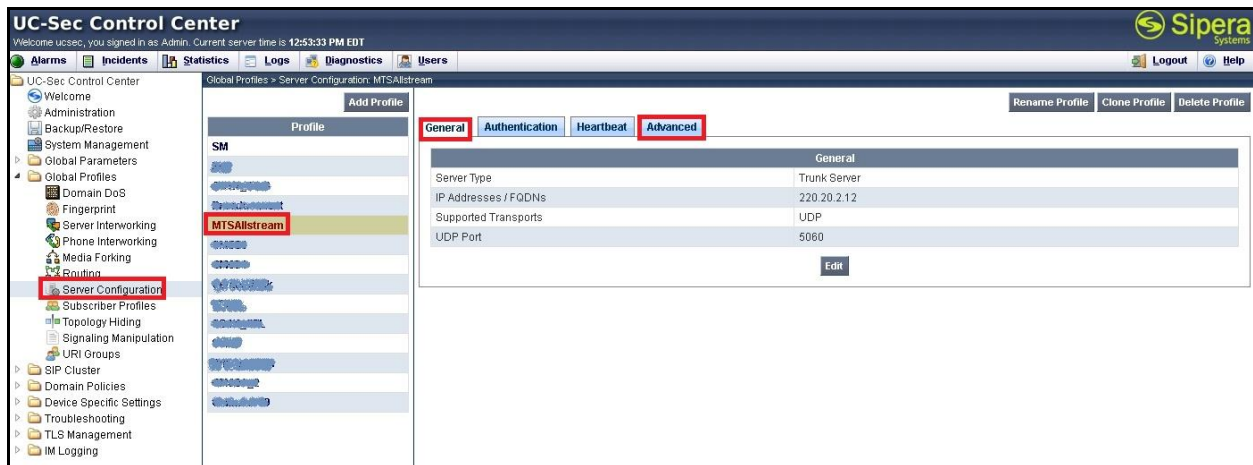
The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. These tabs are used to configure and manage various SIP Call Server specific parameters such as TCP and UDP port assignments, heartbeat signaling parameters, DoS security statistics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

To create a Server Configuration entry, select **UC-Sec Control Center → Global Profiles → Server Configuration**. Click on **Add Profile** (not shown).

In the compliance test, two separate Server Configurations were created, server entry **MTSAllstream** for MTS Allstream and server entry **SM62** for Session Manager.

7.2.6.1 Server Configuration for MTS Allstream

The **Server Configuration** named **MTSAllstream** is added for MTS Allstream, it will be discussed in detail below. **General** and **Advanced** tabs are provisioned but no configuration is done for **Authentication** tab as MTS Allstream does not implement Authentication on a SIP Trunk. The **Heartbeat** tab is kept as disabled as default to allow the Avaya SBCE to forward the OPTIONS heartbeat from Session Manager to MTS Allstream to query the status of the SIP Trunk.



In the **General** tab, set **Server Type** for MTS Allstream to **Trunk Server**. In the compliance test, MTS Allstream supports UDP and listens on port 5060.

The screenshot shows a dialog box titled 'Edit Server Configuration Profile - General'. It contains the following fields and controls:

- Server Type:** A dropdown menu set to 'Trunk Server'.
- IP Addresses / Supported FQDNs:** A text area containing '220.20.2.12'.
- Supported Transports:** Three checkboxes: 'TCP' (unchecked), 'UDP' (checked), and 'TLS' (unchecked).
- TCP Port:** A disabled text field.
- UDP Port:** A text field containing '5060'.
- TLS Port:** A disabled text field.
- Finish:** A button at the bottom.

Under **Advanced** tab, for **Interworking Profile** drop-down list, select **MTSAllstream** as defined in **Section 7.2.4**, and for **Signaling Manipulation Script** drop-down list, select **MTSAllstream_To_CS1K** as defined in **Section 7.2.5.1**. These configurations are applied to the specific SIP profile and SigMa rules for the traffic from MTS Allstream. The other settings are kept as default.

In the **General** tab, specify **Server Type** as **Call Server**. In the compliance test, the link between Avaya SBCE and Session Manager was TCP and Session Manager listens on port 5060.

Edit Server Configuration Profile - General

Server Type	Call Server
IP Addresses / Supported FQDNs Comma seperated list	10.33.1.11
Supported Transports	<input checked="" type="checkbox"/> TCP <input type="checkbox"/> UDP <input type="checkbox"/> TLS
TCP Port	5060
UDP Port	
TLS Port	
Finish	

Under **Advanced** tab, for **Interworking Profile** drop-down list, select **CS1K** as defined in **Section 7.2.4** and for **Signaling Manipulation Script** drop down list select **SM62_4_MTSAllstream** as defined in **Section 7.2.5.2**. The other settings are kept as default.

Edit Server Configuration Profile - Advanced

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	CS1K
Signaling Manipulation Script	SM62_4_MTSAllstream
TCP Connection Type	<input checked="" type="radio"/> SUBID <input type="radio"/> PORTID <input type="radio"/> MAPPING
Finish	

7.3. Domain Policies

The **Domain Policies** feature configures various rule sets (policies) to control unified communications based upon criteria of communication sessions originating from or terminating at the enterprise. These criteria can be used to trigger policies which, in turn, activate various security features of the UC-Sec security device to aggregate, monitor, control and normalize call flow. There are default policies available for use, or a custom domain policy can be created.

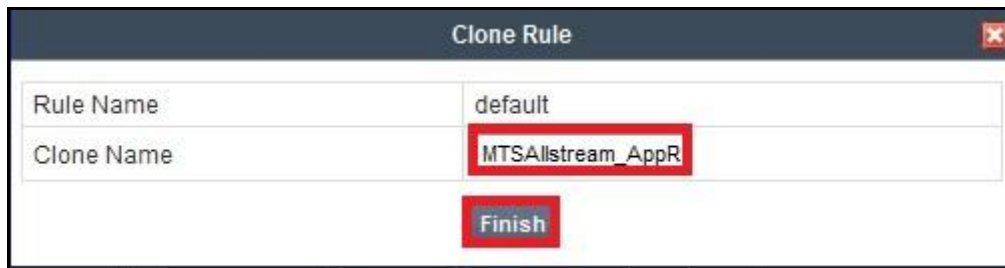
7.3.1. Application Rules

Application Rules define which types of SIP-based Unified Communications (UC) applications the UC-Sec security device will protect: voice, video, and/or Instant Messaging (IM). In addition, it is possible to configure the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion.

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

To clone an application rule, navigate to **UC-Sec Control Center → Domain Policies → Application Rules**. With the default rule chosen, click on **Clone Rule** (not shown).

Enter a rule with a descriptive name **MTSAllstream_AR** and click **Finish**.



Clone Rule	
Rule Name	default
Clone Name	MTSAllstream_AppR
Finish	

Click **Edit** button (not shown) to modify the rule. Set the **Maximum Concurrent Sessions** and **Maximum Session Per Endpoint** for the **Voice** application to a value high enough for the amount of traffic the network is able to process. The following screen shows the modified **Application Rule** with the **Maximum Concurrent Sessions** and **Maximum Session Per Endpoint** set to 1000. In the compliance test, CS1000 was programmed to control the concurrent sessions by setting the number of Virtual Trunks (**Section 5.5.7**) to the allotted number. Therefore, the values in the **Application Rule** named **MTSAllstream_AR** are set high enough to be considered non-blocking.

