



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring MTS SIP Trunk Service with Avaya Communication Server 1000 Release 7.6, Avaya Aura[®] Session Manager Release 6.3 and Avaya Session Border Controller for Enterprise Release 6.3 – Issue 1.0

Abstract

These Application Notes describe the procedure for configuration of the MTS SIP Trunk Service with Avaya Communication Server 1000 Release 7.6, Avaya Aura[®] Session Manager Release 6.3 and Avaya Session Border Controller for Enterprise Release 6.3.

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

MTS SIP Trunk Service provides PSTN access via SIP trunks between the enterprise and the MTS SIP Trunk Service's network as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

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

Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing.....	4
2.2.	Test Results	6
2.3.	Support	6
3.	Reference Configuration.....	7
4.	Equipment and Software Validated	8
5.	Configure Avaya Communication Server 1000.....	9
5.1.	Log into Communication Server 1000 System	9
5.1.1.	Log into System Manager and Element Manager (EM)	9
5.1.2.	Log into Call Server by Using Overlay Command Line Interface (CLI)	11
5.2.	Administer IP Telephony Node	12
5.2.1.	Obtain Node IP address	12
5.2.2.	Administer Terminal Proxy Server (TPS)	14
5.2.3.	Administer Quality of Service (QoS)	15
5.2.4.	Synchronize New Configuration.....	15
5.3.	Administer Voice Codec	17
5.3.1.	Enable Voice Codec G.711	17
5.3.2.	Enable Voice Codec on Media Gateways.....	18
5.4.	Zones and Bandwidth Management.....	19
5.4.1.	Create Zone for IP Phones (Zone 10)	19
5.4.2.	Create Zone for Virtual SIP Trunk (Zone 255)	20
5.5.	Administer SIP Trunk Gateway	21
5.5.1.	Integrated Services Digital Network (ISDN).....	21
5.5.2.	Administer SIP Trunk Gateway to Avaya Communication Server 1000	23
5.5.3.	Administer Virtual D-Channel.....	25
5.5.4.	Administer Virtual Super-Loop	29
5.5.5.	Administer Virtual SIP Routes	29
5.5.6.	Administer Virtual Trunks.....	31
5.5.7.	Administer Calling Line Identification Entries.....	34
5.5.8.	Enable External Trunk to Trunk Transfer.....	36
5.6.	Administer Dialing Plans	37
5.6.1.	Define ESN Access Codes and Parameters (ESN)	37
5.6.2.	Associate NPA and SPN Call to ESN Access Code 1	38
5.6.3.	Digit Manipulation Block Index (DMI).....	39
5.6.4.	Route List Block (RLB) (RLB 14)	40
5.6.5.	Inbound Call – Incoming Digit Translation Configuration	42
5.6.6.	Outbound Call - Special Number Configuration	44
5.6.7.	Outbound Call - Numbering Plan Area (NPA).....	45
5.7.	Administer a Phone	45
5.7.1.	Phone creation.....	45
5.7.2.	Enable Privacy for the Phone.....	47
5.7.3.	Enable Call Forward for Phone.....	48

6.	Configure Avaya Aura [®] Session Manager	50
6.1.	Avaya Aura [®] System Manager Login and Navigation.....	51
6.2.	Specify SIP Domain	53
6.3.	Add Location.....	53
6.4.	Configure Adaptations	55
6.5.	Add SIP Entities	56
6.5.1.	Configure Session Manager SIP Entity	57
6.5.2.	Configure Communication Server 1000 SIP Entity.....	58
6.5.3.	Configure Avaya SBCE SIP Entity	59
6.6.	Add Entity Links	60
6.7.	Configure Time Ranges	62
6.8.	Add Routing Policies	62
6.9.	Add Dial Patterns	64
7.	Configure Avaya Session Border Controller for Enterprise	67
7.1.	Log into the SBCE	67
7.2.	Global Profiles.....	68
7.2.1.	Configure Server Interworking - Avaya Site	68
7.2.2.	Configure Server Interworking – MTS Site.....	69
7.2.3.	Configure Signaling Manipulation	71
7.2.4.	Configure Server – Session Manager	72
7.2.5.	Configure Server – MTS.....	74
7.2.6.	Configure Routing – Avaya Site.....	78
7.2.7.	Configure Routing – MTS Site.....	79
7.2.8.	Configure Topology Hiding – Avaya Site	80
7.2.9.	Configure Topology Hiding – MTS Site	81
7.3.	Domain Policies	82
	Create End Point Policy Groups	82
7.4.	Device Specific Settings.....	84
7.4.1.	Manage Network Settings.....	84
7.4.2.	Create Media Interfaces	87
7.4.3.	Create Signaling Interfaces	88
7.4.4.	Configuration End Point Flows	89
8.	MTS SIP Trunk Service Configuration	92
9.	Verification Steps.....	93
9.1.	General	93
9.2.	Verification of an Active Call on Communication Server 1000	93
9.3.	Protocol Trace	95
10.	Conclusion	96
11.	References.....	96
12.	Appendix.....	97

1. Introduction

These Application Notes illustrate a sample configuration using Avaya Communication Server 1000 (CS1000) Release 7.6, Avaya Aura® Session Manager Release 6.3 and Avaya Session Border Controller for Enterprise (Avaya SBCE) Release 6.3 with MTS SIP Trunk Service. MTS SIP Trunk Service provides PSTN access via SIP Trunks between the enterprise and the MTS SIP Trunk Service's network as an alternative to legacy analog or digital trunks.

2. General Test Approach and Test Results

CS1000 was connected to Avaya SBCE via Session Manager by using SIP Trunks. Avaya SBCE was connected to MTS SIP Trunk Service's network via SIP trunks. Various call types were made from CS1000 to MTS SIP Trunk Service and vice versa to verify interoperability.

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

2.1. Interoperability Compliance Testing

Compliance testing scenarios for the configuration described in these Application Notes included the following:

- General call processing between CS1000 and MTS SIP Trunk Service, including the following:
 - Codec/ptime (G.711 mu-law/20ms), no Voice Activity Detection (VAD).
 - Calling Line Identification Display (CLID).
 - Ring-back tone.
 - Speech (audio) path.
- Incoming PSTN calls to various phone types including UNISTim, SIP, digital, and analog telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN calls from various phone types including UNISTim, SIP, digital, and analog telephones at the enterprise. All outbound PSTN calls were routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya IP Softphone 2050.
- Dialing plan support: local, long distance, international, outbound toll-free, 411 Service, and Operator Assisted Call.
- Call redirection verification: all supported methods (blind transfer, consultative transfer, call forward, and conference). Call redirection was performed from both ends. Note: MTS SIP Trunk Service supports Diversion Header for off-net call forwarding.
- Registration with authentication.
- Response to SIP OPTIONS queries.

- Response to incomplete call attempts and trunk errors.
- Fax T.38.
- Inbound and outbound long hold time call stability.
- Privacy requests (i.e., caller anonymity) and Caller ID restriction for inbound and outbound calls.
- DTMF (RFC2833) in inbound and outbound calls.
- SIP Transport UDP, port 5060.
- Voicemail navigation for inbound and outbound calls.
- CS1000 Mobile-X feature.

The following is item not tested:

- Fax G.711 pass-through was supported, but we could not test it because by default, Avaya PBX accepted what MTS supported and MTS always sent T.38 to negotiate. There was no way for MTS to force t.38 disabled for a particular PBX as it was a global setting on MTS media gateway and gateway controller card.

The following are items not supported:

- MTS did not support the outbound call to 911 Service.
- MTS did not support the inbound toll free because the setup is not available at the compliance testing.
- MTS did not support Codec G.729 at the compliance testing.

The following assumptions were made for the compliance tested configuration:

- CS1000 R7.6 software with latest patches (**see Section 12 Appendix**).
- MTS SIP Trunk Service provides support to setup, configure and troubleshoot on carrier switch during testing execution.

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

- Calls were checked for the correct call progress tones and cadences.
- During the ringing state, the ring back tone and destination ringing were checked.
- Calls were checked in both hands-free and handset mode due to internal Avaya requirement.
- Calls were checked for speech path in both directions using spoken words to ensure clarity of speech.
- The display(s) of the sets/clients involved were checked for consistent and expected CLID and redirection information both prior to answer and after call establishment.
- The speech path and messaging system were observed for timely and quality End to End tone audio path generation and application responses.
- The call server maintenance terminal window was open during the test execution for the monitoring of BUG(s), ERROR and AUD messages (**See Section 5.1.2**).
- Speech path was checked before and after calls were put on/off hold from each end.
- Calls were checked to ensure that all resources such as Virtual trunks, TDM trunks, Sets and VGWs (Voice Gateways) were released when calls were ended (**See SIP Trunk monitoring in Section 9.2**).

2.2. Test Results

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

- **The Calling Line Identification Display (CLID) was not available after hold/resume**
- If the CS1000 phone holds/resumes an outbound call, the dialed digits were no longer displayed. This is a CS1000 known limitation.
- **Blind Call Transfer to PSTN using Avaya 1140E SIP phone does not complete until transferee picks up the call** - Call scenario is when PSTN phone calls to Avaya 1140E SIP phone, Avaya 1140E SIP phone answers the call and performs blind transfer to another PSTN endpoint. The expected behavior of Avaya 1140E SIP phone is after transfer, the phone should display “transfer completed”. But in this case, user presses “transfer” button, answers question of “Consultative transfer with party ?” with “No”, which implies the blind transfer, as the transferee PSTN phone is ringing, the Avaya 1140E SIP phone should be released and display “transfer successfully”. Instead, the Avaya 1140E SIP phone still displays “transferring” and not released until the transferee PSTN phone answers the call. The work around is to hang up the Avaya 1140E SIP phone. This is minor known limitation on Avaya 1140E SIP phone. There is no user impact. Transfer is still completed with two-way audio.
- **Avaya 1140E SIP telephone is hanged up/dropped out of the conference, the conference call is dropped** – During a conference call hosted by the 1140E SIP telephone, if the 1140E SIP telephone is hanged up/dropped out of the conference, the conference call is dropped. This is known CS1000 SIP telephone limitation.

2.3. Support

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

For technical support on the MTS SIP Trunk Service, please contact customer service at 888-689-7073 or visit: <http://www.mts.ca/mts/support>.

3. Reference Configuration

Figure 1 illustrates the test configuration used during the compliance test between CS1000 and MTS SIP Trunk Service. For confidentiality and privacy purposes, actual public IP addresses used in this testing have been masked and replaced with fictitious IP addresses throughout the document.

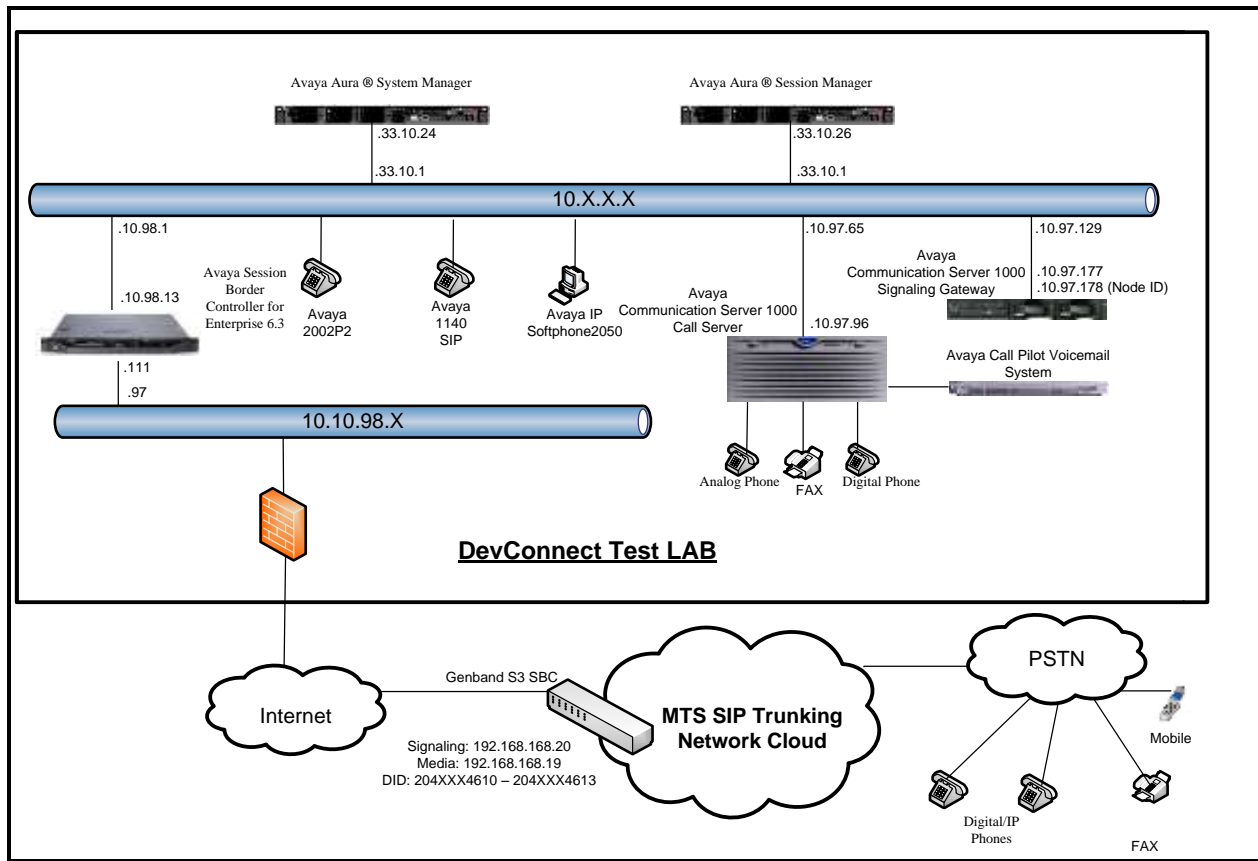


Figure 1 - Network diagram for Avaya and MTS SIP Trunk Service

4. Equipment and Software Validated

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

Avaya systems:

Equipment/Software	Release/Version
Avaya Communication Server 1000 (CPPM)	Call Server: 765 P + Signaling Server: 7.65.16 GA SIP Line Server: 7.65.16 GA
Avaya Call Pilot C201i	Call Pilot Voice Mail Manager: 05.00.41.143
Avaya Aura [®] Session Manager running on Avaya S8800 Server	6.3.13 (6.3.13.631303)
Avaya Aura [®] System Manager running on Avaya S8800 Server	6.3.13 (Build No 6.3.0.8.5682 – Patch 6.3.8.5108 Software Update Revision No: 6.3.13.10.3336)
Avaya Session Border Controller for Enterprise	6.3.2-08-5478
Avaya Phones: 2002 p2 (UNISTim) 1140E SIP	0604DCO 04.04.18.00
Avaya 3904 Digital Phone	Core: 2.4 – Flash: 9.4 PO L1.8
Avaya IP Softphone 2050	4.04.0067
Analog Symphony 2000	N/A
HP Office jet 4500 Fax	N/A

MTS SIP Trunk Service systems:

System	Software
Genband A2/Experius	10.3
Genband S3/Q20	v8.3.8.4

5. Configure Avaya Communication Server 1000

These Application Notes use the Incoming Digit Translation feature to receive calls, the Numbering Plan Area Code (NPA), and the Special Number (SPN) features to route calls from the CS1000 to the PSTN, via SIP trunks to the MTS SIP Trunk Service network.

These Application Notes assume that the basic CS1000 configuration has already been administered. For further information on CS1000, please consult the references in **Section 11**.

The procedures below describe the configuration details for configuring the CS1000.

5.1. Log into Communication Server 1000 System

5.1.1. Log into System Manager and Element Manager (EM)

Open an instance of a web browser and connect to the System Manager using the following address: `https://<System Manager IP address>/SMGR/`. Log in using an appropriate User ID and Password (not shown). Select **Elements** → **Communication Server 1000**.

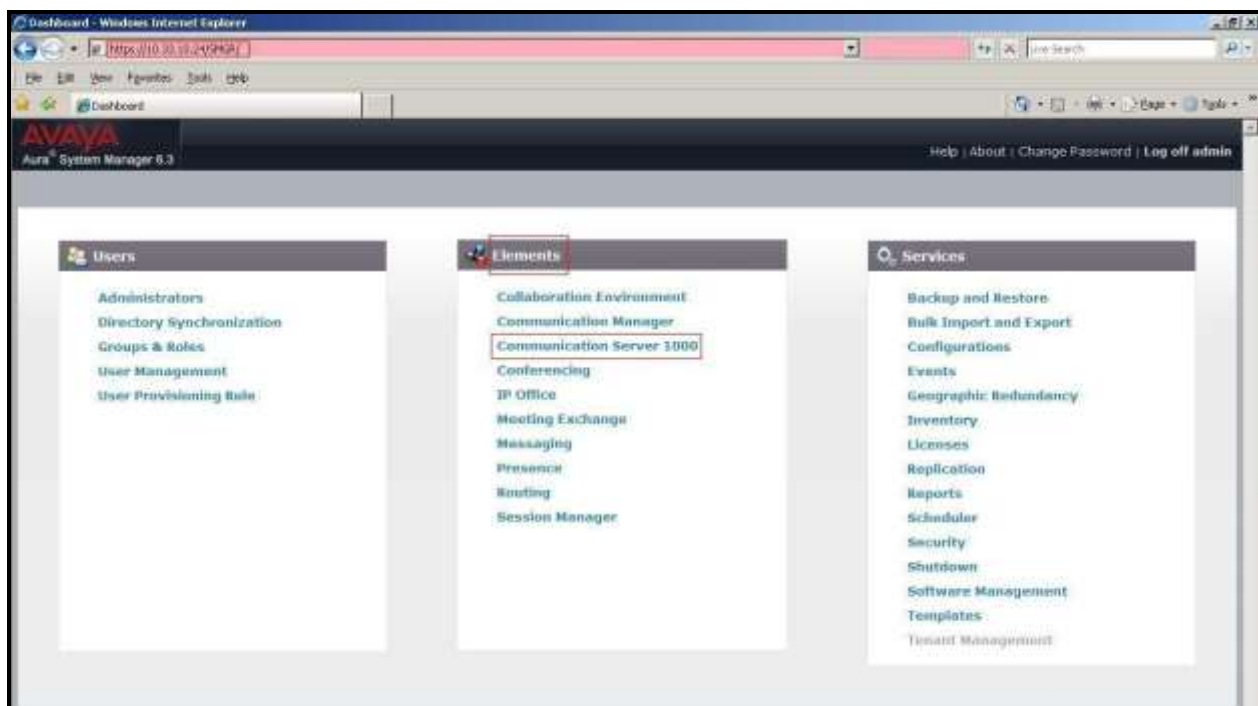


Figure 2 – System Manager Home Screen

The **Avaya Communication Server 1000 Management** screen is displayed. Click on the **Element Name** of the CS1000 Element as highlighted in red box below:

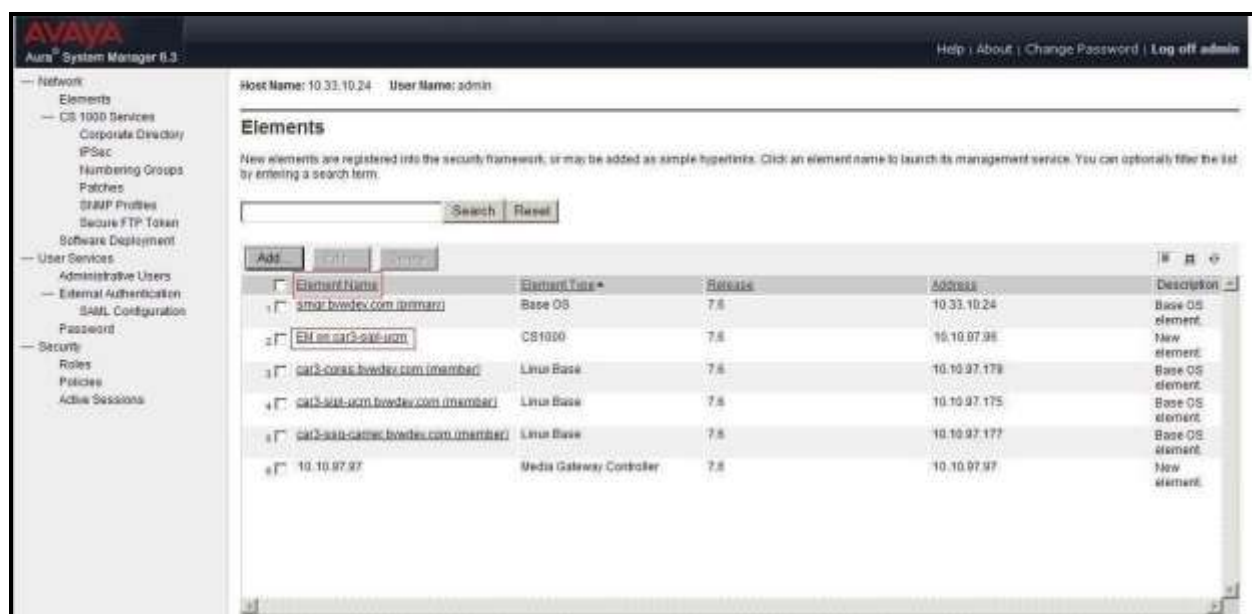


Figure 3 – Communication Server 1000 Management

Log into the CS1000 using an appropriate **User ID** and **Password**.