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

Miscellaneous

CDR Support

☒ None
☐ CDR w/ RTP
☐ CDR w/o RTP

IM Logging
☐

RTCP Keep-Alive
☐

Finish

7.3.2. Media Rules

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

A custom **Media Rule** is created to set the **Quality of Service** and **Media Anomaly Detection**. The sample configuration shows **Media Rule MTSAllstream_MediaR** used for both the enterprise and MTS Allstream.

To create **Media Rule**, navigate to **UC-Sec Control Center → Domain Policies → Media Rules**. With **default-low-med** selected, click **Clone Rule** (not shown).

Enter a **Media Rule** with a descriptive name **MTSAllstream_MediaR** and click **Finish**.

Rule Name

default-low-med

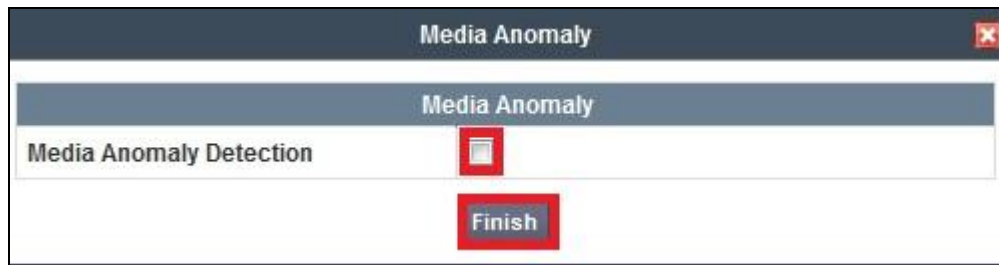
Clone Name

MTSAllstream_Media

Finish

When the RTP of a call is changed on the fly, Avaya SBCE will interpret this as an anomaly and an alert will be created in the **Incidents Log**. Disabling **Media Anomaly Detection** prevents the **RTP Injection Attack** alerts from being created in the log during an audio shuffle.

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



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

To modify the rule, select the **Media Silencing** tab and click **Edit**, uncheck **Media Silencing** and click **Finish**.



Select the **Media QoS** tab and click **Edit** to configure the proper Quality of Service (QoS). Avaya SBCE can be configured to mark the Differentiated Services Code Point (DSCP) in the IP Header with specific values to support Quality of Services policies for the media. The following screen shows the QoS values used for the compliance test.

Media QoS Reporting			
RTCP Enabled	<input type="checkbox"/>		

Media QoS Marking			
Enabled	<input checked="" type="checkbox"/>		
<input type="radio"/> ToS			
Audio Precedence	Routine		000
Audio ToS	Minimize Delay		1000
Video Precedence	Routine		000
Video ToS	Minimize Delay		1000
<input checked="" type="radio"/> DSCP			
Audio	EF		101110
Video	EF		101110

Finish

7.3.3. Signaling Rules

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

To clone a signaling rule, navigate to **UC-Sec Control Center → Domain Policies → Signaling Rules**. With the **default** rule chosen, click on **Clone Rule** (not shown).

In the compliance test, two **Signaling Rules** were created for MTS Allstream and Session Manager.

7.3.3.1 Signaling Rule for MTS Allstream

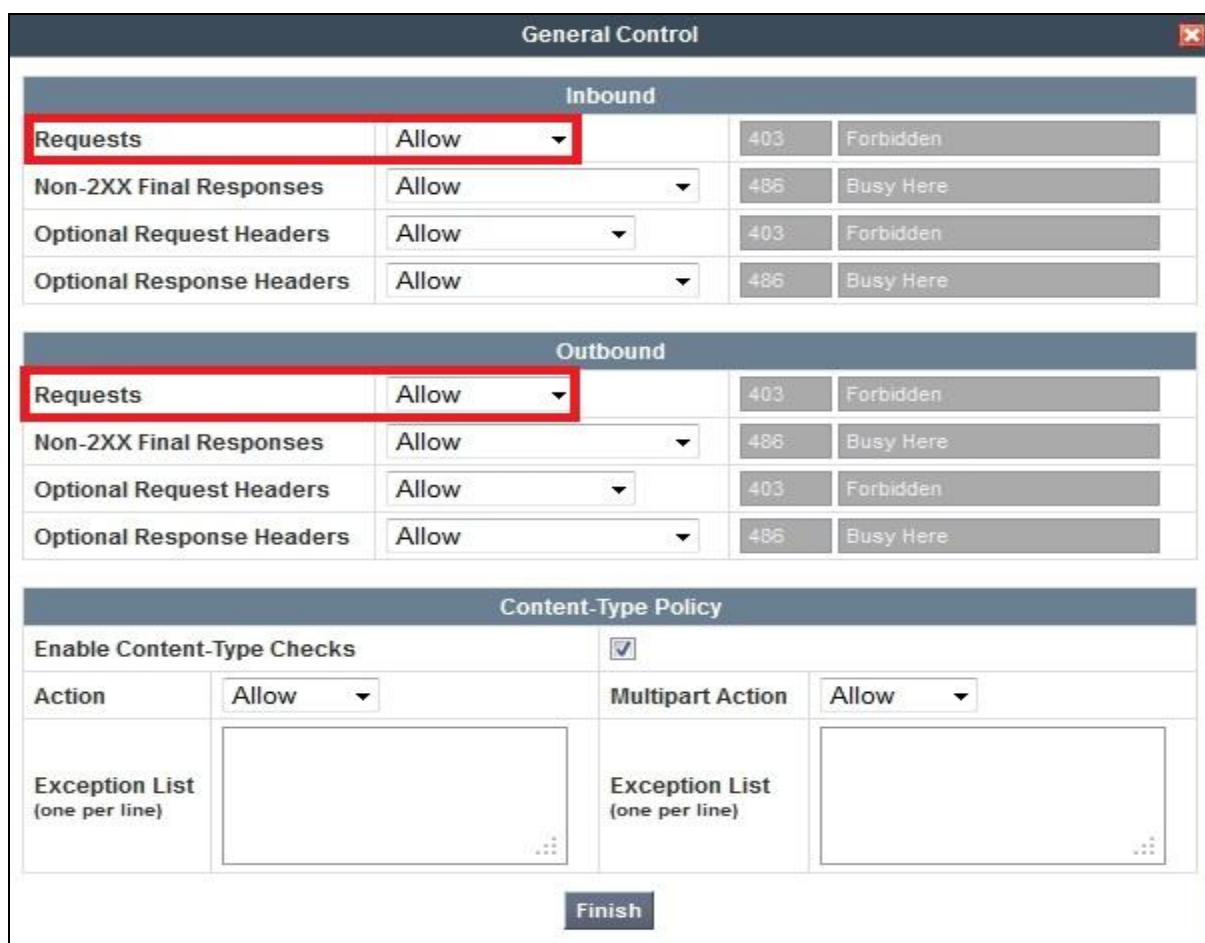
Clone a **Signaling Rule** with a descriptive name **MTSAllstream_SigR** and click **Finish**.



Clone Rule	
Rule Name	default
Clone Name	MTSAllstream_SigR
Finish	

The **MTSAllstream_SigR** is configured to allow MTS Allstream to accept inbound and outbound call requests. It also blocks Accept-Language, Alert-Info, P-Chanrging-Vector and x-nt-e164-clid headers from CS1000 because these headers are not required by MTS Allstream.

Being cloned from the **Signaling Rule default**, the **MTSAllstream_SigR** will block all requests with 403 Forbidden. To start accepting calls, go to **General** tab, click on **Edit**. Then change **Inbound** and **Outbound Request** to **Allow** as shown in following screenshot.



General Control			
Inbound			
Requests	Allow	403	Forbidden
Non-2XX Final Responses	Allow	486	Busy Here
Optional Request Headers	Allow	403	Forbidden
Optional Response Headers	Allow	486	Busy Here
Outbound			
Requests	Allow	403	Forbidden
Non-2XX Final Responses	Allow	486	Busy Here
Optional Request Headers	Allow	403	Forbidden
Optional Response Headers	Allow	486	Busy Here
Content-Type Policy			
Enable Content-Type Checks		<input checked="" type="checkbox"/>	
Action	Allow	Multipart Action	Allow
Exception List (one per line)		Exception List (one per line)	
Finish			

Request Headers setting is to allow or block a header in particular direction for request method. The buttons “**Add In Header Control**” and “**Add Out Header Control**” are used to define the inbound and outbound Request header rules. The signaling rule **MTSAllstream_SigR** will be assigned to Server Configure for MTS Allstream as shown in **Section 7.2.6.1**.

The following screenshot shows three rules added to block the Accept-Language, Alert-Info, P-Charging-Vector and nt-e164-clid headers.

- **Header Name:** Select the header to be manipulated.
- **Method Name:** Select **INVITE** in an outbound call request.
- **Header Criteria:** Click on **Forbidden** to block the header.
- **Action:** Select **Remove header** to delete the header.

The screenshot shows the UC-Sec Control Center interface. The left sidebar contains a tree view with categories like Alarms, Incidents, Statistics, Logs, Diagnostics, and Users. Under 'Domain Policies', 'Signaling Rules' is expanded, and 'MTSAllstream_SigR' is selected. The main panel shows the configuration for this rule. The 'Request Headers' tab is active, displaying a table with the following data:

Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction
1	Accept-Language	INVITE	Forbidden	Remove Header	No	OUT
2	Alert-Info	INVITE	Forbidden	Remove Header	No	OUT
3	P-Charging-Vector	INVITE	Forbidden	Remove Header	Yes	OUT
4	x-nt-e164-clid	INVITE	Forbidden	Remove Header	Yes	OUT

Note: Pre-defined list does not have P-Charging-Vector and nt-e164-clid headers, but the Avaya SBCE provides an option to define these proprietary headers.

Response Headers setting is to allow or block a header in particular direction for response method. The buttons “**Add In Header Control**” and “**Add Out Header Control**” are used to define inbound and outbound Response Header rules. The Signaling Rule **MTSAllstream_SigR** will be assigned to Server Configure for MTS Allstream as shown in **Section 7.2.6.1**.

The following Rules screenshots show three rules added to block the Accept-Language, Alert-Info, P-Charging-Vector and nt-e164-clid headers:

- **Header Name:** Select the header to be manipulated.
- **Method Name:** Select INVITE for an inbound call request.
- **Header Criteria:** Click on **Forbidden** to block the header.
- **Action:** Select **Remove header** to delete the header.

UC-Sec Control Center
Welcome ucsec, you signed in as Admin. Current server time is 1:04:41 PM EDT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

Domain Policies > Signaling Rules: MTSAllstream_SigR

Filter By Device... [v] [Rename Rule] [Clone Rule] [Delete Rule]

Click here to add a description.

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

Add In Header Control Add Out Header Control

Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction	
1	Accept-Language	1XX	INVITE	Forbidden	Remove Header	No	OUT	✖
2	Alert-Info	1XX	INVITE	Forbidden	Remove Header	No	OUT	✖
3	P-Charging-Vector	1XX	INVITE	Forbidden	Remove Header	Yes	OUT	✖
4	x-nt-e164-clid	1XX	INVITE	Forbidden	Remove Header	Yes	OUT	✖

Note: Pre-defined list does not have P-Charging-Vector and nt-e164-clid headers, but the Avaya SBCE provides an option to define these proprietary headers.

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

Signaling QoS

Enabled ☒

☐ ToS

Precedence

ToS

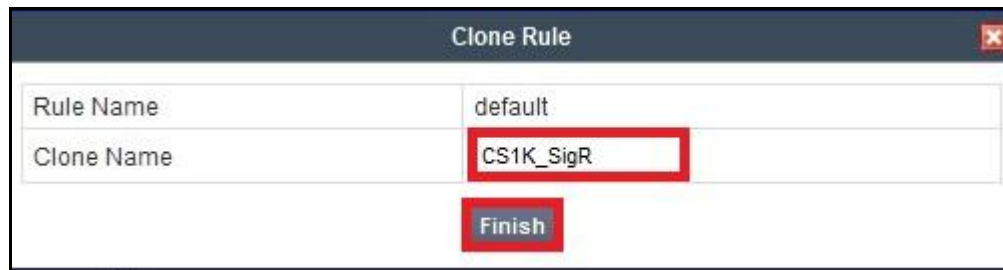
☒ **DSCP**

Value

Finish

7.3.3.2 Signaling Rule for Session Manager

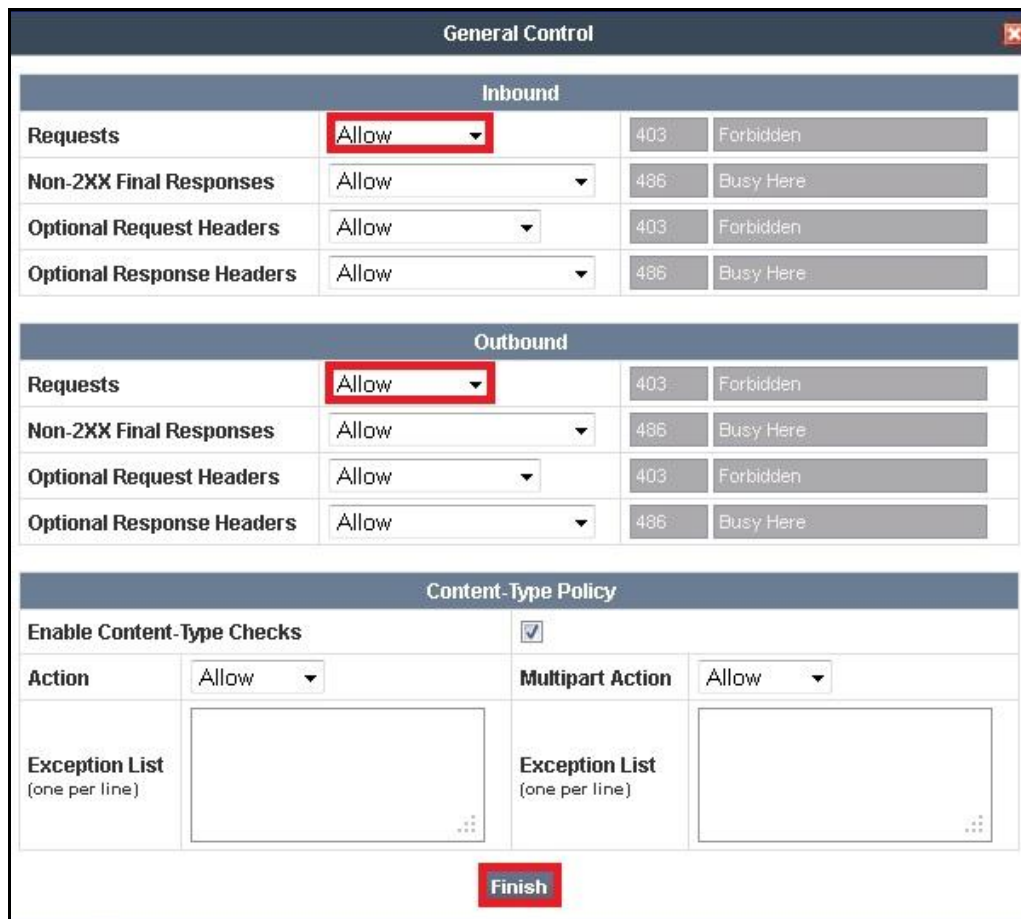
Clone a **Signaling Rule** with a descriptive name **CS1K_SigR** and click **Finish**.