Figure 4 – Communication Server 1000 Log In Screen

The CS1000 Element Manager **System Overview** page is displayed as shown in **Figure 5**.

IP Address: 10.10.97.96

Type: Avaya Communication Server 1000E CPPM Linux

Version: 4121

Release: 765 P +



Figure 5 – Element Manager System Overview

5.1.2. Log into Call Server by Using Overlay Command Line Interface (CLI)

Using Putty, SSH to the IP address of the CS1000 Signaling Server using an account with administrator credentials.

Run the command **cslogin** and log in with the appropriate user account and password. Sample output is shown below.

login as: **← Enter an account with administrator credentials**

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

admin@10.10.97.178's password: **← Enter the password**

Last login: Wed Jul 29 07:20:18 2015 from 10.10.98.78

[admin@car3-cores ~]\$ **cslogin**

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

USERID? **← Enter the user account**

PASS? **← Enter the password**

.

TTY #08 LOGGED IN ADMIN 07:39 3/8/2015

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 log out immediately. This system may be monitored for operational purposes at any time.

>

Note: This screen can be used for monitoring of BUG(s), ERROR and AUD messages.

5.2. Administer IP Telephony Node

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

5.2.1. Obtain Node IP address

These Application Notes assume that the basic CS1000 configuration has already been administered and that a Node has already been created. This section describes the steps for configuring a Node (Node ID 3000) in CS1000 IP network to work with MTS SIP Trunk Service. For further information on CS1000, please consult the references in **Section 11**.

Select **System** → **IP Network** → **Nodes: Servers, Media Cards** and then click on the **Node ID** as shown in **Figure 6**.

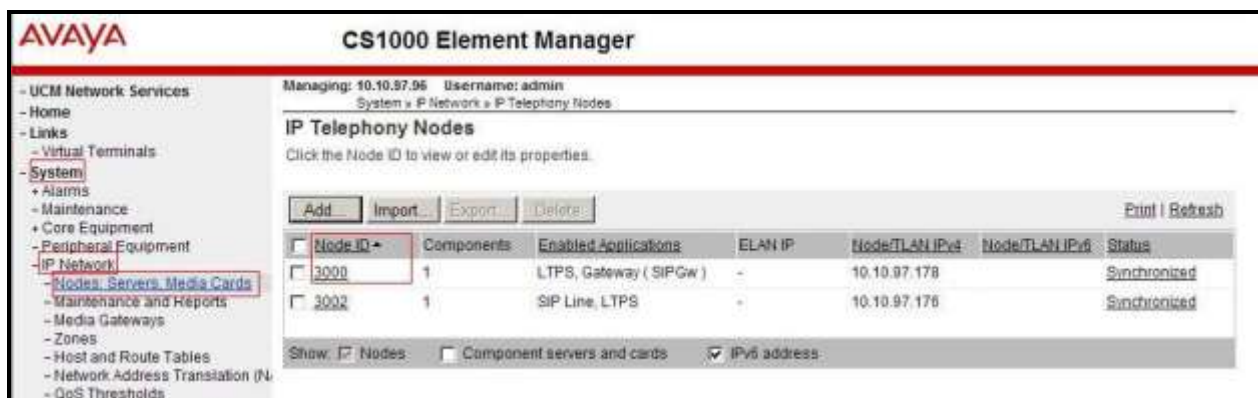


Figure 6 – IP Telephony Node

The **Node Details** screen is displayed in **Figure 7** with the IP address of the CS1000 node. **Call server IP address: 10.10.97.96**. The **Node IPv4 address 10.10.97.178** is a virtual address which corresponds to the **TLAN IPv4** address **10.10.97.177** of the Signaling Server/SIP Signaling Gateway. The SIP Signaling Gateway uses this Node IP address to communicate with other components to process SIP calls.

AVAYA CS1000 Element Manager

Managing: 10.10.97.96 Username: admin
System > IP Network > IP Telephony Nodes > Node Details

Node Details (ID: 3000 - LTPS, Gateway (SIPGw))

Node ID: 3000 * (0-9999)

Call server IP address: 10.10.97.96

TLAN address type: ☒ IPv4 only
☐ IPv4 and IPv6

Embedded LAN (ELAN)

Gateway IP address: 10.10.97.65

Subnet mask: 255.255.255.192

Telephony LAN (TLAN)

Node IPv4 address: 10.10.97.178

Subnet mask: 255.255.255.192

Node IPv6 address:

* Required Value.

Associated Signaling Servers & Cards

Select to add Add Remove Make Leader Print Refresh

Hostname	Type	Deployed Applications	ELAN IP	TLAN IPv4	Role
<input type="checkbox"/> car3-ssg-carrier	Signaling_Server	SIP Line, LTPS, Gateway (SIP/H323), PD, Presence Publisher, IP Media Services	10.10.97.95	10.10.97.177	Leader

Show: ☐ IPv6 addresses

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

Figure 7 – Node Details 1

The **Node Details** screen is displayed in **Figure 8** with the IP Telephony Node Properties and Applications.

AVAYA CS1000 Element Manager

Managing: 10.10.97.36 Username: admin
System > IP Network > IP Telephony Nodes > Node Details

Node Details (ID: 3000 - LTPS, Gateway (SIPGw))

Subnet mask: 255.255.255.192 Subnet mask: 255.255.255.192
Node IPv6 address:

IP Telephony Node Properties

- Voice Gateway (VGW) and Coders
- Quality of Service (QoS)
- LAN
- STTP
- Numbering Zones
- MCDN Alternative Routing Treatment (MALT) Causes

Applications (click to edit configuration)

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

* Required Value. [Save] [Cancel]

Associated Signaling Servers & Cards

[Select to add] [Add] [Remove] [Make Leader] [Print] [Refresh]

Hostname	Type	Deployed Applications	ELAN IP	TLAN IPv4	Role
car3-ssg-carrier	Signaling_Server	SIP Line, LTPS, Gateway (SIPH323), PD, Presence Publisher, IP Media Services	10.10.97.95	10.10.97.177	Leader

Show: ☐ IPv6 address

Figure 8 – Node Details 2

5.2.2. Administer Terminal Proxy Server (TPS)

Continuing from **Section 5.2.1**, on the **Node Details** page, select the **Terminal Proxy Server (TPS)** link as shown in **Figure 8**. Check the **UNISim Line Terminal Proxy Server** checkbox to enable proxy service on this node and then click the **Save** button as shown in **Figure 9**.

AVAYA CS1000 Element Manager

Managing: 10.10.97.36 Username: admin
System > IP Network > IP Telephony Nodes > Node Details > UNISim Line Terminal Proxy Server (LTPS) Configuration

Node ID: 3000 - UNISim Line Terminal Proxy Server (LTPS) Configuration Details

Firmware (DTLS) (Network Connect Server)

UNISim Line Terminal Proxy Server ☒ Enable proxy service on this node

Firmware

IP address: 10.10.97.36
Full file path: download/firmware
Server Account/User ID:
Password:

DTLS

DTLS policy: OFF

Options: ☐ Client authentication ☐ Periodic re-routing

Network Connect Server

* Required Value. [Save] [Cancel]

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

Figure 9 – TPS Configuration Details

5.2.3. Administer Quality of Service (QoS)

Continuing from **Section 5.2.1**, on the **Node Details** page, select the **Quality of Service (QoS)** link as shown in **Figure 8**. The default Diffserv values are as shown in **Figure 10**. Click on the **Save** button.

The screenshot shows the 'CS1000 Element Manager' interface. The left sidebar contains a tree view with categories like 'UCM Network Services', 'System', 'Alarms', 'Maintenance', 'Core Equipment', 'Peripheral Equipment', 'IP Network', 'Nodes, Servers, Media Cards', 'Maintenance and Reports', 'Media Gateways', 'Zones', 'Host and Route Tables', 'Network Address Translation (NAT)', 'QoS Thresholds', 'Personal Directories', 'Unicode Name Directory', 'Interfaces', 'Engineered Values', 'Emergency Services', 'Geographic Redundancy', 'Software', 'Customers', 'Routes and Trunks', 'Routes and Trunks', 'D-Channels', 'Digital Trunk Interface', and 'Dialing and Numbering Plans'. The main content area is titled 'Node ID: 3000 - Quality of Service (QoS)'. It displays a 'Diffserv Codepoint (DSCP)' configuration box with the following settings: 'Enable Avaya automatic QoS' (unchecked), 'Control packets' (40), 'Voice packets' (40), 'VLAN tagging' (checked), and '802.1Q support' (checked). At the bottom, there is a 'Save' button and a 'Cancel' button. A note at the bottom states: 'Note: Changes made on this page will NOT be transferred until the Node is also saved.'

Figure 10 – QoS Configuration Details

5.2.4. Synchronize New Configuration

Continuing from **Section 5.2.3**, return to the **Node Details** page (**Figure 7**) and click on the **Save** button. The **Node Saved** screen is displayed. Click on **Transfer Now**.

The screenshot shows the 'CS1000 Element Manager' interface. The left sidebar is the same as in Figure 10. The main content area is titled 'Node Saved'. It displays a message: 'Node ID: 3000 has been saved on the call server. The new configuration must also be transferred to associated servers and media cards.' Below this message, there are two buttons: 'Transfer Now...' and 'Show Nodes...'. The 'Transfer Now...' button is highlighted with a red box. To the right of the 'Transfer Now...' button, there is a note: 'You will be given an option to select individual servers, or transfer to all.' To the right of the 'Show Nodes...' button, there is a note: 'You may initiate a transfer manually at a later time.'

Figure 11 – Node Saved Screen

The **Synchronize Configuration Files (Node ID <3000>)** screen is displayed. Check the **car3-ssg-carrier** checkbox and click on **Start Sync**. When the synchronization completes, check the **car3-ssg-carrier** checkbox and click on the **Restart Applications**.

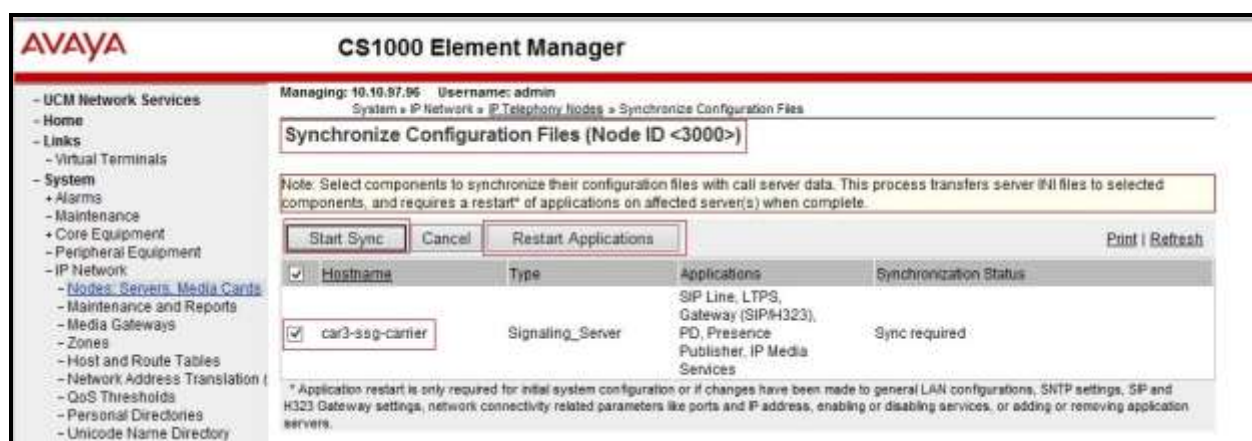


Figure 12 – Node Synchronized Screen

5.3. Administer Voice Codec

5.3.1. Enable Voice Codec G.711

Select **IP Network** → **Nodes: Servers, Media Cards** from the left pane and on the **IP Telephony Nodes** screen displayed (not shown), select the **Node ID** of the CS1000 system. The **Node Details** screen is displayed (see **Section 5.2.1** for more details). On the **Node Details** page shown in **Figure 8**, click on **Voice Gateway (VGW) and Codecs**.

MTS SIP Trunk Service supports **G.711 mu-law** with **Voice payload size 20 milliseconds per frame**. Uncheck **Voice Activity Detection (VAD)** checkbox. Click on the **Save** button.

The screenshot displays the AVAYA CS1000 Element Manager interface. The left navigation pane shows a tree structure with 'IP Network' expanded and 'Nodes: Servers, Media Cards' selected. The main content area is titled 'Node ID: 3000 - Voice Gateway (VGW) and Codecs'. It contains three sections for codec configuration: Codec G711, Codec G722, and Codec G729. Each section has a 'Voice payload size' dropdown and a 'Voice playout (jitter buffer) delay' dropdown. For Codec G711, the payload size is 20 ms and the delay is 20-40 ms. For Codec G722, the payload size is 80 ms and the delay is 80 ms. For Codec G729, the payload size is 20 ms and the delay is 20-40 ms. A 'Voice Activity Detection (VAD)' checkbox is present and unchecked. At the bottom, there is a 'Save' button and a 'Cancel' button. A note at the bottom states: 'Note: Changes made on this page will NOT be transmitted until the Node is also saved.'

Figure 13 – Voice Gateway and Codec Configuration Details

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

5.3.2. Enable Voice Codec on Media Gateways

From the left menu of the Element Manager page in **Figure 13**, select **IP Network → Media Gateways**. The Media Gateways page will appear (not shown). Click on the **MGC** which is located on the right of the page. In the following screen, scroll down to select the **Codec G711** with **Voice payload size 20 ms/frame** and uncheck **VAD** as shown in **Figure 14**. Scroll down to the bottom of the page and click on the **Save** button (not shown).

AVAYA **CS1000 Element Manager**

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

- VGW and IP phone codec profile

Enable echo canceller ☒

Echo canceller tail delay 128 (milliseconds)

Enable dynamic attenuation ☒

Voice activity detection threshold 1 (0 - 4 DBM)

Idle noise level 0 (0 - 1 DBM)

R factor calculation ☐

DTMF tone detection ☒

Enable low latency mode ☐

Remove DTMF delay (squelch DTMF from TDM to IP) ☒

Enable modem/fax pass through mode ☒

Enable V.21 FAX tone detection ☒

Fax TCF method 2

FAX maximum rate 14400 (bps)

FAX playout nominal delay 100 (0 - 300 milliseconds)

FAX no activity timeout 20 (10 - 32000 milliseconds)

FAX packet size 30

- Codec G711 Select ☒

Codec name G711

Voice payload size 20 (ms/frame)

Voice playback (jitter buffer) nominal delay 20

Modifications may cause changes to dependent settings

Voice playback (jitter buffer) maximum delay 40

Modifications may cause changes to dependent settings

VAD ☐

- Codec G729A Select ☐

Codec name G729A

Voice payload size 20 (ms/frame)

Voice playback (jitter buffer) nominal delay 20

Figure 14 – Media Gateways Configuration Details

5.4. Zones and Bandwidth Management

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

5.4.1. Create Zone for IP Phones (Zone 10)

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

Select **IP Network** → **Zones** from the left pane (not shown), click on **Bandwidth Zones** as shown in **Figure 15**.

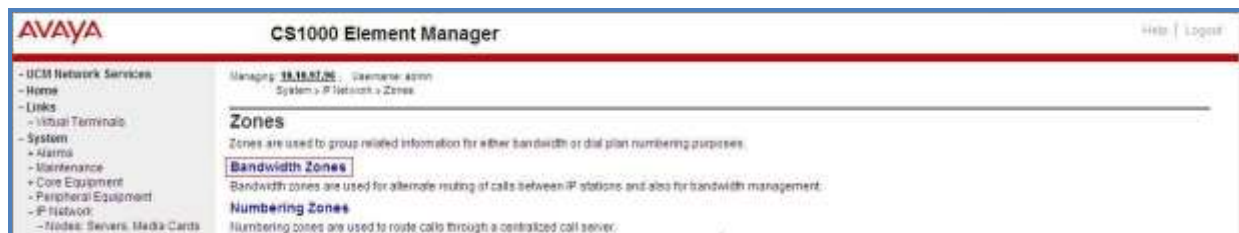


Figure 15 – Zones Page

The **Bandwidth Zones** screen is displayed as shown in **Figure 16**. Click **Add** to create a new zone for IP Phones.

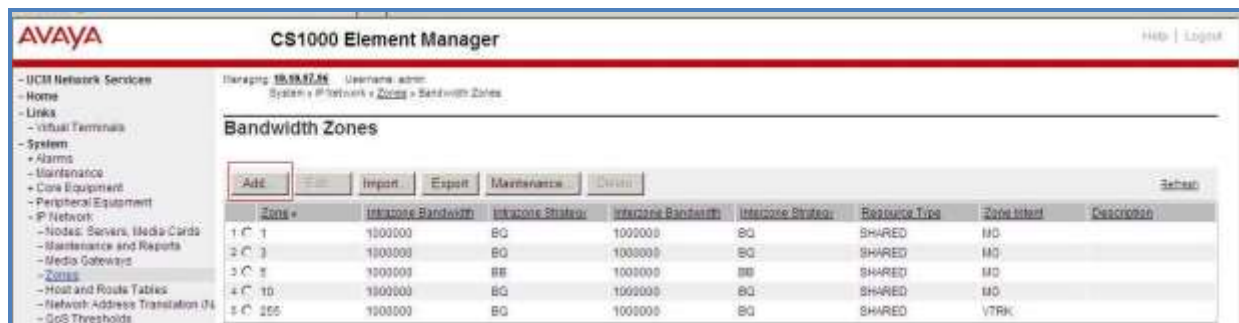


Figure 16 – Bandwidth Zones

Select and input the values as shown below (in the red boxes) in **Figure 17**, and click on the **Submit** button.

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

The screenshot shows the 'Zone Basic Property and Bandwidth Management' page in the AVAYA CS1000 Element Manager. The page is titled 'Managing 10.10.10.10' and 'User: admin'. The left-hand navigation menu includes options like 'UCM Network Services', 'Home', 'Links', 'System', 'Maintenance', 'Core Equipment', 'Peripheral Equipment', 'IP Network', 'Nodes: Servers, Media Cards', 'Maintenance and Reports', 'Media Gateways', 'Zones', 'Host and Route Tables', 'Network Address Translation (NAT)', 'CoS Thresholds', 'Personal Directories', 'Unicode Name Directory', 'Interfaces', 'Engineered Values', 'Emergency Services', 'Geographic Redundancy', 'Software', 'Customers', and 'Routes and Trunks'. The main configuration area has a table with 'Input Description' and 'Input Value' columns. The values are: Zone Number (10), Intrazone Bandwidth (1000000), Intrazone Strategy (Best Quality (BQ)), Interzone Bandwidth (1000000), Interzone Strategy (Best Quality (BQ)), Resource Type (Shared (SHARED)), and Zone Intent (MO (MO)). The 'Submit' button is at the bottom left.

Figure 17 – Bandwidth Management Configuration Details – IP phone

5.4.2. Create Zone for Virtual SIP Trunk (Zone 255)

Follow the steps described in **Section 5.4.1** to create a zone for the virtual SIP trunk. The difference is in the **Zone Intent (ZBRN)** field. Select **VTRK** for virtual trunk as shown in **Figure 18** and then click on the **Submit** button.

The screenshot shows the 'Zone Basic Property and Bandwidth Management' page in the AVAYA CS1000 Element Manager. The page is titled 'Managing 10.10.10.10' and 'User: admin'. The left-hand navigation menu is the same as in Figure 17. The main configuration area has a table with 'Input Description' and 'Input Value' columns. The values are: Zone Number (255), Intrazone Bandwidth (1000000), Intrazone Strategy (Best Quality (BQ)), Interzone Bandwidth (1000000), Interzone Strategy (Best Quality (BQ)), Resource Type (Shared (SHARED)), and Zone Intent (VTRK (VTRK)). The 'Submit' button is at the bottom left.

Figure 18 – Bandwidth Management Configuration Details – Virtual SIP trunk

5.5. Administer SIP Trunk Gateway

This section describes the steps for establishing a SIP connection between the SIP Signaling Gateway and Session Manager.

5.5.1. Integrated Services Digital Network (ISDN)

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

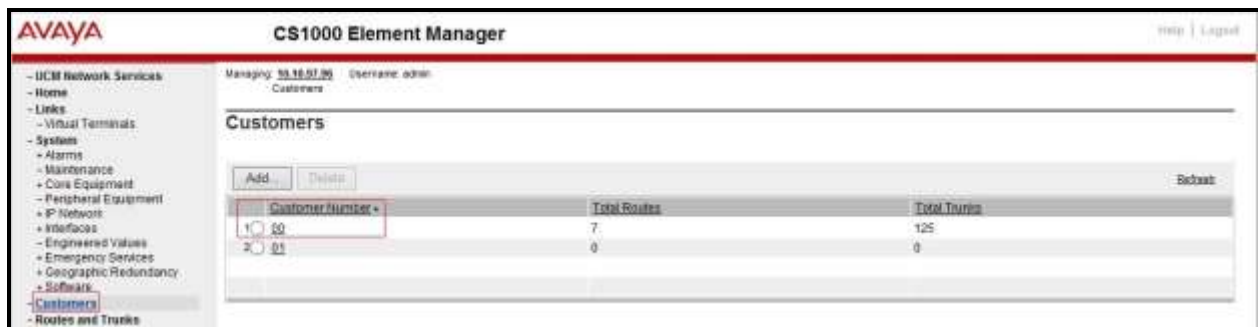


Figure 19 – Customer – ISDN Configuration 1

The system can support more than one customer with different network settings and options. The **Customer Details** page will appear. Select the **Feature Packages** option from **Customer Details** page.

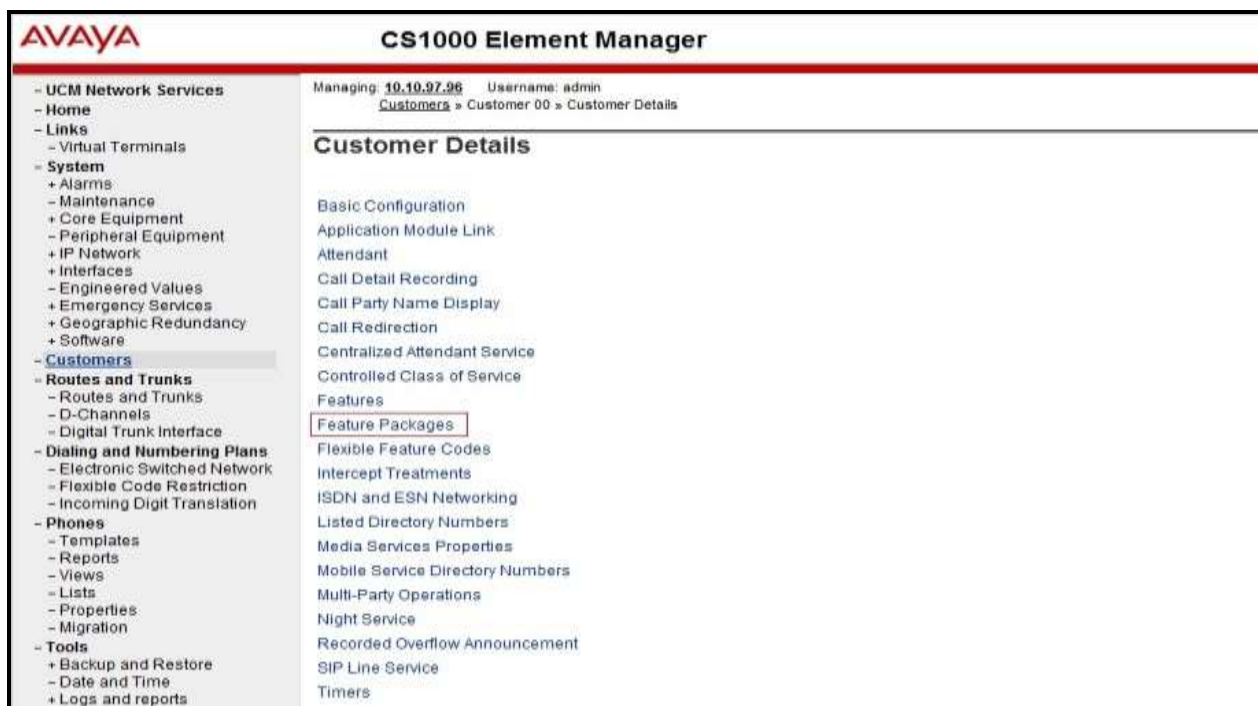


Figure 20 – Customer – ISDN Configuration 2

The screen is updated with a listing of available **Feature Packages** (not all features are shown in **Figure 21** below). Select **Integrated Services Digital Network** to edit the parameters shown below. Check the **Integrated Services Digital Network** option, and retain the default values for all remaining fields. Scroll down to the bottom of the screen, and click on the **Save** button (not shown).

AVAYA CS1000 Element Manager

Managing: 10.10.97.96 Username: admin
Customers » Customer 00 » Customer Details » Feature Packages

Feature Packages

+ Do Not Disturb Individual	Package: 9
+ End-to-End Signaling	Package: 10
+ Message Waiting Center	Package: 46
+ New Flexible Code Restriction	Package: 49
+ Set Relocation	Package: 53
+ Network Alternate Route Selection	Package: 58
+ Distinctive Ringing	Package: 74
+ Departmental Listed Directory Number	Package: 76
+ Command Status Link	Package: 77
+ Pretranslation	Package: 92
+ Dialed Number Identification System	Package: 98
+ Malicious Call Trace	Package: 107
+ Incoming Digit Conversion	Package: 113
+ Directed Call Pickup	Package: 115
+ Enhanced Music	Package: 119
+ Station Camp-On	Package: 121
+ Integrated Digital Access	Package: 122
+ Digital Private Network Signaling System 1	Package: 123
+ Flexible Tones and Cadences	Package: 125
+ Multifrequency Compelled Signaling	Package: 128
+ International Supplementary Features	Package: 131
+ Enhanced Night Service	Package: 133
- Integrated Services Digital Network	Package: 145

+ Dial Access Prefix on CLID table entry option

Integrated Services Digital Network: ☒

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

- Private network identifier: 1 (1 - 16383)

- Node DN:

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

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

Figure 21 – Customer – ISDN Configuration 3

5.5.2. Administer SIP Trunk Gateway to Avaya Communication Server 1000

Select **IP Network** → **Nodes: Servers, Media Cards** from the left pane. In the **IP Telephony Nodes** screen displayed (not shown), select the **Node ID** of the CS1000 system. The **Node Details** screen is displayed as shown in **Figure 8, Section 5.2.1**.

On the **Node Details** screen, select **Gateway (SIPGw)**. Under the **General** tab of the **Virtual Trunk Gateway Configuration Details** screen, enter the following values (highlighted in red boxes) for the specified fields, and retain the default values for the remaining fields as shown in **Figure 22**. The **SIP domain name** and **Local SIP port** should be matched in the configuration of Session Manager (in **Section 6.2**, and **6.6**).

The screenshot displays the AVAYA CS1000 Element Manager interface. The left-hand navigation pane lists various system components, with 'Nodes: Servers, Media Cards' selected. The main content area shows the 'Node ID: 3000 - Virtual Trunk Gateway Configuration Details' screen. The 'General' tab is active, and the 'Vtrk gateway application' is set to 'SIP Gateway (SIPGw)'. The 'SIP domain name' is 'bwrddev7.com', the 'Local SIP port' is '5060', the 'Gateway endpoint name' is 'car3-ssg-carrier', and the 'Application node ID' is '3000'. The 'Enable failsafe NRS' checkbox is unchecked. The 'Virtual Trunk Network Health Monitor' section is also visible, with a 'Monitor IP addresses' checkbox and a list of monitored IP addresses. The interface includes a 'Save' button and a 'Cancel' button at the bottom right.

Figure 22 – Virtual Trunk Gateway Configuration Details

Click on the **SIP Gateway Settings** tab. Under **Proxy or Redirect Server**, enter the following values (highlighted in red boxes) for the specified fields and retain the default values for the remaining fields, as shown in **Figure 23**. Enter the IP address of Session Manager in the **Primary TLAN IP address** field. Enter **5060** for **Port** and select **UDP** for **Transport protocol**. This should be matched in the configuration of Session Manager (see in **Section 6.5.1**). Uncheck the **Support registration** checkbox.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation tree with categories like UCIM Network Services, System, IP Network, and Interfaces. The main content area is titled 'Node ID: 3000 - Virtual Trunk Gateway Configuration Details'. It has three tabs: 'General', 'SIP Gateway Settings' (which is selected), and 'SIP Gateway Services'. Under the 'SIP Gateway Settings' tab, there is a section for 'Proxy or Redirect Server'. This section contains fields for 'Primary TLAN IP address' (10.33.10.26), 'Port' (5060), 'Transport protocol' (UDP), and 'Options' (with 'Support registration' unchecked). Below this is a section for 'Secondary TLAN IP address' (0.0.0.0) and its 'Port' (5060) and 'Transport protocol' (TCP). A note at the bottom states: 'Note: Changes made on this page will NOT be transmitted until the Node is also saved.' There are 'Save' and 'Cancel' buttons at the bottom right.

Figure 23 – Virtual Trunk Gateway Configuration Details

On the same page as shown in **Figure 23**, scroll down to the **SIP URI Map** section. Under **Public E.164 domain names**, enter the following:

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

Under **Private domain names**, enter the following:

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

The remaining fields can be left at their default values as shown in **Figure 24**. Click on the **Save** button.

Figure 24 – Virtual Trunk Gateway Configuration Details

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

5.5.3. Administer Virtual D-Channel

Select **Routes and Trunks** → **D-Channels** (not shown) from the left pane to display the **D-Channels** screen. In the **Choose a D-Channel Number** field, select an available D-channel from the drop-down list and type **DCH** as shown in **Figure 25**. Click on the **to Add** button.

Figure 25 – D-Channels

The **D-Channels 100 Property Configuration** screen is displayed next, as shown in **Figure 26**. Enter the following values for the specified fields, and retain the default values for the remaining fields.

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

Click on **Advanced options (ADVOPT)**. Check on the **Network Attendant Service Allowed** checkbox as shown in **Figure 26**. Other fields are left as default.

Figure 26 – D-Channel Configuration

Click on **Basic Options (BSCOPT)** and click on the **Edit** button on the **Remote Capabilities** field as shown in **Figures 27**.

AVAYA CS1000 Element Manager

Help | Logout

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

- Basic options (BSCOPT)

Action Device And Number (ADAN): DCH

D channel Card Type: DCP

Designator: VoIP

Recovery to Primary: ☐

PRF loop number for Backup D-channel:

User: Integrated Services Signaling Link Dedicated (IS-D)

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

Country: ETS 300 =102 basic protocol (ETSI)

D-Channel PRF loop number:

Primary Rate Interface: **more PRF**

Secondary PRF loops:

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

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: 1000 Range: 0 - 3700

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

- P/N: customer number:

- Progress signal:

- Calling Line Identification:

- Output request Buffer: 32

- D-channel transmission Rate: 56 kbps when LCMF is ALB (56K)

- Channel Negotiation option: No alternative acceptable, exclusive, (1)

- Remote Capabilities: Edit

- B channel Service messaging: ☐

- Change protocol timer value (TMR)

- Advanced options (ADVOPT)

- Feature Packages

Submit Refresh Delete Cancel

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

Figure 27 – D-Channel Configuration

The **Remote Capabilities Configuration** page appears as shown in **Figures 28**. Check the **ND2** and the **MWI** checkboxes.

AVAYA CS1000 Element Manager

Managing: 18.16.07.05 username: admin
Routes and Trunks > DCM Models > DCM Capabilities > Review Capabilities Configuration

Remote Capabilities Configuration

Input Description	Input Value
Basic rate interface (BRI)	<input type="checkbox"/>
Call completion on busy using integer value (CCBI)	<input type="checkbox"/>
Call completion on busy using object identifier (CCBO)	<input type="checkbox"/>
Call completion on busy for GSK and EuroISDN BRI (CCBS)	<input type="checkbox"/>
Call completion on no response using integer value (CCNI)	<input type="checkbox"/>
Call completion on no response using object identifier (CCNO)	<input type="checkbox"/>
Call completion to no reply for GSK and EuroISDN BRI (CCNR)	<input type="checkbox"/>
Network call park (CPK)	<input type="checkbox"/>
Connected line identification presentation (COLP)	<input type="checkbox"/>
Call transfer integer (CTI)	<input type="checkbox"/>
Call transfer object (CTO)	<input type="checkbox"/>
Diversion info. is sent using integer value (DV1I)	<input type="checkbox"/>
Diversion info. is sent using object identifier (DV1O)	<input type="checkbox"/>
Rerouting requests processed using integer value (DV2I)	<input type="checkbox"/>
Rerouting requests processed using object identifier (DV2O)	<input type="checkbox"/>
Diversion info. sent. rerouting requests processed (DV3I)	<input type="checkbox"/>
EuroISDN - div. info sent. rerouting req. processed (DV3O)	<input type="checkbox"/>
Call transfer notification and invocation to EuroISDN (ECTO)	<input type="checkbox"/>
Multicous call identification (MCID)	<input type="checkbox"/>
ISDN QSIG conversion (ISQC)	<input type="checkbox"/>
Remote D-channel is on a MSOL card (MSL)	<input type="checkbox"/>
Message waiting interworking with DMS-100 (MWI)	<input checked="" type="checkbox"/>
Network access data (NAC)	<input type="checkbox"/>
Network call trace supported (NCT)	<input type="checkbox"/>
Network name display method 1 (ND1)	<input type="checkbox"/>
Network name display method 2 (ND2)	<input checked="" type="checkbox"/>
Network name display method 3 (ND3)	<input type="checkbox"/>
Name display - integer ID coding (NDI)	<input type="checkbox"/>
Name display - object ID coding (NDO)	<input type="checkbox"/>

Copyright © 2005-2011 Avaya Inc. All rights reserved.

Figure 28 – Remote Capabilities Configuration

Click on the **Return – Remote Capabilities** button (not shown).

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

5.5.4. Administer Virtual Super-Loop

Select **System** → **Core Equipment** → **Superloops** from the left pane to display the **Superloops** screen. If the Superloop does not exist, please click the **Add** button to create a new one as shown in **Figure 29**. In this example, Superloop 4, 96, 100, and 124 have been added and are being used.



Figure 29 – Administer Virtual Super-Loop Page

5.5.5. Administer Virtual SIP Routes

Select **Routes and Trunks** → **Routes and Trunks** (not shown) from the left pane to display the **Routes and Trunks** screen. In this example, **Customer 0** is being used. Click on the **Add route** button as shown in **Figure 30**.



Figure 30 – Add route

The **Customer 0, New Route Configuration** screen is displayed next (not shown). The **Basic Configuration** section is displayed. Enter the following values for the specific fields, and retain the default values for the remaining fields. The screenshot of Basic Configuration section of existing route 100 is displayed to edit as shown in **Figures 31**.

- **Route data block (RDB) (TYPE):** RDB as default.
- **Customer number (CUST):** 0 as customer 0 is in used.
- **Route number (ROUT):** Enter an available route number (example: route 100).
- **Designator field for trunk (DES):** A descriptive text (100).
- **Trunk type (TKTP):** TIE trunk data block (TIE).
- **Incoming and outgoing trunk (ICOG):** Incoming and Outgoing (IAO).
- **Access code for the trunk route (ACOD):** An available access code (example: 8100).

- Check the **The route is for a virtual trunk route (VTRK)** field, 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**). **Note:** The Zone value is filled out as 255, but after it is added, the screen is displayed with prefix 00.
- For the **Node ID of signaling server of this route (NODE)** field, enter the node number **3000** (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. Scrolling down to the bottom of the screen, enter the following values for the specified fields, and retain the default values for the remaining fields.
 - **Mode of operation (MODE):** Select **Route uses ISDN Signalling Link (ISLD)**.
 - **D channel number (DCH):** Enter **100** (created in **Section 5.5.3**).
 - **Interface type for route (IFC):** Select **Meridian M1 (SL1)**.
 - **Private network identifier (PNI):** Enter **1**. **Note:** The value is filled out as 1, but after it is added, the screen is displayed with prefix 0000.
 - **Network calling name allowed (NCNA):** Check this option to allow calling name display.
 - **Network call redirection (NCRD):** Check this option to allow call redirection.
 - **Insert ESN access code (INAC):** Check this option to insert ESN access code (Refer to **Section 5.6.1**).

The screenshot shows the Avaya CS1000 Element Manager interface. The main window is titled 'Customer 0, Route 100 Property Configuration'. The 'Basic Configuration' tab is selected. The configuration fields are as follows:

- Route data block (RDB) (TYPE): [Field]
- Customer number (CUST): [Field]
- Route number (ROUT): [Field]
- Designator field for trunk (DCE): [Field]
- Trunk type (TRTP): [Field]
- Incoming and outgoing trunk (ICOG): [Field]
- Access code for the trunk route (ACOG): [Field]
- Trunk type (ST1SP) (ST1SP): [Field]
- The route is for a virtual trunk route (VTRK): [Field]
- Zone for codec selection and bandwidth management (ZONE): [Field]
- Node ID of signaling server of this route (NODE): [Field]
- Protocol ID for the route (PCID): [Field]
- Print correlation ID in CDR for the route (ICDR): [Field]
- Integrated services digital network option (ISDN): [Field]
- Mode of operation (MODE): [Field]
- D channel number (DCH): [Field]
- Interface type for route (IFC): [Field]
- Private network identifier (PNI): [Field]
- Network calling name allowed (NCNA): [Field]
- Network call redirection (NCRD): [Field]
- Trunk route optimization (TRO): [Field]
- Recognition of DTIS ABCD FALT signal for ISL (FALT): [Field]
- Channel type (CHTY): [Field]
- Call type for outgoing direct dialed TR route (CTRP): [Field]
- Insert ESN access code (INAC): [Field]

Figure 31 – Route Configuration 1

Click on **Basic Route Options**, check the **North American toll scheme (NATL)** and **Incoming DID digit conversion on this route (IDC)** checkboxes. Enter **1** for both **Day IDC tree number** and **Night IDC tree number** as shown in **Figure 32**. Click on the **Submit** button.

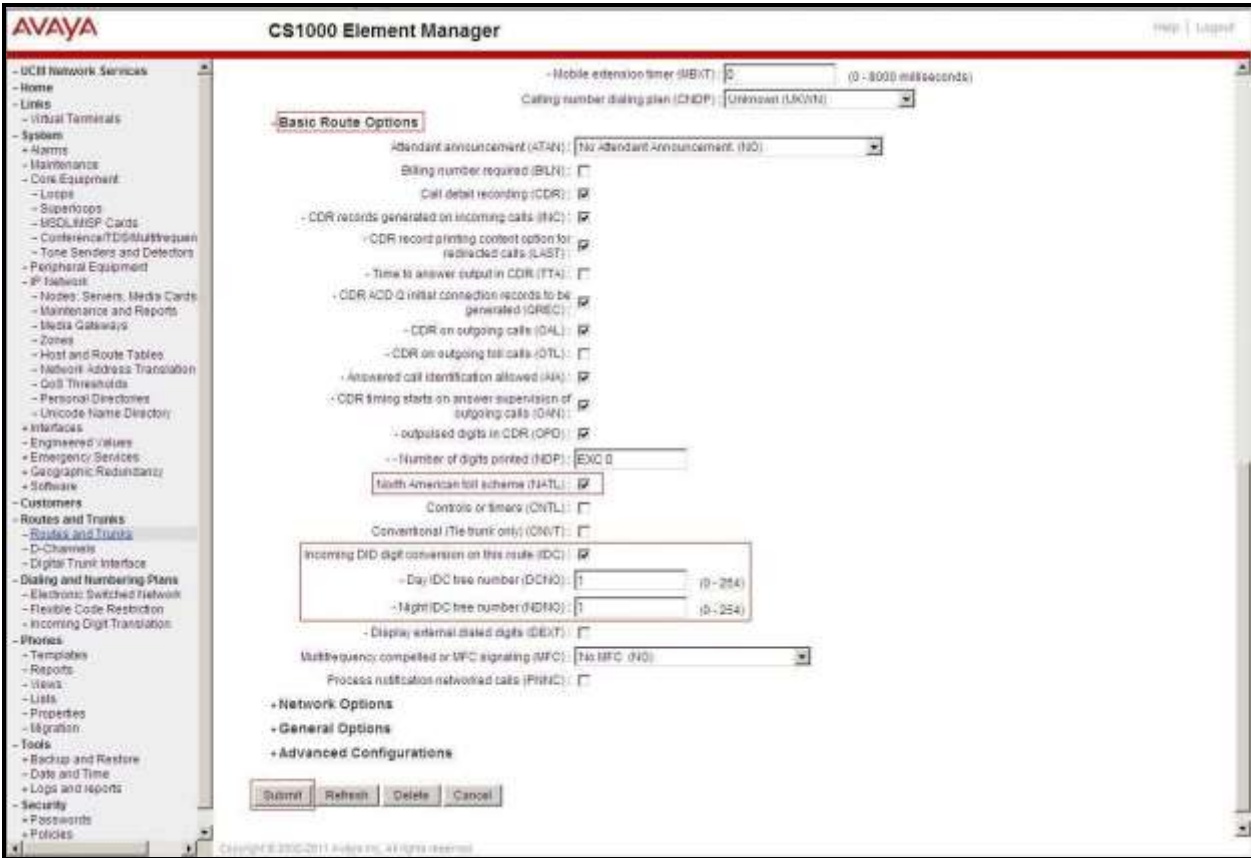


Figure 32 – Route Configuration 2

5.5.6. Administer Virtual Trunks

Select **Routes and Trunks** → **Route and Trunks** (not shown). The Route list is now updated with the newly added routes. In the example, the Route 100 was being added. Click on the **Add trunk** button as shown in **Figure 33**.