Clone Rule	
Rule Name	default
Clone Name	CS1K_SigR
Finish	

This **CS1K_SigR** is configured to allow CS1000 to accept inbound and outbound call requests.

Being cloned from the **Signaling Rule default**, the **CS1K_SigR** will block all requests with 403 Forbidden. To start accepting calls, select **CS1K_SigR** then go to **General** tab, click on **Edit** (not shown). Then change **Inbound-Requests** and **Outbound-Requests** to **Allow** as shown in following screenshot and click **Finish**.



General Control			
Inbound			
Requests	Allow	403	Forbidden
Non-2XX Final Responses	Allow	486	Busy Here
Optional Request Headers	Allow	403	Forbidden
Optional Response Headers	Allow	486	Busy Here
Outbound			
Requests	Allow	403	Forbidden
Non-2XX Final Responses	Allow	486	Busy Here
Optional Request Headers	Allow	403	Forbidden
Optional Response Headers	Allow	486	Busy Here
Content-Type Policy			
Enable Content-Type Checks		<input checked="" type="checkbox"/>	
Action	Allow	Multipart Action	Allow
Exception List (one per line)		Exception List (one per line)	
Finish			

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

7.3.4. Endpoint Policy Groups

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

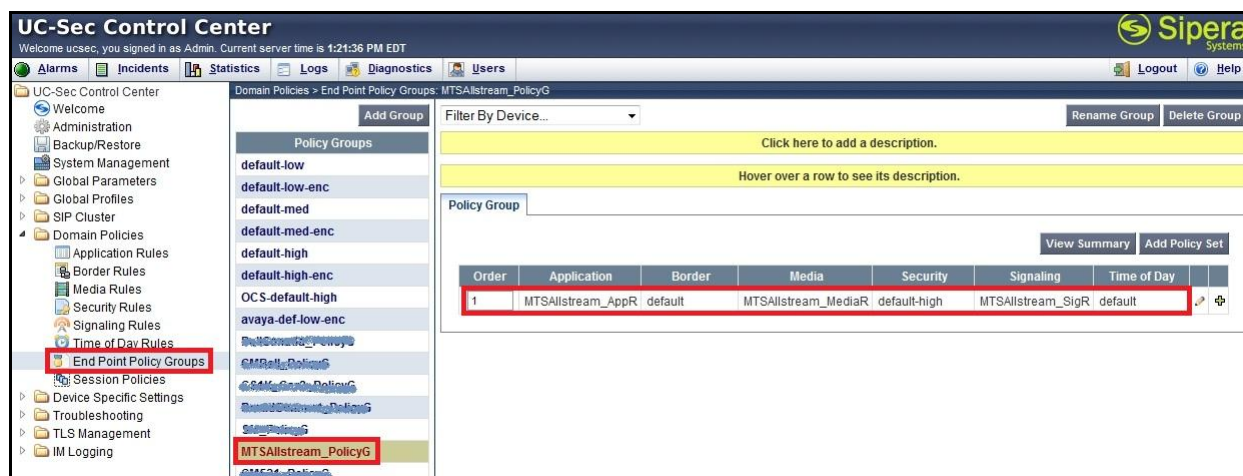
Endpoint Policy Groups are created for the Session Manager and the MTS Allstream.

To create a new policy group, navigate to **UC-Sec Control Center → Domain Policies → Endpoint Policy Groups** and click on **Add Group** (not shown).

7.3.4.1 Endpoint Policy Group for MTS Allstream

The following screen shows **MTSAllstream_PolicyG** created for MTS Allstream:

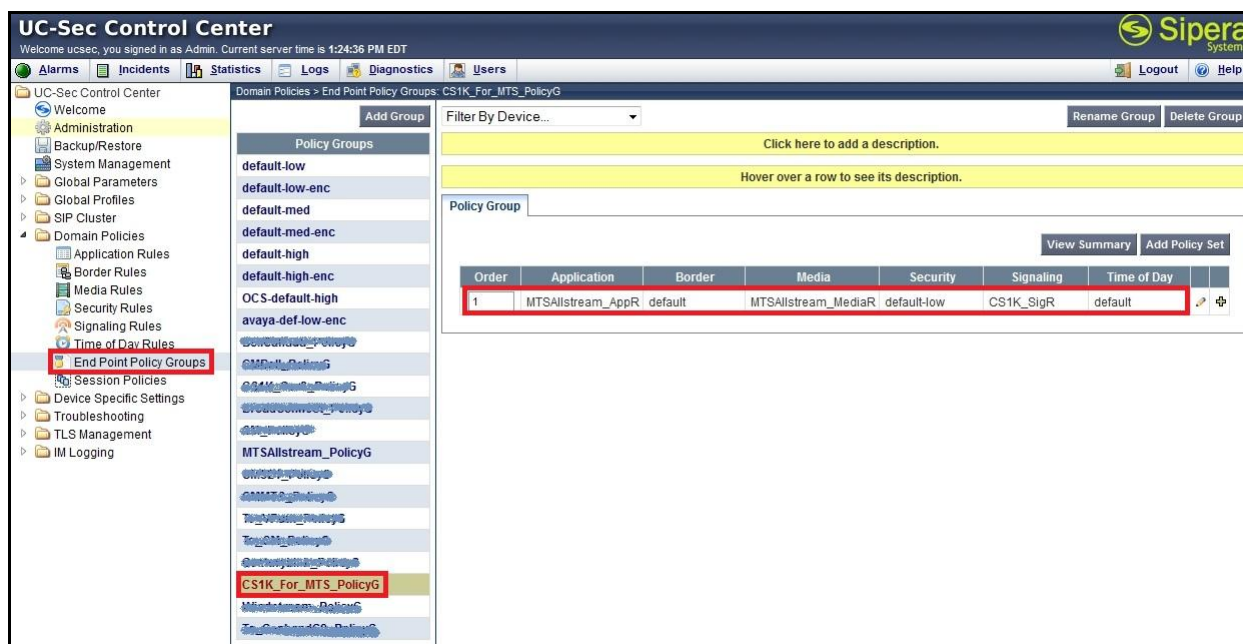
- Set **Application** and **Media** rules created in **Section 7.3.1** and **Section 7.3.2**.
- Set **Signaling** rule **MTSAllstream_SigR** created in **Section 7.3.3.1**.
- Set **Border** and **Time of Day** rules to **default**.
- Set **Security** rule to **default-high**.