Figure 33 – Routes and Trunks

The **Customer 0, Route 100, Trunk 1 Property Configuration** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields. Media Security (sRTP) needs to be disabled at the trunk level by editing the **Class of Service** (CLS) at the bottom of the basic trunk configuration page. Click on the **Edit** button as shown in **Figure 34**.

Note: The Multiple trunk input number (MTINPUT) field may be used to add multiple trunks in a single operation, or repeat the operation for each trunk. In the sample configuration, 32 trunks were created.

- **Trunk data block:** IP Trunk (**IPTI**).
- **Terminal Number:** Available terminal number (Superloop 100 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.
- **Card Density:** 8D.
- **Start arrangement Incoming:** Select **Immediate (IMM)**.
- **Start arrangement Outgoing:** Select **Immediate (IMM)**.
- **Trunk group access restriction:** Desired trunk group access restriction level.
- **Channel ID for this trunk:** An available starting channel ID.

Figure 34 – New Trunk Configuration

For **Media Security**, select **Media Security Never (MSNV)**. Enter the values for the specified fields as shown in **Figure 35**. Scroll down to the bottom of the screen and click **Return Class of Service** and click on the **Save** button (shown in **Figure 34**).

Input Description	Input Value
- ACD Priority	ACD Priority not required (APN)
- Analog Semi-Permanent Connections	Analog Semi-Permanent Connections Denied (SPCD)
- ARF Supervised COT	
- Barring	
- Battery Supervised COT	
- Bus/Tone Supervised COT	
- Calling Line Identification	
- Calling party	Calling party Denied (CND)
- Central Office Ringback	
- Central Switchhook Flash	Central Switchhook Flash Denied (THFD)
- Dial Pulse	Digitone (DTN)
- DTR PAD value	
- Echo Canceling	Echo Canceling Denied (ECD)
- Hong Kong DTI	
- Loop Break Supervised COT	
- Make-break ratio for dial pulse	10 pulses per second (P10)
- Manual Incoming	Manual Incoming Denied (MID)
- Media Security	Media Security Never (MSNV)
- Network Hook Flash Over (HOF)	
- Potency	
- Priority	Low Priority (LPR)
- Restriction level	Unrestricted (LPR)
- Reversed Ear Piece	Reversed Ear Piece denied (REP)
- Short or long line	
- Transmission Class of Service	Non-Transmission Compensated (NTC)
- Warning Tone	Warning Tone Allowed (WTA)
- Reversed Ear Piece	Reversed Ear Piece denied (REP)
- ARF Supervised COT	

Return Class of Service Cancel

Figure 35 – Class of Service Configuration

5.5.7. Administer Calling Line Identification Entries

Select **Customers** on the left pane, then select **00 → ISDN and ESN Networking** (Not shown). Click on **Calling Line Identification Entries** as shown in **Figure 36**.

AVAYA CS1000 Element Manager

Managing: 10.09.07.04 Username: admin
Customer 00 → Customer Details → ISDN and ESN Networking

ISDN and ESN Networking

General Properties

Flexible trunk to trunk connection option:

Flexible orbiting prevention timer:

Country code: (it - 0000)

Core for processing the called number

National access code:

International access code:

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

Network option: ☒ Coordinated dialing plan routing

Integrated services digital network: ☒

Microsoft converged office dialing plan:

Private dialing plan for non-QD users: ☒ Coordinated dialing plan
☒ Uniform dialing plan

Calling Line Identification

Information for incoming/outgoing calls:

Stor: (it - 4096)

Country code: (it - 0000)

Core displayed as part of calling number

Calling Line Identification Entries

Save Cancel

Figure 36 – ISDN and ESN Networking

Click on **Add** as shown in **Figure 37**.

AVAYA CS1000 Element Manager

Managing: 10.09.07.04 Username: admin
Customer 00 → Customer Details → ISDN and ESN Networking → Calling Line Identification Entries

Calling Line Identification Entries

Search for CLID

Start range:

End range:

Search

Calling Line Identification Entries

Add Cancel

Refresh

Figure 37 – Calling Line Identification Entries

The add entry **0** screen is displayed. Enter or select the following values for the specified fields and retain the default values for the remaining fields. The **Edit Calling Line Identification** of the existing entry 0 is displayed as shown in **Figure 38**.

- **National Code:** Leave it blank.
- **Local Code:** Input prefix digits assigned by MTS SIP Trunk Service, in this case 6 digits – **204XXX**. This **Local Code** will be used for call display purpose for Call Type = Unknown.
- **Home Location Code:** Input the prefix digits assigned by MTS SIP Trunk Service, in this case 6 digits – **204XXX**. This **Home Location Code** will be used for call display purpose for Call Type = National (NPA).
- **Local Steering Code:** Input prefix digits assigned by MTS SIP Trunk Service, in this case 6 digits – **204XXX**. This **Local Steering Code** will be used for call display purpose for Call Type = Local Subscriber (NXX).
- **Use DN as DID:** YES.
- **Calling Party Name Display:** Uncheck **Roman characters**.

Click on the **Save** button as shown in **Figure 38**.

Figure 38 – Edit Calling Line Identification 0

5.5.8. Enable External Trunk to Trunk Transfer

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

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

```
>ld 15
CDB000
MEM AVAIL: (U/P): 33600126   USED U P: 8345621 954062   TOT: 45579868
DISK SPACE NEEDED: 1722 KBYTES
REQ: chg
TYPE: net

TYPE NET_DATA
CUST 0
OPT
...
TRNX YES  ← Enable transfer feature
EXTT YES  ← Enable external trunk to trunk Transfer
...
```

5.6. Administer Dialing Plans

5.6.1. Define ESN Access Codes and Parameters (ESN)

Select **Dialing and Numbering Plans** → **Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen as shown in **Figure 39**.

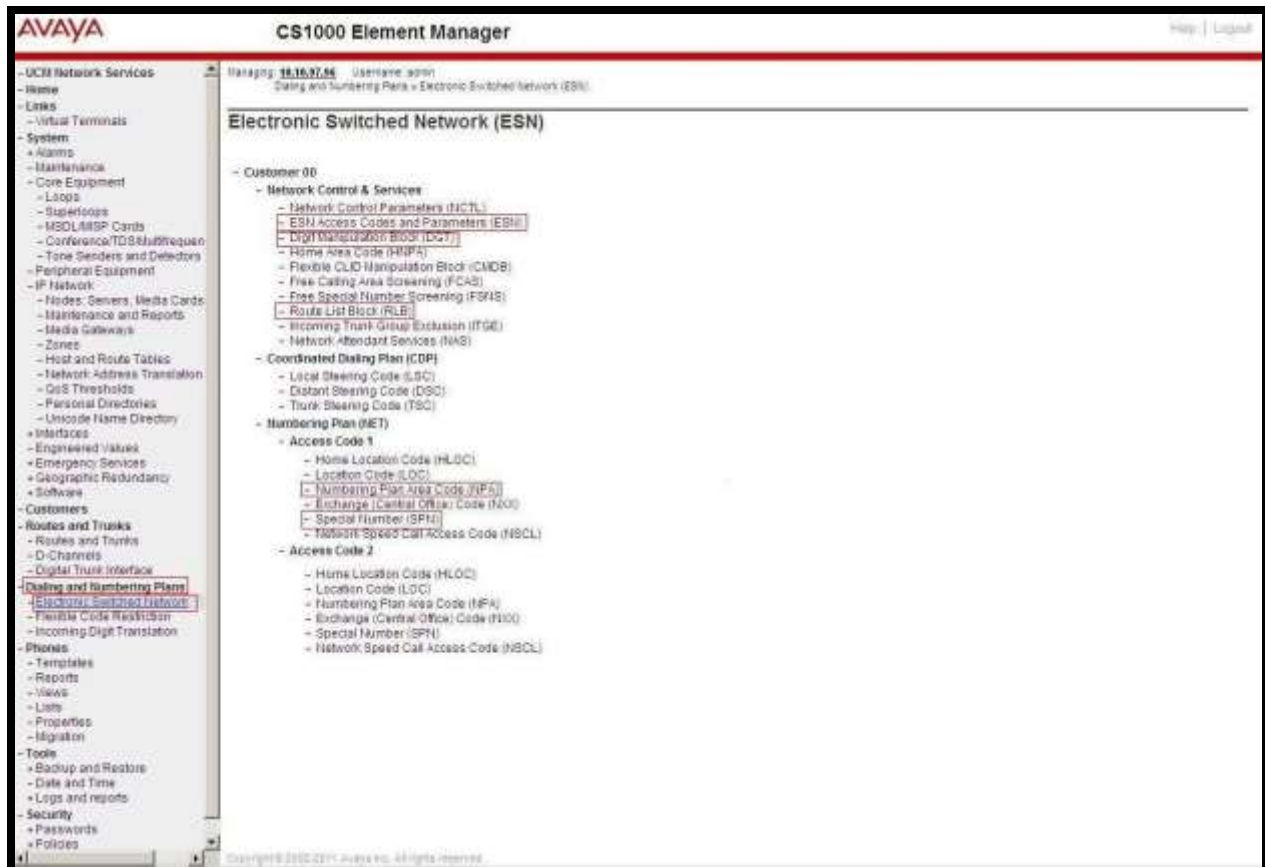


Figure 39 – ESN Configuration

On **Electronic Switched Network (ESN)** screen, select **ESN Access Codes and Parameters** to define **NARS/BARS Access Code 1** as shown in **Figure 40**.

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

Figure 40 – ESN Access Codes and Parameters

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

Log in to Call Server CLI (please refer to **Section 5.1.2** for more details), change Customer Net Data block by using **ld 15**.

```
>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 0
OPT
AC2 xNPA xSPN ← Set NPA, SPN not to associate to ESN Access Code 2
FNP
CLID
...
```

Verify Customer Net Data block by using **ld 21**.

```
>ld 21
PT1000

REQ: prt
TYPE: net
TYPE NET_DATA
CUST 0

TYPE NET_DATA
CUST 00
OPT RTA
AC1 INTL NPA SPN NXX LOC ← NPA, SPN are associated to ESN Access Code 1
AC2
FNP YES
...
```

5.6.3. Digit Manipulation Block Index (DMI)

The following steps show how to add DMI for the outbound call. There is an index, which was added to the Digit Manipulation Block List (14).

Select **Dialing and Numbering Plans → Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen as shown in **Figure 39**. Select **Digit Manipulation Block (DGT)**. The **Digit Manipulation Block List** is displayed as shown in **Figure 41**. In the **Please choose the** field, select an available **Digit Manipulation Block Index** from the drop-down list, and click on the **to Add** button.



Figure 41 – Add a DMI

The DMI_14 screen will open. In this testing, no leading digits are to be deleted, therefore, enter **0** for **Number of leading digits to be deleted** and select **NPA (NPA)** for **Call Type to be used by the manipulated digits** and then click on the **Submit** button as shown in **Figure 42**.

Figure 42 – DMI_14 Configuration

5.6.4. Route List Block (RLB) (RLB 14)

This session shows how to add a RLB associated with the DMI created in **Section 5.6.3**. Select **Dialing and Numbering Plans → Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen as shown in **Figure 39**. Select **Route List Block (RLB)**.

Enter an available value in the textbox for the **Please enter a route list index** (in this case **14**) and click on the **to Add** button as shown in **Figure 43**. The screen shown in **Figure 44** will open.

Figure 43 – Add a Route List Block

Enter the following values for the specified fields, and retain the default values for the remaining fields as shown in **Figure 44**. Scroll down to the bottom of the screen, and click on the **Submit** button (not shown).

- **Digit Manipulation Index: 14** (created in **Section 5.6.3**).
- **Incoming CLID Table: 0** (created in **Section 5.5.7**).
- **Route number: 100** (created in **Section 5.5.5**).

AVAYA CS1000 Element Manager

Managing: 10.10.10.10 Username: admin

Routing and Numbering Plans > Electronic Switched Network (ESN) > Customer CO > Network Control & Services > Route List Block > Route List Block > Data Entry of a Route List Block

Data Entry of a Route List Block

Route List Block Index: 14

General Properties

Entry Number for the Route List: 0

Indexes

Time of Day Schedule: 0

Facility Restriction Level: 0 (0 - 7)

Digit Manipulation Index: 14

ISL D-Channel Down Digit Manipulation Index: 0 (0 - 1000)

Free Calling Area Screening Index: 0

Free Special Number Screening Index: 0

Business Network Extension Route: 0

Incoming CLID Table: 0 (0 - 100)

Options

Local Termination entry: 0

Route Number: 100

Strip Conventional Signaling: 0

Use Tone Detector: 0

Conversion to LDN: 0

Expensive Route: 0

Strategy on Congestion: No Reroute (NRR)

OSG Alternate Routing Causes: OSG Alternate Routing Cause 1

Preferred Routing: Preferred Route 1

SDH Drop Back Policy: Drop Back Disabled (DBD)

ISDN Off-Hook Queuing Option: 0

Off-Hook Queuing Allowed: 0

Figure 44 – RLB_14 Route List Block Configuration

5.6.5. Inbound Call – Incoming Digit Translation Configuration

This section describes the configuration steps required in order to receive calls from the PSTN via the MTS SIP Trunk Service.

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 as shown in **Figure 45**.

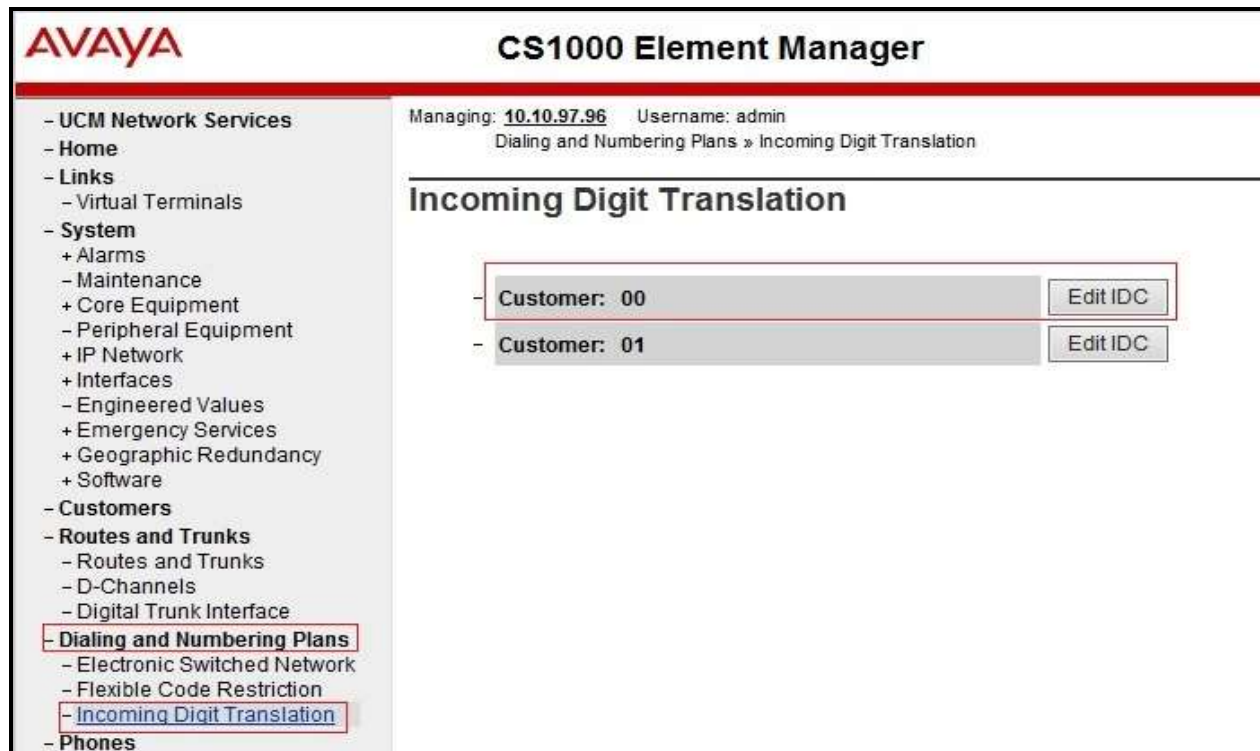


Figure 45 – Incoming Digit Translation

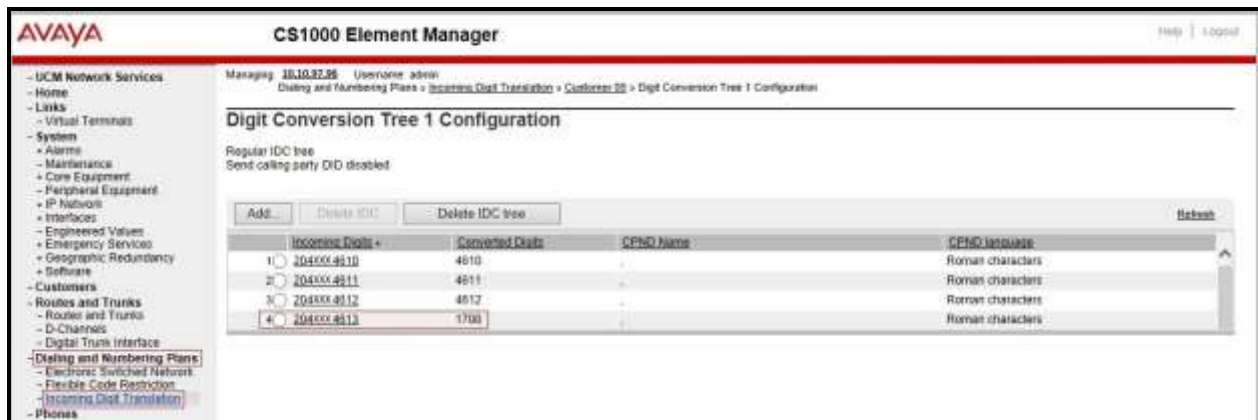
Click on the **New DCNO** to create the digit translation mapping. In this example, **Digit Conversion Tree Number 1** has been previously created as shown in **Figure 46**.



Figure 46 – Incoming Digit Conversion Property

Detailed configuration of the Digit Conversion Tree Configuration is shown in **Figure 47**. The **Incoming Digits** can be added to map to the Converted Digits which would be the associated CS1000 system phone DN. This **DCNO** has been assigned to route 100 as shown in **Figure 32**.

In the following configuration, the incoming call from the PSTN to DID with prefix **204XXX** will be translated to the associated DN with 4 digits. For testing purposes, DID number **204XXX4613** is translated to **1700** for voicemail testing or translated to 4613 for Mobile Service Access DN number.



	Incoming Digits	Converted Digits	CPND Name	CPND Language
1	204XXX4610	4610	-	Roman characters
2	204XXX4611	4611	-	Roman characters
3	204XXX4612	4612	-	Roman characters
4	204XXX4613	1700	-	Roman characters

Figure 47 – Digit Conversion Tree

5.6.6. Outbound Call - Special Number Configuration

There are special numbers which have been configured to be used for this testing such as: 0, 1800, 411, and so on.

Select **Dialing and Numbering Plans** → **Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen as show in **Figure 39**. Select **Special Number (SPN)**. Enter a SPN number and then click on the **to Add** button. **Figure 48** shows all the special numbers used for this testing.



Figure 48 – SPN numbers

5.6.7. Outbound Call - Numbering Plan Area (NPA)

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

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)** as shown in **Figure 39**. Enter the area code desired in the textbox and click on the **to Add** button. The 1303, 1416, and 1613 area codes were used in this configuration as shown in **Figure 49**.

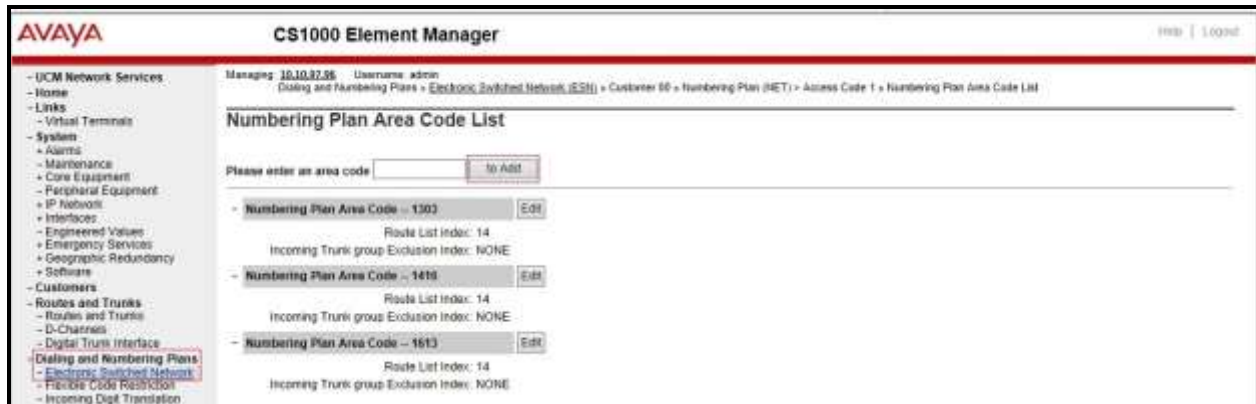


Figure 49 – Numbering Plan Area List

5.7. Administer a Phone

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

5.7.1. Phone creation

Refer to **Section 5.5.4** to create a Virtual Superloop **96** used for IP phones. Refer to **Section 5.4.1** to create a bandwidth zone **10** for IP phones. Log in to the Call Server Command Line Interface (please refer to **Section 5.1.2** for more detail). Create an IP phone by using **ld 11** as shown below:

```
>ld 11
REQ: new
TYPE: 2002p2
TN 96 0 0 2
DATE
PAGE
DES
MODEL_NAME
EMULATED
DES 2002P2 ← Describe information for IP Phone
TN 96 0 00 02 VIRTUAL ← Set Terminal Number for IP Phone
TYPE 2002P2
CDEN 8D
CTYP XDLC
```

CUST 0
 NUID
 NHTN
 CFG_ZONE **00010** ← Set bandwidth zone for IP phone
 CUR_ZONE 00010
 MRT
 ERL 12345
 ECL 0
 FDN
 TGAR 0
 LDN NO
 NCOS 7
 SGRP 0
 RNPG 0
 SCI 0
 SSU
 LNRS 16
 XLST
 SCPW
 SFLT NO
 CAC_MFC 0
 CLS UNR FBA WTA LPR MTD FNA HTA TDD CRPD
 MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
 POD SLKD CCSD SWD LNA CNDA
 CFTD SFA MRD DDV CNIA CDCA MSID DAPA BFED RCBF
 ICDD CDMD LLCN MCTD CLBD AUTU
 GPUD DPUD DNDD CFXA ARHD CLTD ASCD
 CPFA CPTA ABDD CFHD FICD NAID BUZZ AGRD MOAD
 UDI RCC HBTD AHD IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
 DRDD EXR0 USMD USRD ULAD CCBF RTDD RBDD RBHD PGND OCBF FLXD FTTC DNDY DNO3
 MCBN FDSD NOVD VOLA VOUD CDMR PRED RECD MCDD T87D SBMD
 MSNV FRA PKCH MWTD DVLD CROD ELCD
 CPND_LANG ENG
 HUNT
 PLEV 02
 PUID
 UPWD
 DANI NO
 AST
 IAPG 0
 AACS NO
 ITNA NO
 DGRP
 MLWU_LANG 0
 MLNG ENG
 DNDR 0
KEY 00 SCR 4610 0 MARP ← Set the position of DN 4610 to display on key 0 of the phone
 CPND
 CPND_LANG ROMAN
 NAME MTS_01 ← Set name to display
 XPLN 13
 DISPLAY_FMT FIRST, LAST
 01
 <Text removed for brevity>

5.7.2. Enable Privacy for the Phone

This section shows how to enable Privacy for a phone by changing its class of service (CLS). This feature cannot be enabled or disabled from the phone. By modifying the configuration of the phone created in **Section 5.7.1**, the display of the outbound call will be changed appropriately.

To hide the display number, set **CLS** (Class of Service) to **DDGD**. CS1000 will include “Privacy:id” in the SIP message header before sending it to MTS SIP Trunk Service.

```
>ld 11
REQ: chg
TYPE: 2002p2
TN 96 0 0 2
ECHG yes
ITEM CLS DDGD
...
```

To allow the display number, set **CLS** to **DDGA**. CS1000 will not send the Privacy header to MTS SIP Trunk Service.

```
>ld 11
REQ: chg
TYPE: 2002p2
TN 96 0 0 2
ECHG yes
ITEM CLS DDGA
...
```

5.7.3. Enable Call Forward for Phone

This section shows how to configure the Call Forward feature at the system and phone level.

Select **Customer → 00 → Call Redirection**. The Call Redirection page is shown in **Figure 50**.

- **Total redirection count limit: 0** (unlimited).
- **Call forward: Originating.**
- **Number of normal ringing cycles for CFNA: 3.**
- Click **Save** to save the configuration.

The screenshot shows the 'Call Redirection' configuration page in the Avaya CS1000 Element Manager. The left sidebar contains a navigation tree with categories like 'UCM Network Services', 'System', 'Customers', 'Routes and Trunks', 'Dialing and Numbering Plans', 'Phones', 'Tools', and 'Security'. The main content area is titled 'Call Redirection' and includes the following settings:

- Call redirection by day:** A checkbox that is unchecked.
- Days for day option 0, 1, 2, 3:** Four input fields, all empty.
- Redirection Holidays:** A section with a checkbox 'Do not disturb hunting' which is unchecked.
- Total redirection count limit:** A dropdown menu set to '0'.
- Options:** A group of checkboxes including 'Call forward reminder tone for 500/2500 sets', 'CFNA treatment for call waiting calls on a DDI', 'DID call to second degree busy treatment', 'Message center' (checked), and 'Prevention of reciprocal call forward' (checked).
- Call forward:** A radio button selection with 'Originating' selected and 'Forwarding' unselected.
- Number of normal ringing cycles for CFNA:** A section with three dropdown menus for 'Option 0', 'Option 1', and 'Option 2', all set to '3'.
- Number of distinctive ringing cycles for CFNA:** A section with three dropdown menus for 'Option 0', 'Option 1', and 'Option 2', all set to '3'.
- Calls routed to message center:** A section with three checkboxes: 'No answer DID calls' (unchecked), 'No answer non-DID calls' (unchecked), and 'DID calls to busy telephones' (unchecked).

At the bottom right of the page are 'Save' and 'Cancel' buttons.

Figure 50 – Call Redirection

To enable Call Forward All Call (CFAC) feature for a phone over SIP trunk, use **ld 11**. Change its **CLS** to **CFXA**, and **SFA**, then program the forward number on the phone set. The following is the configuration of a phone that has CFAC enabled with forwarding number **61303XXX9045**.

```
>ld 11
REQ: chg
TYPE: 2002P2
TN 96 0 0 2

ECHG yes
ITEM CLS CFXA SFA
ITEM key 19 CFW 16 61303XXX9045
```

To enable Call Forward Busy (CFB) feature for phone over SIP trunk, use **ld 11**. Change its **CLS** to **FBA**, **HTA**, and **SFA**, then program the forward number as **HUNT** and **FDN**. The following is the configuration of a phone with CFB enabled to forwarding number **61303XXX9045**.

```
>ld 11
REQ: chg
TYPE: 2002P2
TN 96 0 0 2
ECHG yes
ITEM CLS FBA HTA SFA
ITEM HUNT 61303XXX9045
ITEM FDN 61303XXX9045
```

To enable Call Forward No Answer (CFNA) feature for a phone over SIP trunk, use **ld 11**. Change its **CLS** to **FNA**, and **SFA**, then program the forward number as **HUNT** and **FDN**. The following is the configuration of a phone that has CFNA enabled with forwarding number **61303XXX9045**.

```
>ld 11
REQ: chg
TYPE: 2002P2
TN 96 0 0 2
ECHG yes
ITEM CLS FNA SFA
ITEM HUNT 61303XXX9045
ITEM FDN 61303XXX9045
```

6. Configure Avaya Aura[®] Session Manager

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

- SIP Domain.
- Logical/physical Location that can be occupied by SIP Entities.
- Adaptation module to perform dial plan manipulation.
- SIP Entities corresponding to CS1000, Avaya SBCE and Session Manager.
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities.
- Routing Policies, which define route destinations and control call routing between the SIP Entities.
- Dial Patterns, which specify dialed digits and govern which Routing Policy is used to service a call.

It may not be necessary to create all the items above when configuring 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. Avaya Aura® System Manager Login and Navigation

Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL “https://<ip-address>/SMGR”, where “<ip-address>” is the IP address of System Manager. At the **System Manager Log On** screen, enter an appropriate **User ID** and **Password** and press the **Log On** button (not shown). The initial screen shown below is then displayed.

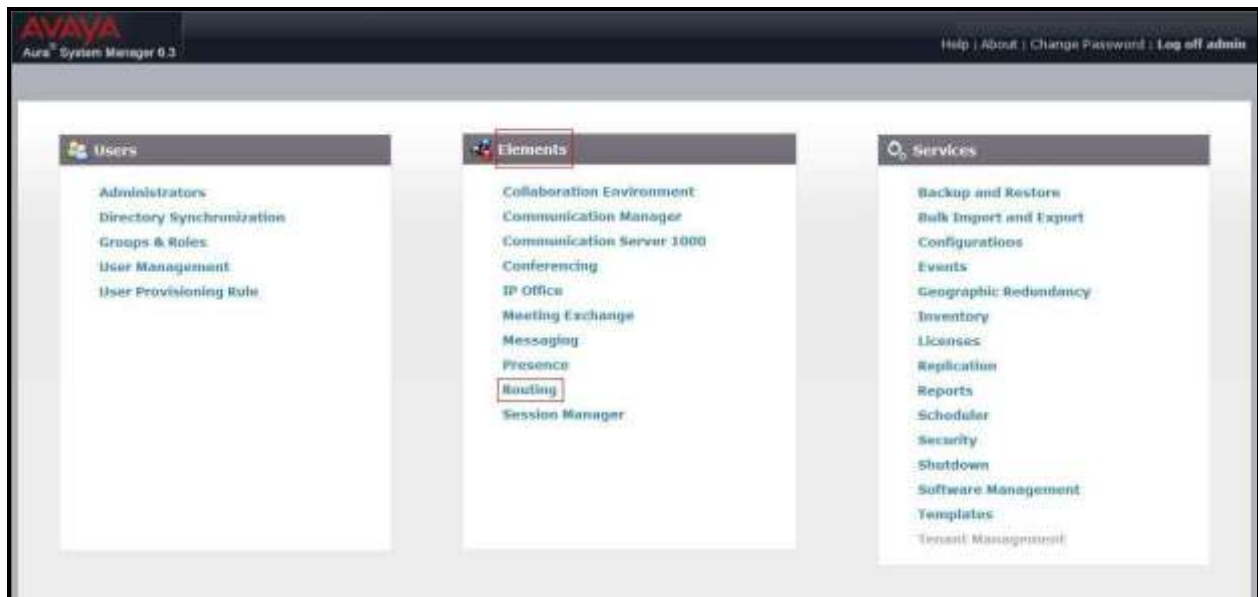


Figure 51 – System Manager Home Screen

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

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

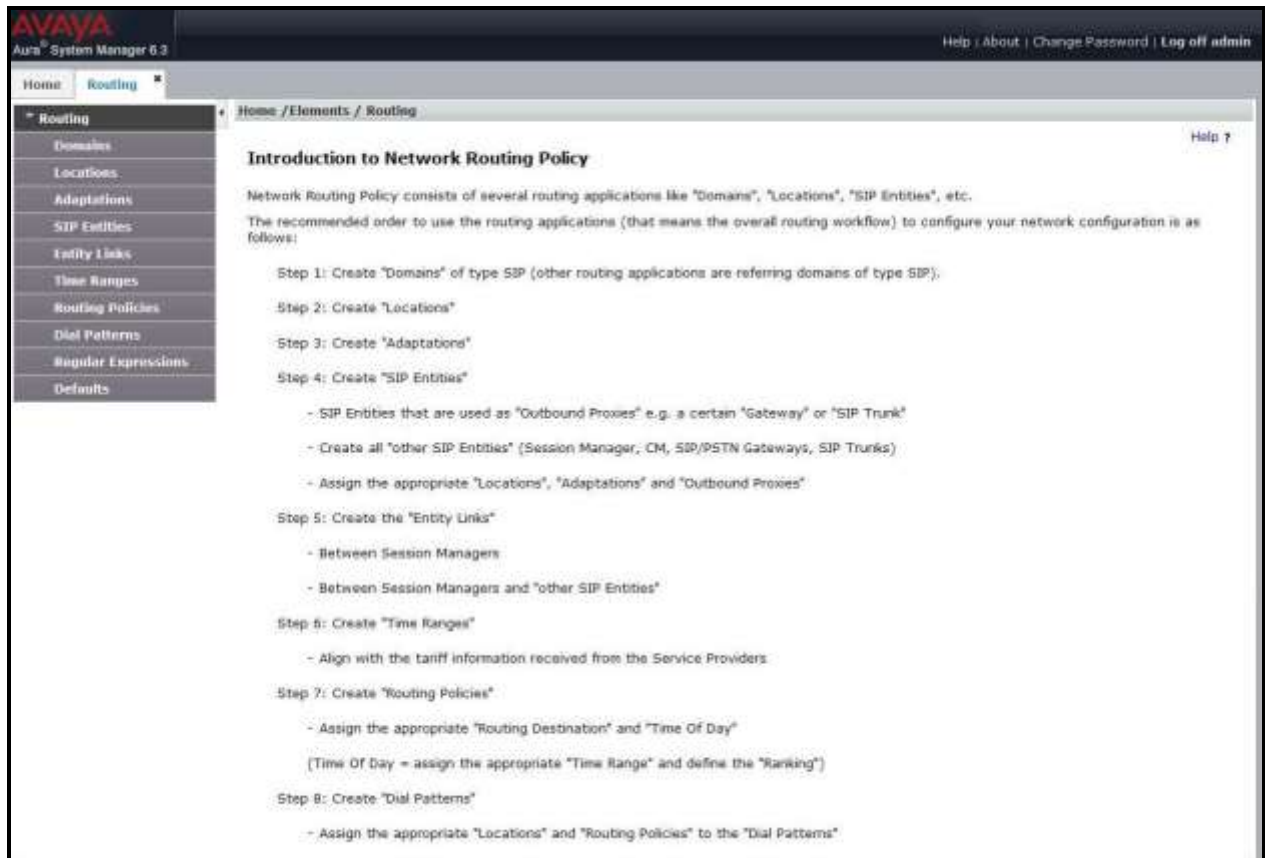


Figure 52 – Network Routing Policy

6.2. Specify SIP Domain

Create a SIP Domain for each domain of which Session Manager will need to be aware in order to route calls. For the compliance test, this includes the enterprise domain **bwdev7.com**.

Navigate to **Routing → Domains** in the left-hand navigation pane and click the **New** button in the right pane. In the new right pane that appears (not shown), fill in the following:

- **Name:** Enter the domain name (refer to **Section 5.5.2**).
- **Type:** Select **sip** from the pull-down menu.
- **Notes:** Add a brief description (optional).

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

The screen below shows the existing entry for the enterprise domain.



Figure 53 – Domain Management

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. A single Location was defined for the enterprise even though multiple subnets were used. The screens below show the addition of the Location named **Belleville**, which includes all equipment in the enterprise including CS1000, Session Manager and Avaya SBCE.

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 new right pane that appears (shown below), fill in the following:

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

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

AVAYA
Aura System Manager 6.3

Help | About | Change Password | Log off admin

Home Routing

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

Home / Elements / Routing / Locations

Location Details

General

Name: Belleville

Notes: GSSCP Belleville

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth: 10000000

Multimedia Bandwidth: 10000000

Audio Calls Can Take Multimedia Bandwidth: ☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 2000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): 2000 Kbit/Sec

* Minimum Multimedia Bandwidth: 64 Kbit/Sec

* Default Audio Bandwidth: 80 Kbit/Sec

Commit Cancel

Figure 54 – Location Configuration

In the **Location Pattern** section, click **Add** to enter IP Address patterns. The following patterns were used in testing:

- **IP Address Pattern:** 10.33.*, 10.10.97.*, 10.10.98.*

Location Pattern

Add Remove

3 Items Refresh Filter: Enable

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

Select: All, None

Commit Cancel

Figure 55 – IP Ranges Configuration

Click **Commit** to save.

Note that call bandwidth management parameters should be set per customer requirement.

6.4. Configure Adaptations

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

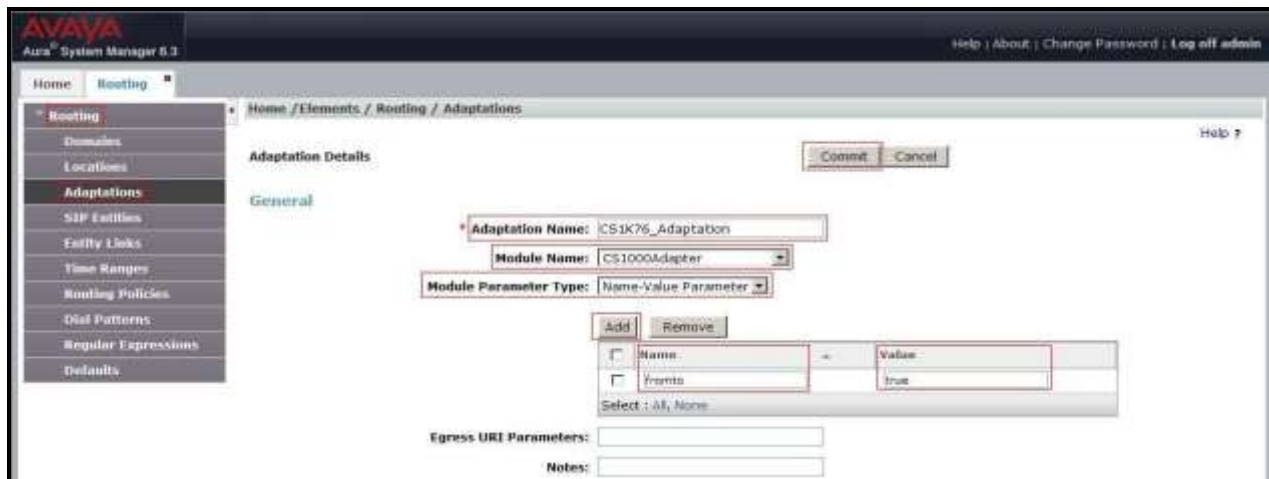


Figure 56 - CS1000 Adaptation

An Adaptation is configured to convert the History Info to Diversion Header and to remove MIME. To add a new adaptation, select **Routing → Adaptations**. Click the **New** button in the right pane (not shown). Enter an appropriate **Adaptation Name** to identify the adaptation. Select **DiversionTypeAdapter** from the **Module Name** drop-down menu. Select **Name-Value Parameter** from the **Module Parameter Type** drop-down menu. Click **Add** button to add **Name** as **MIME** and **Value** as **no**. Click the **Commit** button after changes are completed.