7.3.4.2 Endpoint Policy Group for Session Manager

The following screen shows CS1K_For_MTS_PolicyG created for Session Manager:

- Set **Application** and **Media** rules created in Section 7.3.1 and Section 7.3.2.
- Set **Signaling** rule CS1K_SigR created in Section 7.3.3.2.
- Set the **Border** and **Time of Day** rules to **default**.
- Set the **Security** rule to **default-low**.



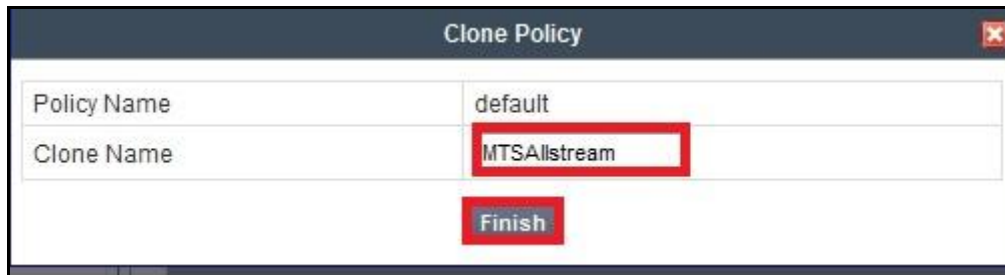
7.3.5. Session Policy

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

In the compliance test, the **Session Policy** named **MTSAllstream** was created to match the codec configuration on MTS Allstream. The policy also allows Avaya SBCE to anchor media in off-net call transfer scenarios.

To clone a **Session Policy**, navigate to **UC-Sec Control Center → Domain Policies → Session Policies**. With the **default** rule chosen, click on **Clone Rule** (not shown). It is applied to both CS1000 and MTS Allstream.

Enter a descriptive name **MTSAllstream** for the new policy and click **Finish**.



Clone Policy	
Policy Name	default
Clone Name	MTSAllstream
Finish	

MTS Allstream supports voice codec G.729 and G.711MU in prioritized order with payload 101 for RFC2833/ DTMF. To define **Codec Prioritization** for Audio Codec, select the profile **MTSAllstream** created above, click on **Edit** (not shown). Select **Preferred Codec #1** as G.711MU, **Preferred Codec #2** as G.729 and **Preferred Codec #3** as Dynamic (101) for RFC2833/ DTMF. Check **Allow Preferred Codecs Only** to prevent the unsupported codec from being sent to both ends.

Notes:

- The T.38 fax is not yet supported by MTS Allstream SIP Trunking Service.
- This **Session Policy** prioritizes voice codec G.711MU to establish the voice call. It is mandatory for a G.711MU fax call to be successful because both CS1000 and MTS Allstream cannot switch the voice call using different codec to G.711MU for fax.

Codec Prioritization	
Audio Codec	
Codec Prioritization	<input checked="" type="checkbox"/>
Allow Preferred Codecs Only	<input checked="" type="checkbox"/>
Preferred Codec #1	PCMU (0)
Preferred Codec #2	G729 (18)
Preferred Codec #3	Dynamic (101)
Preferred Codec #4	None
Preferred Codec #5	None
Video Codec	
Codec Prioritization	<input type="checkbox"/>
Allow Preferred Codecs Only	<input type="checkbox"/>
Preferred Codec #1	CelB (25)
Preferred Codec #2	None
Preferred Codec #3	None
Preferred Codec #4	None
Preferred Codec #5	None
Finish	

To enable **Media Anchoring** on Avaya SBCE, select Session Policy **MTSAllstream** created above then select tab **Media**, click **Edit** (not shown). Check on **Media Anchoring**.

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

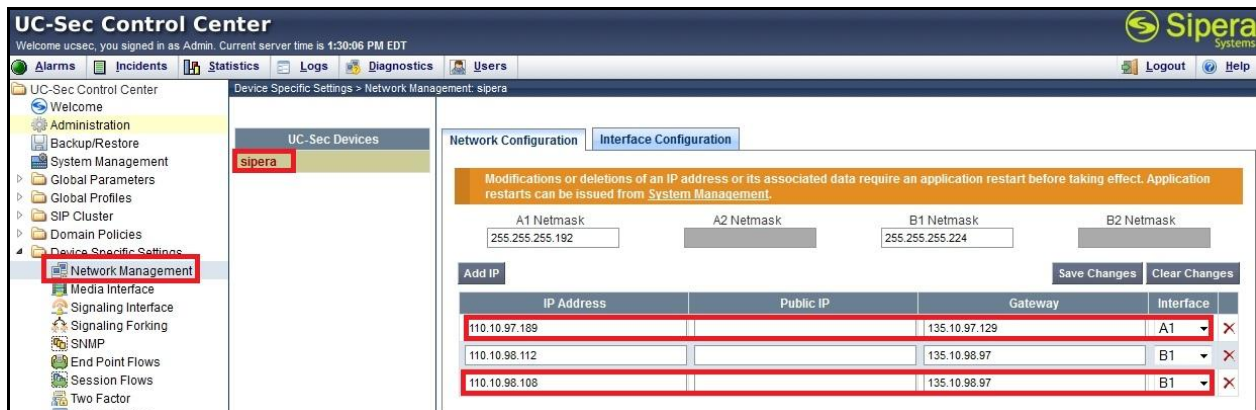
7.4. Device Specific Settings

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

7.4.1. Network Management

The **Network Management** screen is where the network interface settings are configured and enabled. During the installation process of Avaya SBCE, certain network-specific information is defined such as device IP address (es), public IP address (es), netmask, gateway, etc. to interface the device to the network. This information populates the various **Network Management** tab displays, which can be edited as needed to optimize device performance and network efficiency.