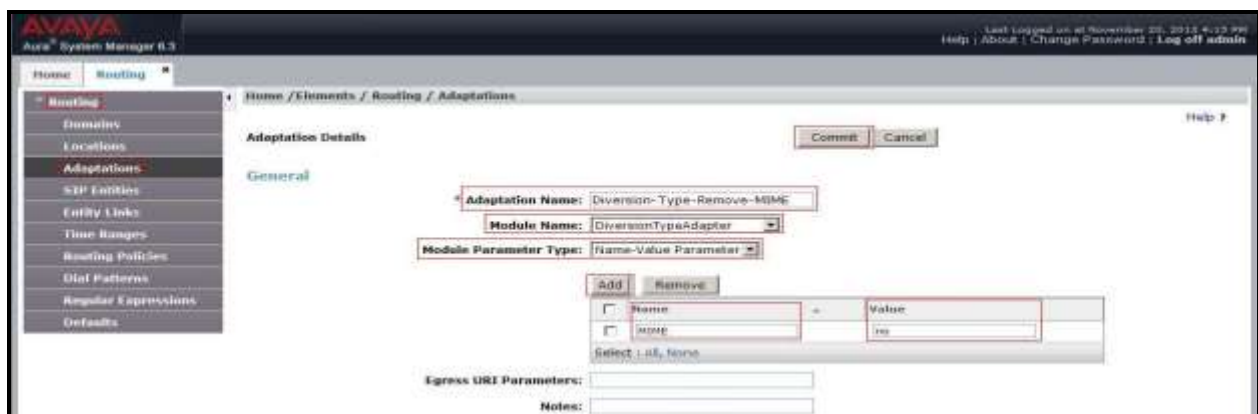


Figure 57 – Diversion Header Adaptation

6.5. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to Session Manager which includes CS1000 and Avaya SBCE. Navigate to **Routing → SIP Entities** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

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

- **Name:** Enter a descriptive name.
- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling.
- **Type:** Select **Session Manager** for Session Manager, **Other** for CS1000 and Avaya SBCE.
- **Adaptation:** This field is only present if **Type** is not set to **Session Manager**. If applicable, select the appropriate Adaptation module that will be applied to the SIP Entity being created.
- **Location:** Select the Location that applies to the SIP Entity being created. For the compliance test, all components were located in Location **Belleville**.
- **Time Zone:** Select the time zone for the Location above.

In this configuration, there are three SIP Entities.

- Session Manager SIP Entity
- Communication Manager 1000 SIP Entity
- Avaya Session Border Controller for Enterprise SIP Entity

6.5.1. Configure Session Manager SIP Entity

The following screen shows the addition of the Session Manager SIP Entity named **SM63**. The IP address of Session Manager's signaling interface **10.33.10.26** is entered for **FQDN or IP Address**. The **Location** field is set to **Belleville**. Select **Time Zone** as **America/Toronto**.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The left-hand navigation pane shows a tree structure with 'Routing' selected, and 'SIP Entities' highlighted under it. The main content area is titled 'SIP Entity Details' and 'General'. The form contains the following fields: 'Name' (SM63), 'FQDN or IP Address' (10.33.10.26), 'Type' (Session Manager), 'Notes' (SM RB.3), 'Location' (Belleville), 'Outbound Proxy' (empty), 'Time Zone' (America/Toronto), and 'Credential name' (empty). At the bottom, there is a 'SIP Link Monitoring' section with a dropdown menu set to 'Use Session Manager Configuration'. 'Commit' and 'Cancel' buttons are visible at the top right of the form area.

Figure 58 – Session Manager SIP Entity

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 listens for SIP requests.
- **Protocol:** Transport protocol to be used with this port.
- **Default Domain:** The default domain associated with this port. For the compliance test, this was the enterprise SIP Domain.

Defaults can be used for the remaining fields. Click the **Commit** button (not shown) to save.

The compliance test used port **5060** with **UDP** for connecting to CS1000 and Avaya SBCE.

Port

TCP Failover port:

TLS Failover port:

2 Items Refresh Filter: Enable

Port	Protocol	Default Domain	Notes
5060	UDP	bvwddev7.com	

Select : All, None

Figure 59 – Session Manager SIP Entity Port

6.5.2. Configure Communication Server 1000 SIP Entity

The following screen shows the addition of the CS1000 SIP Entity named **car3-ssg-carrier**. In order for Session Manager to send SIP service provider traffic on a separate Entity Link to CS1000, it is necessary to create a separate SIP Entity for CS1000, in addition to the one created at Session Manager installation, for use with all other SIP traffic within the enterprise. The **FQDN or IP Address** field is set to the IP address of CS1000 signaling Node **10.10.97.178**. Select **Type** as **Other**. Select **Adaptation** as **CS1K76_Adaptation** (created in **Section 6.4**). The **Location** field is set to **Belleville** which is the location that includes the subnet where CS1000 resides. Select **Time Zone** as **America/Toronto**.

AVAYA
Aura System Manager 6.3

Last Logged in at October 21, 2014 4:54 AM Log off admin

Home / Elements / Routing / SIP Entities

SIP Entity Details

General

Name: car3-ssg-carrier

FQDN or IP Address: 10.10.97.178

Type: Other

Notes:

Adaptation: CS1K76_Adaptation

Location: Belleville

Time Zone: America/Toronto

SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: none

CommProfile Type Preference:

Figure 60 – Communication Server 1000 SIP Entity

6.5.3. Configure Avaya SBCE SIP Entity

The following screen shows the SIP Entity for the Avaya SBCE named **SBCE**. The **FQDN or IP Address** field is set to the IP address of the Avaya SBCE's private network interfaces. Select **Type** as **Other**. Select **Adaptation** as **Diversion-Type-Remove-MIME** (created in **Section 6.4**). The **Location** field is set to **Belleville** which includes the subnet where Avaya SBCE resides. Select **Time Zone** as **America/Toronto**.

The following screenshot shows the SIP Entity for Avaya SBCE.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The left-hand navigation menu is expanded, showing the 'Routing' section with sub-items: Demos, Locations, Adaptations, SIP Entities (highlighted), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'SIP Entity Details' and 'General'. It contains the following fields and values:

- Name:** SBCE
- FQDN or IP Address:** 10.10.98.13
- Type:** Other (selected from a dropdown)
- Notes:** (empty text field)
- Adaptation:** Diversion-Type-Remove-MIME (selected from a dropdown)
- Location:** Belleville (selected from a dropdown)
- Time Zone:** America/Toronto (selected from a dropdown)
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text field)
- Call Detail Recording:** none (selected from a dropdown)
- CommProfile Type Preference:** (empty dropdown)

At the top right of the main area, there are 'Commit' and 'Cancel' buttons. The top status bar shows 'Last Logged on at January 13, 2015 7:48 AM' and a 'Log off admin' link.

Figure 61 – Avaya SBCE SIP Entity

6.6. Add Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. Two Entity Links were created: one to CS1000 and one to Avaya SBCE.

To add an Entity Link, navigate to **Routing → Entity Links** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager being used.
- **Protocol:** Select the transport protocol used for this link.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end.
- **SIP Entity 2:** Select the name of the other system as defined in **Section 6.5**.
- **Port:** Port number on which the other system receives SIP requests from the Session Manager.
- **Connection Policy:** Select **trusted**. Note: If this box is not selected as trusted, calls from the associated SIP Entity specified in **Section 6.5** will be denied.

Click **Commit** to save.

The following screen illustrates the Entity Link to the CS1000. The protocol and ports defined here must match the values used for the CS1000 signaling in **Section 5.5.2**.



Figure 62 – Communication Server 1000 Entity Link

The following screen illustrates the Entity Link to Avaya SBCE. The protocol and ports defined here must match the values used for Avaya SBCE mentioned in **Section 7.2.4**, later in this document.



Figure 63 – Avaya SBCE Entity Link

6.7. Configure Time Ranges

Time Ranges are configured for time-based routing. In order to add Time Ranges, select **Routing** → **Time Ranges** in the left-hand navigation pane and then click **New** button in the right pane.

The Routing Policies shown subsequently will use the **24/7** range since time-based routing was not the focus of these Application Notes.



Figure 64 – Time Ranges

6.8. 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: one for the CS1000 and one for Avaya SBCE. To add a Routing Policy, navigate to **Routing** → **Routing Policies** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown on the next page), fill in the following:

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

- **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 screen shows the **Routing Policy Details** for the policy named **MTS_Inbound_To_CS1K76** associated with incoming PSTN calls from MTS SIP Trunk Service to the CS1000. Observe the **SIP Entity as Destination** is the entity named **car3-ssg-carrier**.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar contains a navigation menu with options: Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies (selected), Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Routing Policy Details' and includes a 'General' tab. The 'Name' field is 'MTS_Inbound_To_CS1K76'. The 'Disabled' checkbox is unchecked. The 'Retries' field is '0'. The 'Notes' field is empty. Below this, the 'SIP Entity as Destination' section shows a table with one entry: 'car3-ssg-carrier' with FQDN or IP Address '10.10.97.178' and Type 'Other'.

Name	FQDN or IP Address	Type	Notes
car3-ssg-carrier	10.10.97.178	Other	

Figure 65 – Routing to Communication Server 1000

The following screen shows the **Routing Policy Details** for the policy named **MTS_Outbound_To_SP4**. This is associated with outgoing calls from the CS1000 to the PSTN via MTS SIP Trunk Service, through Avaya SBCE. Observe the **SIP Entity as Destination** is the entity named **SBCE**.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar contains a navigation menu with options: Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies (selected), Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Routing Policy Details' and includes a 'General' tab. The 'Name' field is 'MTS_Outbound_To_SP4'. The 'Disabled' checkbox is unchecked. The 'Retries' field is '0'. The 'Notes' field is empty. Below this, the 'SIP Entity as Destination' section shows a table with one entry: 'SBCE' with FQDN or IP Address '10.10.98.25' and Type 'Other'.

Name	FQDN or IP Address	Type	Notes
SBCE	10.10.98.25	Other	

Figure 66 – Routing to Avaya SBCE

6.9. Add Dial Patterns

Dial Patterns are used to route calls through Session Manager. For the compliance test, Dial Patterns were configured to route calls from the CS1000 to MTS SIP Trunk Service and vice versa. Dial Patterns define which Route Policy will be selected as route destination 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-hand navigation pane and click on the **New** button in the right pane (not shown). In the new right pane that appears (shown below), fill in the following:

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

- **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. Other Dial Patterns (e.g., 1800, 411, etc.) were similarly defined.

The following screen shows that outbound dialed numbers with a maximum of 11 digits that begin with **1303** and have a destination SIP Domain of **bwvdev7.com** use the Routing Policy Names **MTS_Outbound_To_SP4** as defined in **Section 6.8**.

Avaya Aura System Manager 6.3

Home / Elements / Routing / Dial Patterns

Dial Pattern Details:

General

* Pattern: 1303

* Min: 11

* Max: 11

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: bwvdev7.com

Notes: MTS Outbound Calls

Originating Locations and Routing Policies

Add Remove

1 Item

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
-ALL-		MTS_Outbound_To_SP4	0	<input type="checkbox"/>	SSCE	

Select: All, None

Figure 67 – Dial Pattern 1303

Note that the above Dial Pattern did not restrict outbound calls to specific US/Canada area codes. In real deployments, appropriate restriction can be exercised per customer business policies.

The following screen shows that inbound 10-digit numbers that start with **204** use Routing Policy Name **MTS_Inbound_To_CS1K76** as defined in **Section 6.8**. This Dial Pattern matches the DID numbers assigned to the enterprise by MTS SIP Trunk Service.

Dial Pattern Details

General

* Pattern: 204

* Min: 3

* Max: 10

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: bvwdev7.com

Notes: MTS Inbound Calls

Originating Locations and Routing Policies

Add Remove

1 Item

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
Seleville		MTS_Inbound_To_CS1K76	0	<input type="checkbox"/>	car3-asg-carrier	

Select: All, None

Figure 68 – Dial Pattern 647

The following screen illustrates a list of dial patterns used for inbound and outbound calls between the enterprise and the PSTN.

Dial Patterns

New Edit Delete Duplicate More Actions

45 Items

Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Notes
0	1	11	<input type="checkbox"/>			bvwdev7.com	MTS Outbound Calls
011	3	15	<input type="checkbox"/>			bvwdev7.com	MTS Outbound Calls
1303	11	11	<input type="checkbox"/>			bvwdev7.com	MTS Outbound Calls
1410	11	11	<input type="checkbox"/>			bvwdev7.com	MTS Outbound Calls
1613	11	11	<input type="checkbox"/>			bvwdev7.com	MTS Outbound Calls
1800	11	11	<input type="checkbox"/>			bvwdev7.com	MTS Outbound Calls
204	3	10	<input type="checkbox"/>			bvwdev7.com	MTS Inbound Calls
411	3	3	<input type="checkbox"/>			bvwdev7.com	MTS Outbound Calls

Select: All, None

Page: 1 of 3

Figure 69 – Dial Pattern List

7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of Avaya SBCE necessary for interoperability with the Session Manager and MTS SIP Trunk Service.

Avaya elements reside on the Private side and the MTS SIP Trunk Service resides on the Public side of the network, as illustrated in **Figure 1**.

Note: The following section assumes that Avaya SBCE has been installed and that network connectivity exists between the systems. For more information on Avaya SBCE, see relevant product documentation references in **Section 11** of these Application Notes.

7.1. Log into the SBCE

Access the web interface by typing “<https://x.x.x.x/sbc/>” (where x.x.x.x is the management IP of the Avaya SBCE).

Enter the **Username** and **Password**.



The image shows the login page for the Avaya Session Border Controller for Enterprise. On the left, there is a large red 'AVAYA' logo and the text 'Session Border Controller for Enterprise'. On the right, under the heading 'Log In', there are two input fields: 'Username:' with the value 'ucsec' and 'Password:' with a masked password represented by dots. Below these fields is a 'Log In' button. Further down, there is a disclaimer text: 'This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws.' followed by a monitoring notice: 'The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.' and a compliance statement: 'All users must comply with all corporate instructions regarding the protection of information assets.' At the bottom, it says '© 2011 - 2013 Avaya Inc. All rights reserved.'

Figure 70 – Avaya SBCE Login

7.2. Global Profiles

When selected, Global Profiles allows for configuration of parameters across all Avaya SBCE appliances.

7.2.1. Configure Server Interworking - Avaya Site

Server Interworking allows to configure and manage various SIP call server-specific capabilities such as call hold, 180 handling, etc.

From the menu on the left-hand side, select **Global Profiles → Server Interworking**

- Select **avaya-ru** in Interworking Profiles.
- Click **Clone**.
- Enter **Clone Name: SM63** and click **Finish** (not shown).

From the list of **Interworking Profiles**, click on **SM63** to edit.

- On the **General** tab, set **T.38 Support** as **Yes** (MTS supports Fax T.38 during the compliance testing). Other options can be left at default.
- On the **Timers**, **URI Manipulation**, **Header Manipulation** and **Advanced** tabs, all options can be left at default. Click **Finish** (not shown).

The following screen shows that Session Manager server interworking profile (named: **SM63**) was added.

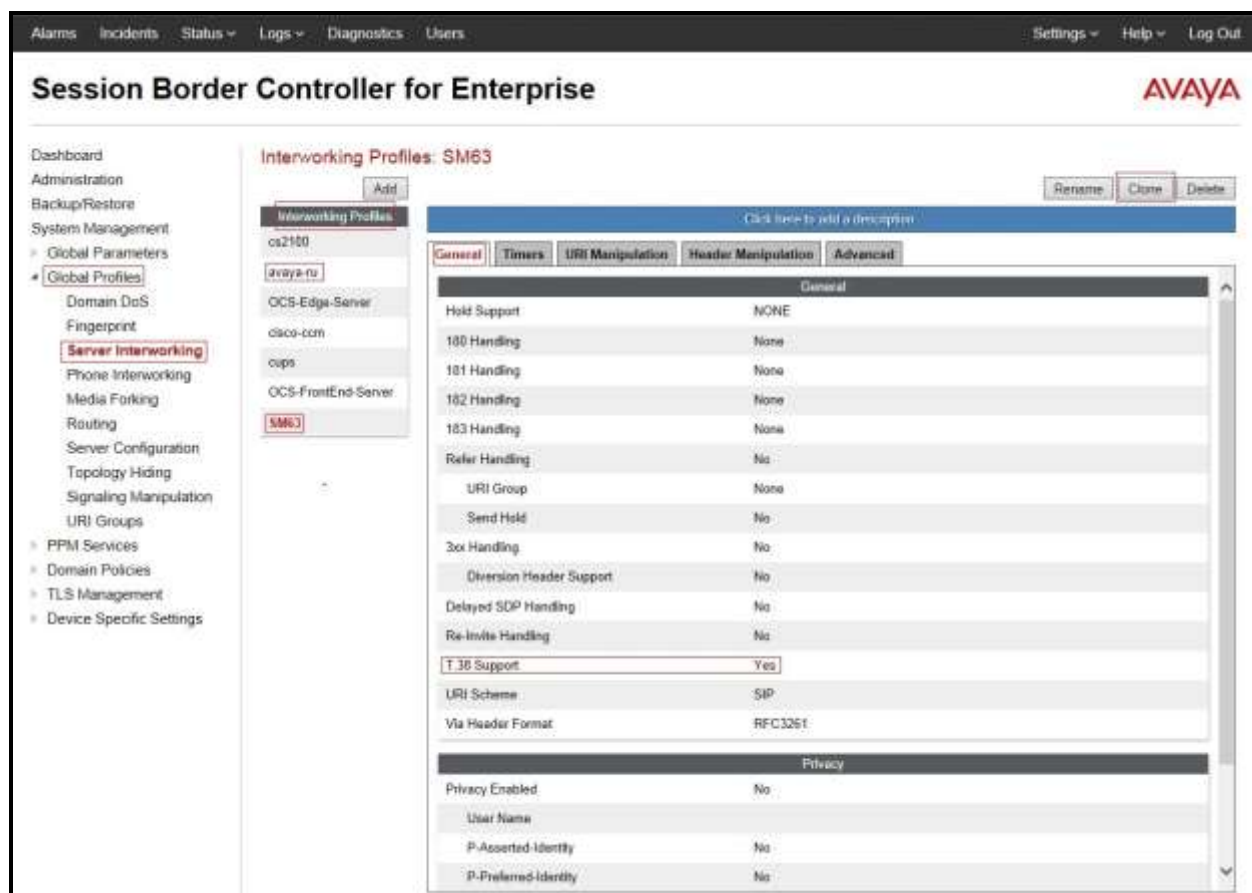


Figure 71 - Server Interworking – Avaya site

7.2.2. Configure Server Interworking – MTS Site

From the menu on the left-hand side, select **Global Profiles** → **Server Interworking** and click **Add** as highlighted below.

- Enter **Profile Name: SP3**.
- On the **General** tab, set **T.38 Support** as **Yes** (MTS supports Fax T.38 during the compliance testing). Other options can be left at default.
- On the **Timers**, **URI Manipulation**, **Header Manipulation** and **Advanced** tabs, all options can be left at default. Click **Finish** (not shown).

The following screen shows that the MTS SIP Trunk Service interworking profile (named **SP3**) was added.

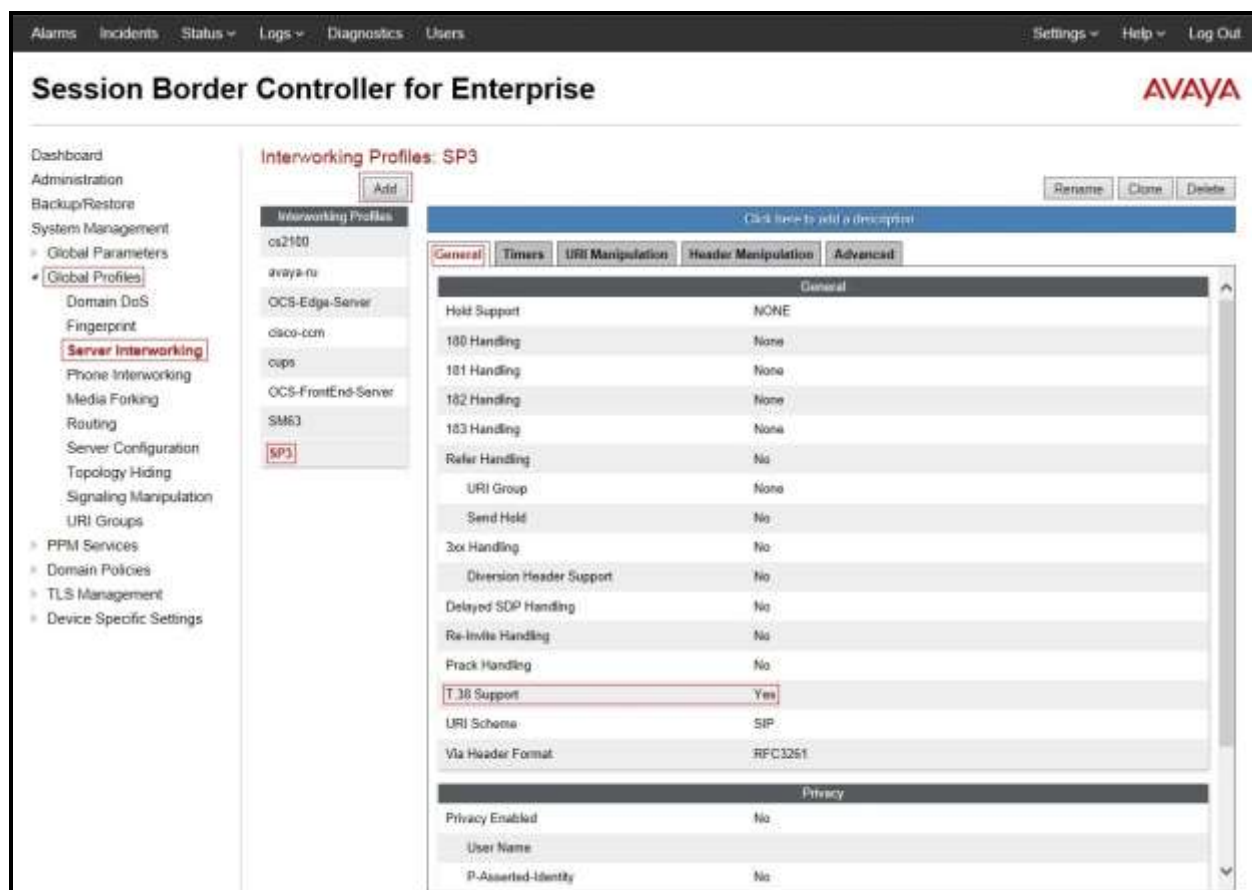


Figure 72 - Server Interworking – MTS site

7.2.3. Configure Signaling Manipulation

The SIP signaling header manipulation feature adds the ability to add, change and delete any of the headers and other information in a SIP message.

- Select **Global Profiles** from the menu on the left-hand side.
- Select the **Signaling Manipulation**.
- Select **Add**. Enter **Script Title: SP3**. In the script editing window, enter the text exactly as shown in the screenshot below to remove user “avayapbx1” in SIP URI in Request-Line Header of the OPTIONS sending from MTS SIP Trunking.
- Click **Save** (not shown).

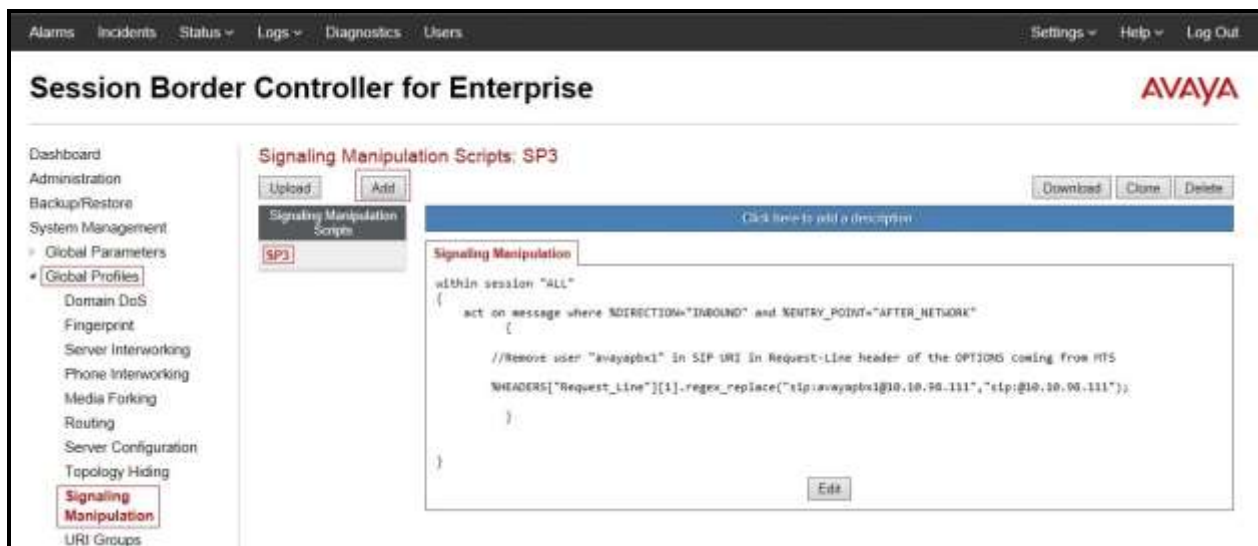


Figure 73 – Signaling Manipulation

7.2.4. Configure Server – Session Manager

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow one to configure and manage various SIP call server-specific parameters such as UDP port assignment, IP Server type, heartbeat signaling parameters and some advanced options.

From the menu on the left-hand side, select **Global Profiles** → **Server Configuration** and click **Add** as highlighted below.

Enter **Profile Name**: **SM63**.

On **General** tab, enter the following:

- **Server Type**: Select **Call Server**.
- **IP Address/FQDN**: **10.33.10.26** (Session Manager IP Address).
- **Port**: **5060**.
- **Transport**: **UDP**.
- Click **Finish** (not shown).



Figure 74 – Session Manager - General Server Configuration

On the **Advanced** tab:

- Select **SM63** for **Interworking Profile** (Refer to **Section 7.2.1**).
- Click **Finish** (not shown).



Figure 75 – Session Manager - Advanced Server Configuration

7.2.5. Configure Server – MTS

From the menu on the left-hand side, select **Global Profiles** → **Server Configuration** and click **Add** as highlighted below.

Enter **Profile Name**: **SP3**.

On **General** tab, enter the following:

- **Server Type**: Select **Trunk Server**.
- **IP Address/FQDN**: **192.168.168.20** (MTS Signaling Server IP Address).
- **Port**: **5060**.
- **Transport**: **UDP**.
- Click **Finish** (not shown).



Figure 76 – MTS - General Server Configuration

On the **Authentication** tab, click on **Edit** button to enter the following:

- Check **Enable Authentication** option.
- **User Name:** avayapbx1 (MTS provided this user name during this compliance testing).
- **Realm:** Blank.
- **Password:** ***** (MTS provided this password during this compliance testing).
- **Confirm Password:** ***** (MTS provided this password during this compliance testing).
- Click **Finish** button.

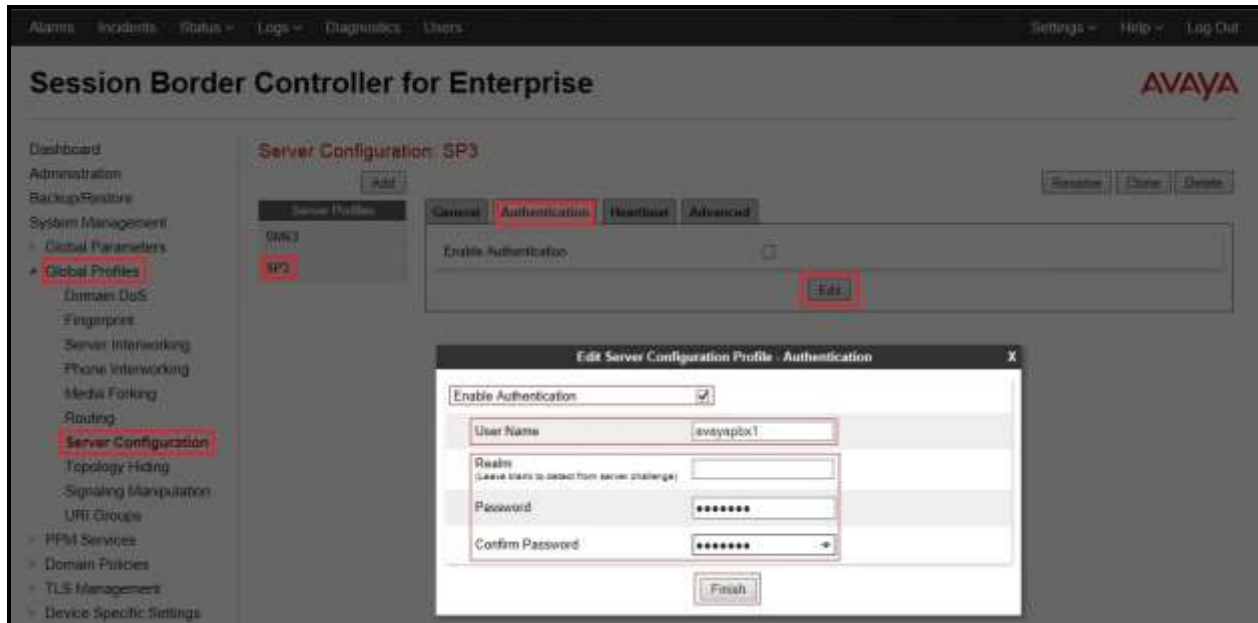


Figure 77 - MTS - Authentication Server Configuration

On the **Heartbeat** tab, click on **Edit** button to enter the following:

- Check **Enable Heartbeat** option.
- **Method: REGISTER**. (MTS supported REGISTER during the compliance testing).
- **Frequency: 60 seconds**.
- **From URI: avayapbx1@avaya.mts.ca**.
- **To URI: avayapbx1@avaya.mts.ca**.
- Click **Finish** button.

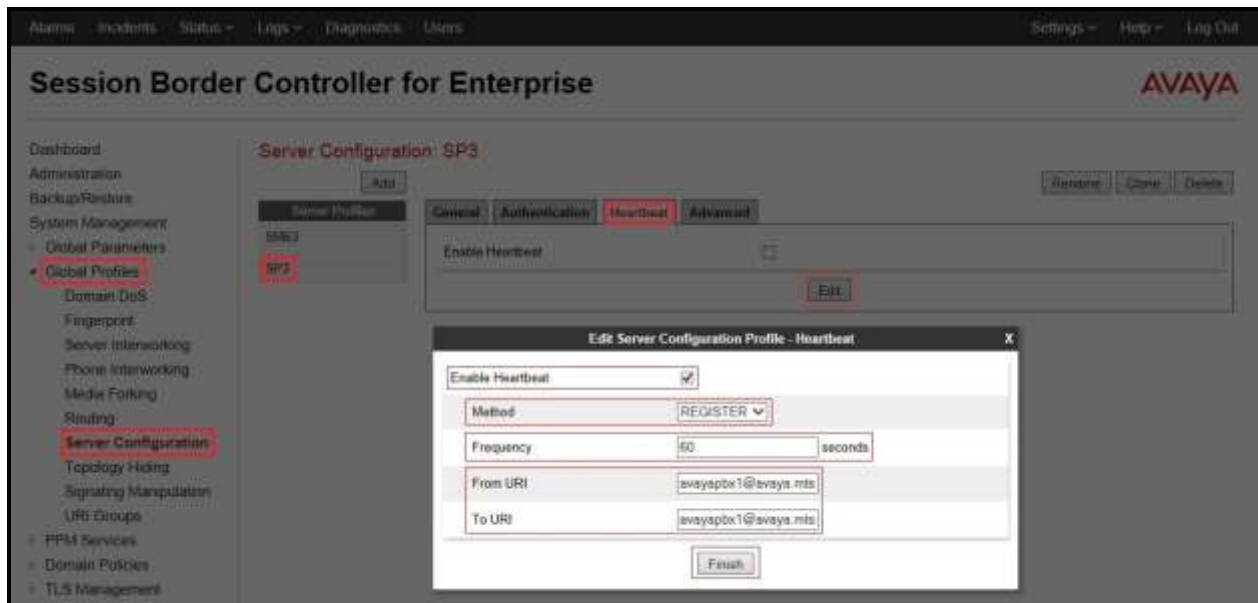


Figure 78 - MTS - Heartbeat Server Configuration

On the **Advanced** tab, click on **Edit** button to enter the following:

- **Interworking Profile: SP3** (Refer to **Section 7.2.2**).
- **Signaling Manipulation Script: SP3** (Refer to **Section 7.2.3**).
- Click **Finish** button.

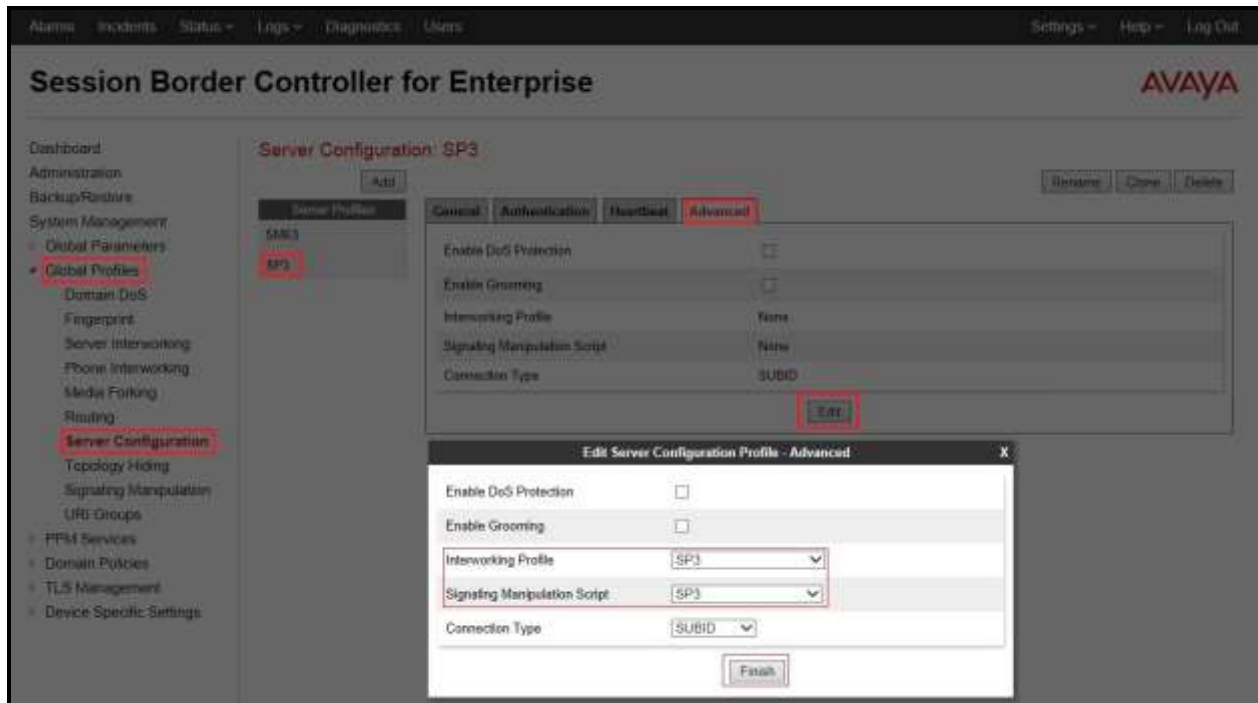


Figure 79 - MTS - Advanced Server Configuration

7.2.6. Configure Routing – Avaya Site

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.

From the menu on the left-hand side, select **Global Profiles** → **Routing** and click **Add** as highlighted below.

Enter **Profile Name: SP3_To_SM63** (not shown).

- **URI Group: ***.
- **Load Balancing: Priority.**
- Check **Next Hop Priority**.
- Click **Add** button to add a Next-Hop Address
- **Priority/Weight: 1.**
- **Server Configuration: SM63** (Refer to **Section 7.2.4**).
- **Next Hop Address: 10.33.10.26:5060 (UDP)** (Session Manager IP address).
- Click **Finish** button.

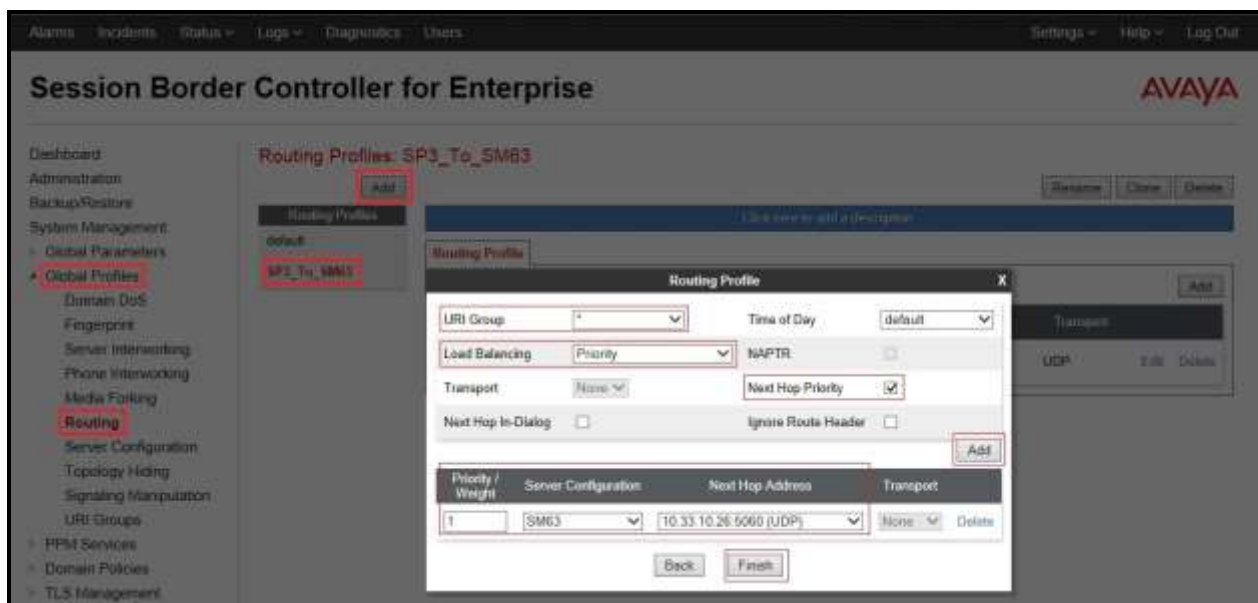


Figure 80 - Routing to Avaya

7.2.7. Configure Routing – MTS Site

The Routing Profile allows one to manage parameters related to routing SIP signaling messages.

From the menu on the left-hand side, select **Global Profiles** → **Routing** and click **Add** as highlighted below.

Enter **Profile Name: SM63_To_SP3** (not shown).

- **URI Group: ***
- **Load Balancing: Priority.**
- Check **Next Hop Priority**.
- Click **Add** button to add a Next-Hop Address
- **Priority/Weight: 1.**
- **Server Configuration: SP3** (Refer to Section 7.2.5).
- **Next Hop Address: 192.168.168.20:5060 (UDP)** (MTS Signaling Server IP address).
- Click **Finish** button.

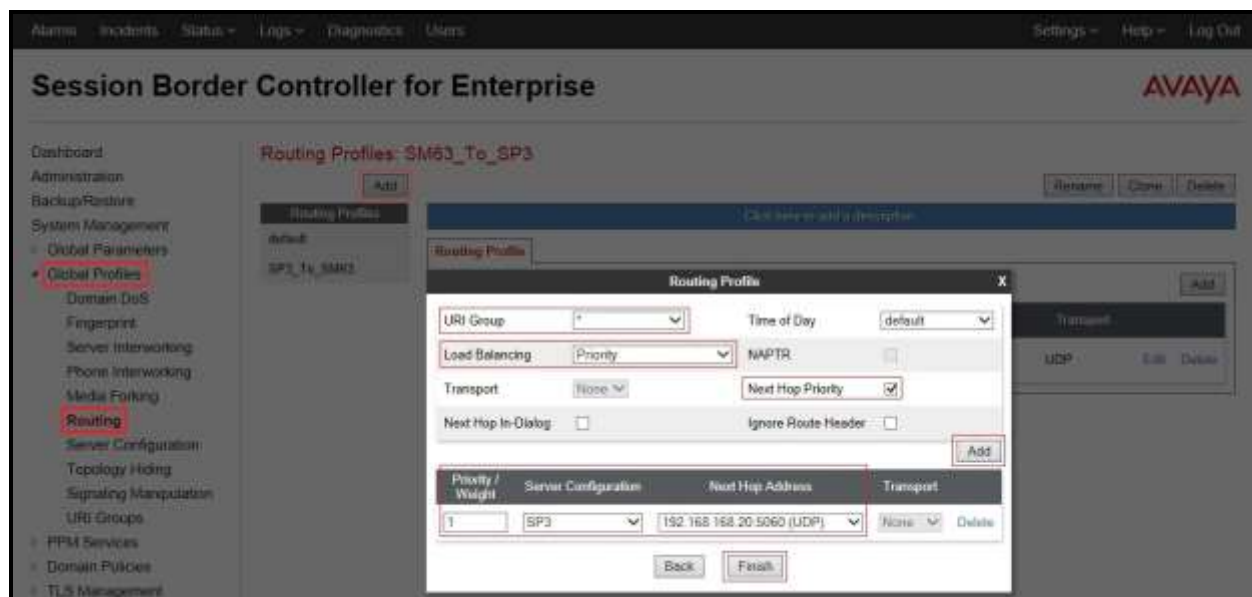


Figure 81 - Routing to MTS

7.2.8. Configure Topology Hiding – Avaya Site

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

From the menu on the left-hand side, select **Global Profiles** → **Topology Hiding**.