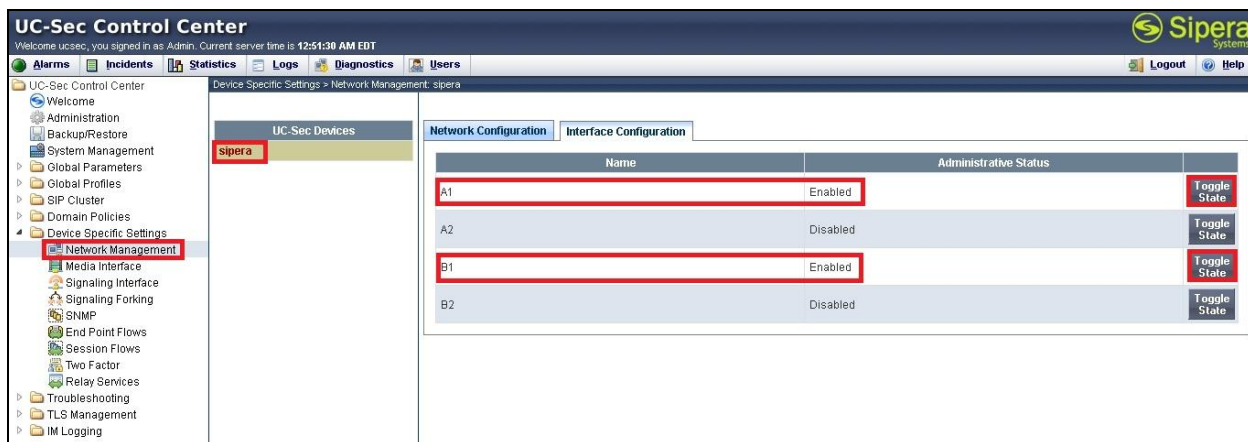
Navigate to **UC-Sec Control Center → Device Specific Settings → Network Management** and under **Network Configuration** tab verify the IP addresses assigned to the interfaces and that the interfaces are enabled. The following screen shows the private interface is assigned to **A1** and the public interface is assigned to **B1**.



The screenshot shows the UC-Sec Control Center interface. The left sidebar has a tree view with 'Network Management' selected. The main area is titled 'Device Specific Settings > Network Management: sipera'. It has two tabs: 'Network Configuration' and 'Interface Configuration'. The 'Interface Configuration' tab is active, showing a table of IP addresses and their assigned interfaces. The table has columns for IP Address, Public IP, Gateway, and Interface. The first row shows IP 110.10.97.189 assigned to interface A1. The second row shows IP 110.10.98.112 assigned to interface B1. The third row shows IP 110.10.98.108 assigned to interface B1. There are 'Save Changes' and 'Clear Changes' buttons at the top right of the table.

IP Address	Public IP	Gateway	Interface
110.10.97.189		135.10.97.129	A1
110.10.98.112		135.10.98.97	B1
110.10.98.108		135.10.98.97	B1

Enable the interfaces used to connect to the inside and outside networks on the **Interface Configuration** tab. The following screen shows interface **A1** and **B1** are **Enabled**. To enable an interface click it's **Toggle State** button.



7.4.2. Media Interface

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

To create a new **Media Interface**, navigate to **UC-Sec Control Center → Device Specific Settings → Media Interface** and click **Add Media Interface** (not shown).

Media Interfaces are created for both the inside and outside interfaces. The following screen shows the **Media Interfaces** were created in the compliance test.

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



7.4.3. Signaling Interface

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

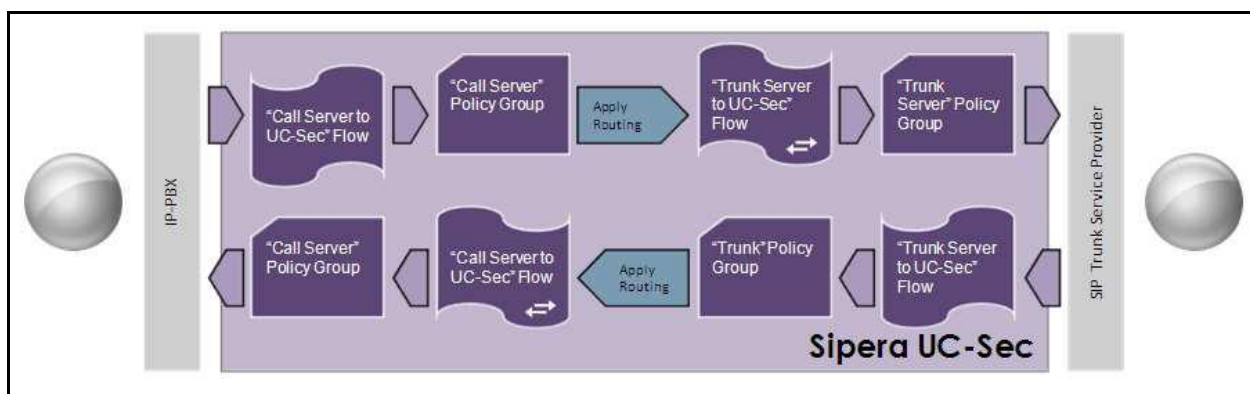
To create a new **Signaling Interface**, navigate to **UC-Sec Control Center → Device Specific Settings → Signaling Interface** and click **Add Signaling Interface** (not shown).

Signaling Interface is created for both inside and outside interfaces. The following screen shows the **Signaling Interfaces** were created in the compliance test with TCP/5060 and UDP/5060 used respectively for the inside and outside IP interface.

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
InsideSIP	110.10.97.189	5060	---	---	None	✖
OutsideSIP_SBCE	110.10.98.112	---	5060	---	None	✖
OutsideSIP	110.10.98.108	---	5060	---	None	✖
InsideSIP_TCP_5080	110.10.97.189	5080	---	---	None	✖
InsideSIP_TCP_5090	110.10.97.189	5090	---	---	None	✖

7.4.4. End Point Flows - Server Flow

When a packet is received by UC-Sec, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow. The following screen illustrates the flow through Avaya SBCE to secure a SIP Trunk call.

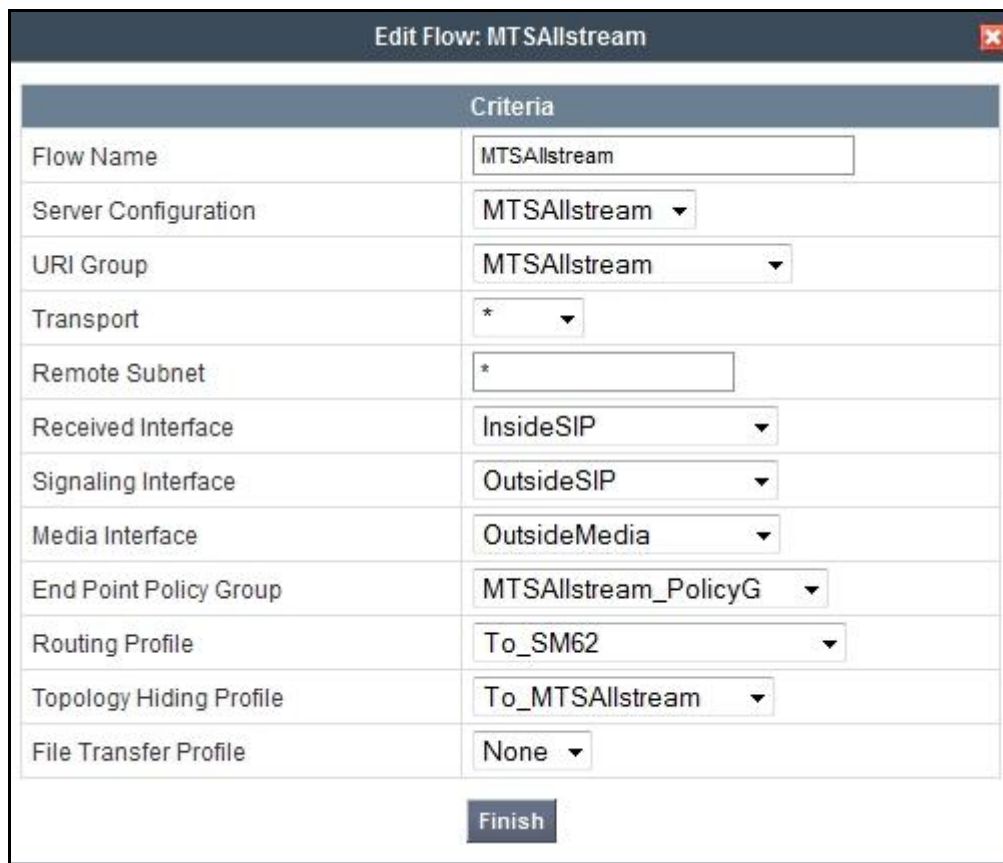


In the compliance test, separate Server Flows were created for MTS Allstream and Session Manager. To create a Server Flow, navigate to **UC-Sec Control Center → Device Specific Settings → End Point Flows**. Select the Server Flows tab and click **Add Flow** (not shown). In the new window that appears, enter the following values. The other fields are kept default.

- **Flow Name:** Enter a descriptive name
- **Server Configuration:** Select a Server Configuration created in **Section 7.2.6** to assign to the Flow
- **URI Group:** Select the URI Group created in **Section 7.2.1** to assign to the Flow
- **Received Interface:** Select the Signaling Interface created in **Section 7.4.3** the Server Configuration is allowed to receive SIP messages from

- **Signaling Interface:** Select the Signaling Interface created in **Section 7.4.3** used to communicate with the Server Configuration
- **Media Interface:** Select the Media Interface created in **Section 7.4.2** used to communicate with the Server Configuration
- **End Point Policy Group:** Select the End Point Policy Group created in **Section 7.3.4** assigned to the Server Configuration
- **Routing Profile:** Select the Routing Profile created in **Section 7.2.2** the Server Configuration will use to route SIP messages to
- **Topology Hiding Profile:** Select the Topology-Hiding profile created in **Section 7.2.3** to apply toward the Server Configuration
- Click **Finish**

The following screen shows the Server **Flow Name (MTS Allstream)** configured for MTS Allstream.



Criteria	
Flow Name	MTSAllstream
Server Configuration	MTSAllstream ▼
URI Group	MTSAllstream ▼
Transport	* ▼
Remote Subnet	*
Received Interface	InsideSIP ▼
Signaling Interface	OutsideSIP ▼
Media Interface	OutsideMedia ▼
End Point Policy Group	MTSAllstream_PolicyG ▼
Routing Profile	To_SM62 ▼
Topology Hiding Profile	To_MTSAllstream ▼
File Transfer Profile	None ▼

Finish

The following screen shows the Server **Flow Name (SM62_4_MTSAllstream)** configured for Session Manager.

Criteria	
Flow Name	SM62_For_MTSAllstream
Server Configuration	SM62
URI Group	MTSAllstream
Transport	*
Remote Subnet	*
Received Interface	OutsideSIP
Signaling Interface	InsideSIP
Media Interface	InsideMedia
End Point Policy Group	CS1K_For_MTS_PolicyG
Routing Profile	To_MTSAllstream
Topology Hiding Profile	To_CS1K
File Transfer Profile	None

Finish

7.4.5. Session Flows

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

To create a session flow, navigate to **UC-Sec Control Center → Device Specific Settings → Session Flows**. Click **Add Flow** (not shown).

A common Session Flow is created for both Session Manager and the MTS Allstream. In the new window that appears, enter the following values. Use default values for the remaining fields:

- **Flow Name:** Enter a descriptive name
- **URI Group #1:** Select the URI Group created in **Section 7.2.1** to assign to the Session Flow as the source URI Group
- **URI Group #2:** Select the URI Group created in **Section 7.2.1** to assign to the Session Flow as the destination URI Group
- **Session Policy:** Select the session policy created in **Section 7.3.5** to assign to the Session Flow

- Click **Finish**

Note: A unique **URI Group** is used for source and destination, since it contains multiple URIs defined for the source as well as for the destination.

The following screen shows the **Session Flow** named **MTSAllstream** is created.

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

Finish

8. MTS Allstream SIP Trunking Service Configuration

MTS Allstream is responsible for the configuration of its SIP Trunking Service. The customer will need to provide the IP address used to reach the Avaya SBCE at enterprise side. MTS Allstream will provide the customer with the necessary information to configure the SIP connection from enterprise to the MTS Allstream. The information provided by MTS Allstream includes:

- IP address of the MTS Allstream Session Border Controller.
- MTS Allstream SIP domain. In the compliance test, MTS Allstream preferred to use IP address as a URI-Host.
- CPE SIP domain. In the compliance test, MTS Allstream preferred to use IP address of Avaya SBCE as a URI-Host.
- Supported codecs.
- DID numbers.
- IP addresses and port numbers used for signaling or media through any security devices.

The sample configuration between MTS Allstream and the enterprise for the compliance test was a static configuration. There is no registration on the SIP trunk implemented on either MTS Allstream or enterprise side.

9. Verification and Troubleshooting

This section provides verification steps that may be performed in the field to verify that the solution is configured properly. This section also provides a list of useful troubleshooting commands.

9.1. Verification Steps

The following activities are performed for each test scenario.

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

9.2. Protocol Traces

The following SIP headers are inspected using Wireshark traces:

- Request-URI: verify the request number and SIP domain
- From: verify the display name and display number
- To: verify the display name and display number
- P-Assert-Identity: verify the display name and display number
- Privacy: verify the “user, id” masking

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

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

9.3. Troubleshooting

a) Avaya SBCE

Using a network sniffing tool (e.g., Wireshark) to monitor the SIP signaling messages between MTS Allstream and Avaya SBCE

Following is an example inbound call from MTS Allstream to CS1000.

- Inbound INVITE request from MTS Allstream:

```
INVITE sip:6477761226@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:6477761226@110.10.98.108;user=phone>
From: <sip:16139675279@220.20.2.12;user=phone>;tag=3546180151-253410
P-Asserted-Identity: <sip:16139675279@220.20.2.12;user=phone>
Call-ID: 42919-3546180151-253400@nextone-msw-lab-3.mtsallstream.com
CSeq: 1 INVITE
Allow: CANCEL, INVITE, BYE, OPTIONS, REGISTER, NOTIFY, INFO, REFER, SUBSCRIBE,
PRACK, UPDATE, MESSAGE, PUBLISH
Via: SIP/2.0/UDP
220.20.2.12:5060;branch=z9hG4bKb897bdd90d9972c59bfc5f903c540be1
Contact: <sip:16139675279@220.20.2.12:5060;tgrp=TOROONSBCIOT1>
Content-Type: application/sdp
Accept: application/sdp
Content-Length: 227

v=0
o=nextone-msw-lab-3 505427280 505427280 IN IP4 220.20.2.12
s=sip call
c=IN IP4 220.20.2.13
t=0 0
m=audio 19962 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
```

- 200OK/SDP response by CS1000:

```
SIP/2.0 200 OK
From: <sip:16139675279@220.20.2.12;user=phone>;tag=3546180151-253410
To: <sip:6477761226@110.10.98.108;user=phone>;tag=5cec7a8-be610a87-13c4-55013-
a9c96-2a93fdae-a9c96
CSeq: 1 INVITE
Call-ID: 42919-3546180151-253400@nextone-msw-lab-3.mtsallstream.com
Contact: <sip:6477761226@110.10.98.108:5060;transport=udp;user=phone>
Record-Route: <sip:110.10.98.108:5060;ipcs-line=8456;lr;transport=udp>
Allow:
INVITE,ACK,BYE,REGISTER,REFER,NOTIFY,CANCEL,PRACK,OPTIONS,INFO,SUBSCRIBE,UPDATE
Supported: 100rel, x-nortel-sipvc, replaces
User-Agent: Nortel CS1000 SIP GW release_7.0 version_ssLinux-7.50.17
Via: SIP/2.0/UDP
220.20.2.12:5060;branch=z9hG4bKb897bdd90d9972c59bfc5f903c540be1
Require: timer
Server: AVAYA-SM-6.2.1.0.621009
```

```
Privacy: none
P-Asserted-Identity: "MTS x1226" <sip:6477761226@110.10.98.108;user=phone>
Content-Type: application/sdp
Content-Length: 253

v=0
o=- 144 1 IN IP4 110.10.98.108
s=-
c=IN IP4 110.10.98.108
t=0 0
m=audio 35084 RTP/AVP 0 101 111
c=IN IP4 110.10.98.108
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=rtpmap:111 X-nt-inforeq/8000
a=ptime:20
a=maxptime:20
a=sendrecv
```

Following is an example outbound call from CS1000 to MTS Allstream.

- Outbound INVITE request from CS1000:

```
INVITE sip:16139675258@220.20.2.12;user=phone SIP/2.0
From: "MTS x1226" <sip:6477761226@110.10.98.112;user=phone>;tag=5ceaf28-be610a87-13c4-55013-a9c0a-6a3c0bbf-a9c0a
To: <sip:16139675258@220.20.2.12;user=phone>
CSeq: 1 INVITE
Call-ID: 73783e8-be610a87-13c4-55013-a9c0a-416ee11-a9c0a
Contact: <sip:6477761226@110.10.98.108:5060;transport=udp;user=phone>
Record-Route: <sip:110.10.98.108:5060;ipcs-line=8437;lr;transport=udp>
Allow: INVITE, ACK, BYE, REGISTER, REFER, NOTIFY, CANCEL, PRACK, OPTIONS, INFO,
SUBSCRIBE, UPDATE
Supported: 100rel, x-nortel-sipvc, replaces
User-Agent: Nortel CS1000 SIP GW release_7.0 version_ssLinux-7.50.17 AVAYA-SM-
6.2.1.0.621009
Max-Forwards: 65
Via: SIP/2.0/UDP 110.10.98.108:5060;branch=z9hG4bK-s1632-000961312022-1--s1632-
Privacy: none
P-Asserted-Identity: "MTS x1226" <sip:6477761226@110.10.98.108;user=phone>
Content-Type: application/sdp
Content-Length: 217

v=0
o=- 143 1 IN IP4 110.10.98.108
s=-
c=IN IP4 110.10.98.108
t=0 0
m=audio 35082 RTP/AVP 0 101
c=IN IP4 110.10.98.108
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=ptime:20
a=maxptime:20
a=sendrecv
```

- 200OK/SDP response by MTS Allstream:

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 110.10.98.108:5060;received=110.10.98.108;branch=z9hG4bK-s1632-000961312022-1--s1632-
Record-Route: <sip:110.10.98.108:5060;ipcs-line=8437;lr;transport=udp>
To: <sip:16139675258@220.20.2.12;user=phone>;tag=3546180013-365742
From: "MTS x1226" <sip:6477761226@110.10.98.112;user=phone>;tag=5ceaf28-be610a87-13c4-55013-a9c0a-6a3c0bbf-a9c0a
Call-ID: 73783e8-be610a87-13c4-55013-a9c0a-416ee11-a9c0a
CSeq: 1 INVITE
Allow: CANCEL, INVITE, BYE, OPTIONS, REGISTER, NOTIFY, INFO, REFER, SUBSCRIBE, PRACK, UPDATE, MESSAGE, PUBLISH
Contact: <sip:16139675258@220.20.2.12:5060>
Content-Type: application/sdp
Accept: application/sdp
Content-Length: 227

v=0
o=nextone-msw-lab-3 504051291 504051291 IN IP4 220.20.2.12
s=sip call
c=IN IP4 220.20.2.13
t=0 0
m=audio 19960 RTP/AVP 0 18 8 101
a=ptime:20
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
```

b) CS1000 Verification Steps.

- 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.

- Log into Call Server CLI (please refer to **Section 5.1.2** for more detail)
- Log into 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: 220.20.2.12
FAR-END MEDIA ENDPOINT IP: 110.10.97.216  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: 110.10.98.133  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

```

Following is an example after the call on 1230 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 (6477761226). 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
.

```

Following is an 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
.

```

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Communication Server 1000 7.5, Avaya Aura® Session Manager 6.2 and Avaya Session Border Controller for Enterprise 4.0.5 to MTS Allstream SIP Trunking Service. MTS Allstream SIP Trunking Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large the enterprises. MTS Allstream SIP Trunking Service provides a flexible, cost-saving alternative to traditional analog and ISDN-PRI trunks.

All of the test cases have been executed. Despite the number of observations seen during testing as noted in **Section 2.2**, the test results met the objectives outlined in **Section 2.1**. The MTS Allstream SIP Trunking Service is considered **compliant** with Avaya Communication Server 1000 7.5, Avaya Aura® Session Manager 6.2 and Avaya Session Border Controller for Enterprise 4.0.5.

11. References

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

- [1] *Network Routing Service Fundamentals*, Avaya Communication Server 1000, Release 7.5, 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.
- [7] *Installing and Configuring Avaya Aura® System Platform*, Release 6.03, February 2011.
- [8] *Administering Avaya Aura® System Platform*, Release 6, June 2010.
- [9] *Installing and Upgrading Avaya Aura® System Manager*, Release 6.1, November 2010.
- [10] *Installing and Configuring Avaya Aura® Session Manager*, Release 6.1, April 2011, Number 03-603473.
- [11] *Administering Avaya Aura® Session Manager*, Release 6.1, May 2011, Document Number 03-603324.
- [12] *Administering Avaya one-X® Communicator*, April 2011.
- [13] *Using Avaya one-X® Communicator*, April 2011.
- [14] *UC-Sec Install Guide* (102-5224-400v1.01)
- [15] *UC-Sec Administration Guide* (010-5423-400v106)
- [16] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [17] *RFC 3515, The Session Initiation Protocol (SIP) Refer Method*, <http://www.ietf.org/>
- [18] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>
- [19] *RFC 4244, An Extension to the Session Initiation Protocol (SIP) for Request History Information*, <http://www.ietf.org/>

Product documentation for MTS Allstream SIP Trunking Service is available from MTS Allstream.

©2012 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.