Select **default** under **Topology Hiding Profiles**, and click **Clone**. Enter **Clone Name**: **SP3_To_SM63**. Click **Finish** (not shown).

Select **SP3_To_SM63** under **Topology Hiding Profiles**, and click **Edit**.

- For the Header **To**,
 - In the **Criteria** column select **IP/Domain**.
 - In the **Replace Action** column select: **Overwrite**.
 - In the **Overwrite Value** column: **bvwdev7.com**.
- For the Header **Request-Line**,
 - In the **Criteria** column select **IP/Domain**.
 - In the **Replace Action** column select: **Overwrite**.
 - In the **Overwrite Value** column: **bvwdev7.com**.
- For the Header **From**,
 - In the **Criteria** column select **IP/Domain**.
 - In the **Replace Action** column select: **Overwrite**.
 - In the **Overwrite Value** column: **bvwdev7.com**.

Click **Finish** (not shown).

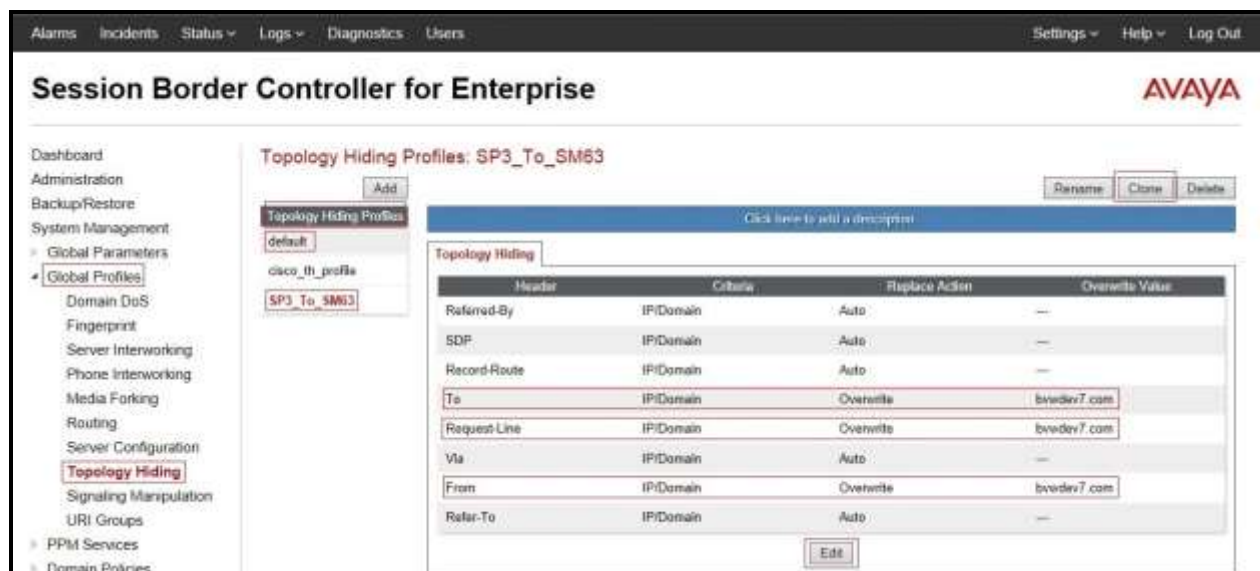


Figure 82 - Topology Hiding Session Manager

From the menu on the left-hand side, select **Global Profiles** → **Topology Hiding**.

Select **SM63_To_SP3** under **Topology Hiding Profiles**, and click **Edit**.

- Click **Finish** (not shown).



7.3. Domain Policies

The Domain Policies feature allows one to configure, apply, and manage various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise. These criteria can be used to trigger different policies which will apply on call flows, change the behavior of the call, and make sure the call does not violate any of the policies. There are default policies available to use, or one can create a custom domain policy.

Create End Point Policy Groups

The End Point Policy Group feature allows one to create Policy Sets and Policy Groups. A Policy Set is an association of individual, SIP signaling-specific security policies (rule sets): application, border, media, security, signaling, and ToD, each of which was created using the procedures contained in the previous sections.) A Policy Group is comprised of one or more Policy Sets. The purpose of Policy Sets and Policy Groups is to increasingly aggregate and simplify the application of SBCE security features to very specific types of SIP signaling messages traversing through the enterprise.

From the menu on the left-hand side, select **Domain Policies → End Point Policy Groups**.

- Select **Add**.
- Enter **Group Name: SM63_SP3_PolicyG**.
 - **Application Rule: default.**
 - **Border Rule: default.**
 - **Media Rule: default-low-med.**
 - **Security Rule: default-med.**
 - **Signaling Rule: default.**
 - **Time of Day: default.**
- Select **Finish** (not shown).



Figure 84 – Session Manager - End Point Policy Group

From the menu on the left-hand side, select **Domain Policies → End Point Policy Groups**.

- Select **Add**.
- Enter **Group Name: SP3_PolicyG**.
 - **Application Rule: default.**
 - **Border Rule: default.**
 - **Media Rule: default-low-med.**
 - **Security Rule: default-med.**
 - **Signaling Rule: default.**
 - **Time of Day: default.**
- Select **Finish** (not shown).

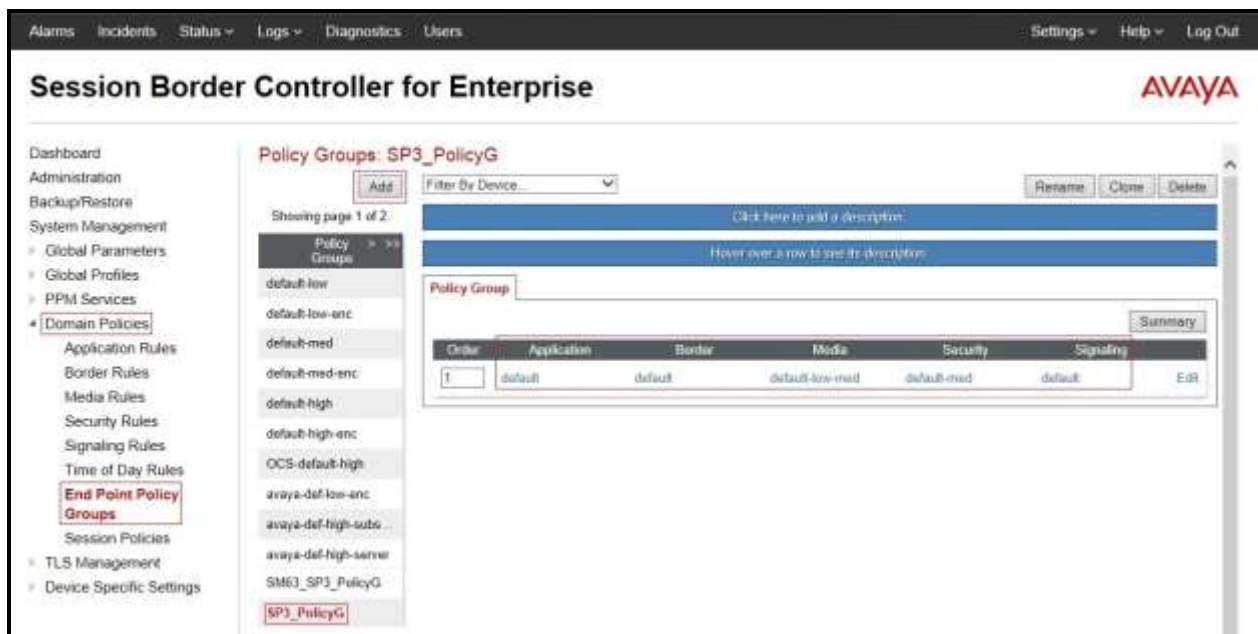


Figure 85 - MTS - End Point Policy Group

7.4. Device Specific Settings

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

7.4.1. Manage Network Settings

From the menu on the left-hand side, select **Device Specific Settings → Network Management**.

- Select **Networks** tab and click **Add** button to add a network of inside interface as followings:
 - **Name:** Network_A1.
 - **Default Gateway:** 10.10.98.1.
 - **Subnet Mask:** 255.255.255.192.
 - **Interface:** A1 (This is Avaya SBCE inside interface).
 - Click **Add** button to add **IP Address** for inside interface: 10.10.98.13.
 - Click **Finish** button to save the changes.

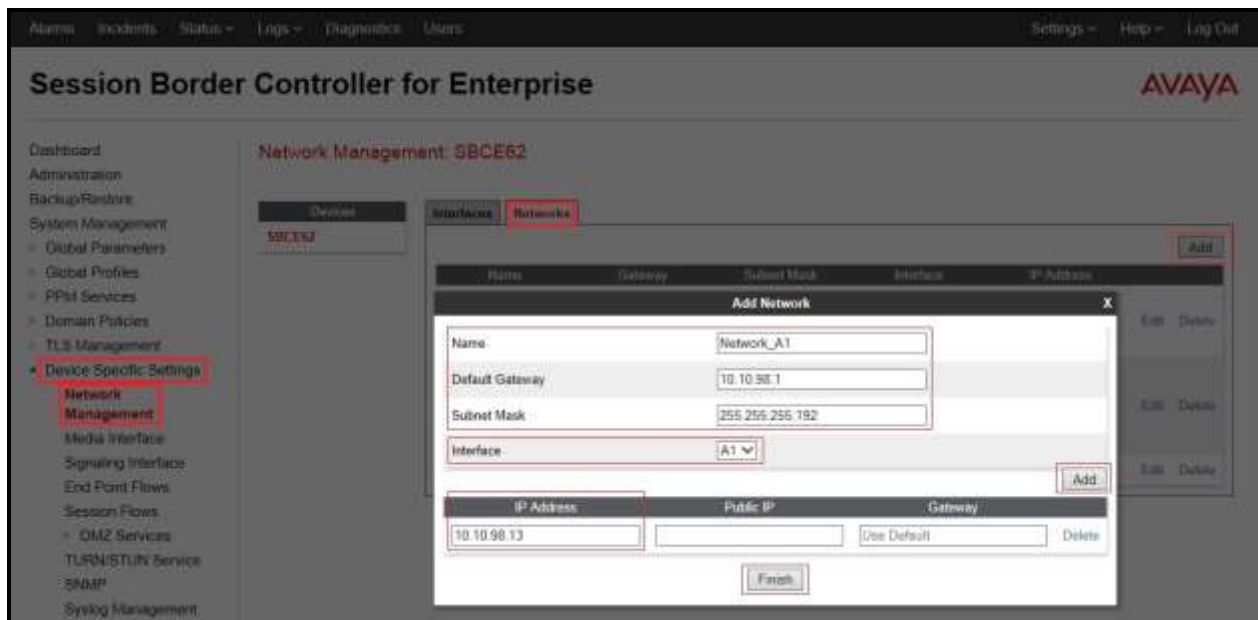


Figure 86 - Network Management – Inside Interface

From the menu on the left-hand side, select **Device Specific Settings → Network Management**.

- Select **Networks** tab and click **Add** button to add a network of outside interface as followings:
 - **Name: Network_B1.**
 - **Default Gateway: 10.10.98.97.**
 - **Subnet Mask: 255.255.255.224.**
 - **Interface: B1** (This is Avaya SBCE outside interface).
 - Click **Add** button to add **IP Address** for outside interface: **10.10.98.111.**
 - Click **Finish** button to save the changes.

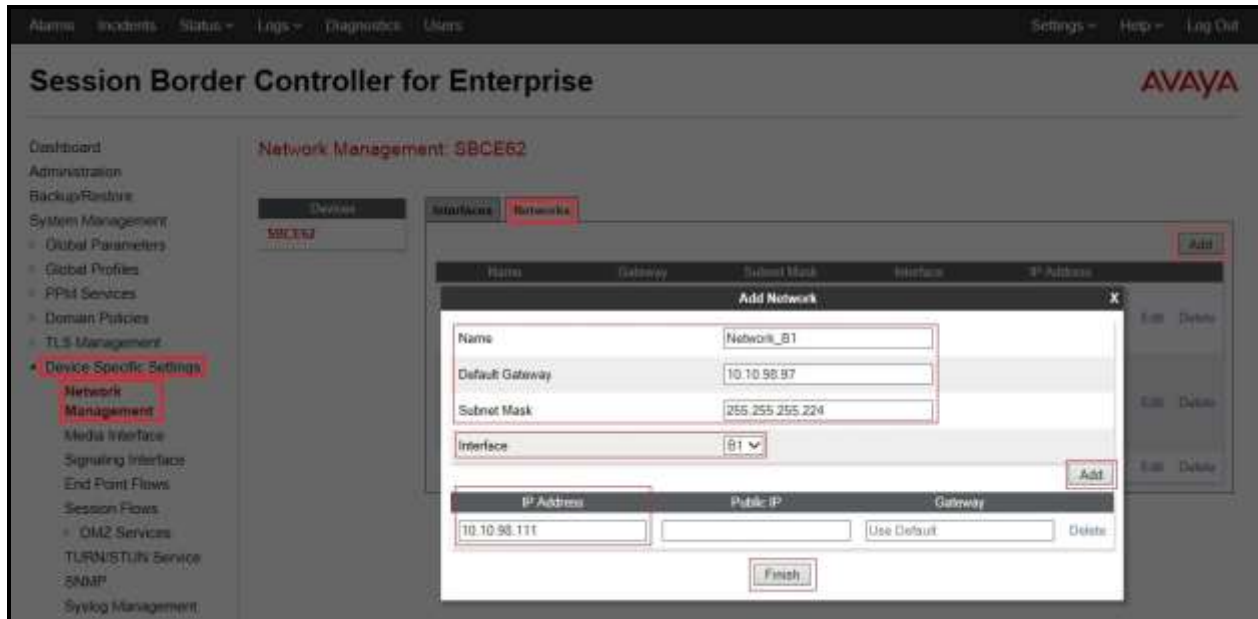


Figure 87 - Network Management – Outside Interface

From the menu on the left-hand side, select **Device Specific Settings** → **Network Management**.

- Select **Interfaces** tab
- Click on the **Status** of the physical interfaces being used and change them to **Enabled** state.



Figure 88 - Network Interfaces Status

7.4.2. Create Media Interfaces

Media Interfaces define the type of signaling on the ports. The default media port range on the Avaya can be used for both inside and outside ports.

From the menu on the left-hand side, select **Device Specific Settings** → **Media Interface**.

- Select **Add**.
 - **Name:** **InsideMedia1**.
 - **Media IP:** **10.10.98.13** (Avaya SBCE Internal IP Address toward Session Manager).
 - **Port Range:** **35000 – 40000**.
 - Click **Finish** (not shown).
- Select **Add**.
 - **Name:** **OutsideMedia1**.
 - **Media IP:** **10.10.98.111** (Avaya SBCE External IP Address toward MTS SIP Trunk Service).
 - **Port Range:** **35000 – 40000**.
 - Click **Finish** (not shown).



Figure 89 - Media Interface

7.4.3. Create Signaling Interfaces

Signaling Interfaces define the type of signaling on the ports.

From the menu on the left-hand side, select **Device Specific Settings** → **Signaling Interface**.

- Select **Add**.
 - **Name: InsideUDP1.**
 - **Signaling IP: 10.10.98.13** (Avaya SBCE Internal IP Address toward Session Manager).
 - **UDP Port: 5060.**
 - Click **Finish** (not shown).
- Select **Add**.
 - **Name: OutsideUDP1.**
 - **Signaling IP: 10.10.98.111** (Avaya SBCE External IP Address toward MTS SIP Trunk Service).
 - **UDP Port: 5060.**
 - Click **Finish** (not shown).



Figure 90 - Signaling Interface

7.4.4. Configuration End Point Flows

Endpoint flows are used to determine the signaling endpoints involved in a call in order to apply the appropriate policies. When a packet arrives at the Avaya SBCE, the content of the packet (IP addresses, URIs, etc) is used to determine which flow it matches. Once the flow is determined, the flow points to policies and profiles which control processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for the destination endpoint are applied. Thus, two flows are involved in every call: the source endpoint flow and the destination endpoint flow. In the case of the compliance test, the signaling endpoints are Session Manager and the MTS SIP Trunk Service.

7.4.4.1 Create End Point Flows – Session Manager Flows

From the menu on the left-hand side, select **Device Specific Settings** → **End Point Flows**.

- Select the **Server Flows** tab.
- Select **Add**, enter **Flow Name: SP3_Flow**.
 - **Server Configuration: SP3** (refer to Section 7.2.5).
 - **URI Group: ***.
 - **Transport: ***.
 - **Remote Subnet: ***.
 - **Received Interface: InsideUDP1** (refer to Section 7.4.3).
 - **Signaling Interface: OutsideUDP1** (refer to Section 7.4.3).
 - **Media Interface: OutsideMedia1** (refer to Section 7.4.2).
 - **End Point Policy Group: SP3_PolicyG** (refer to Section 7.3).
 - **Routing Profile: SP3_To_SM63** (refer to Section 7.2.6).
 - **Topology Hiding Profile: SM63_To_SP3** (refer to Section 7.2.9).
 - Click **Finish** button.

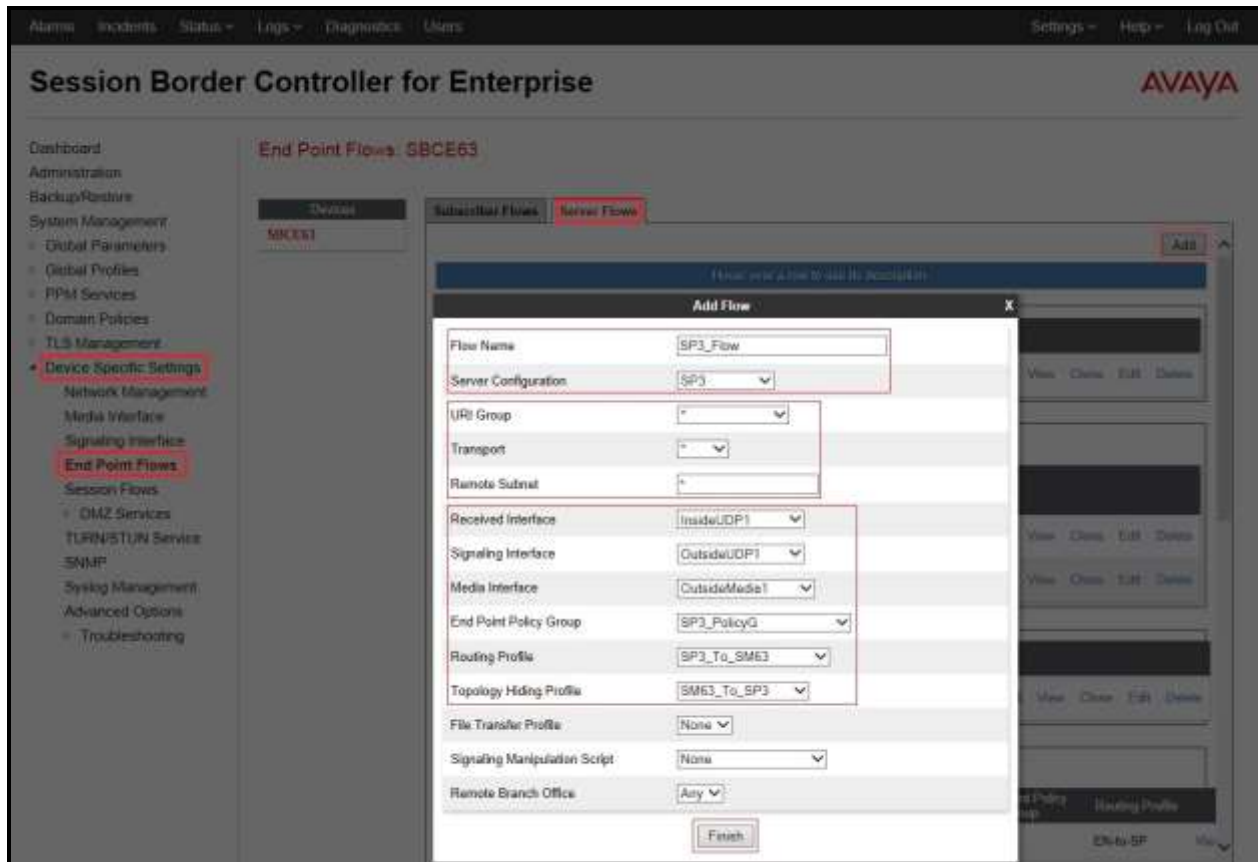


Figure 91 - End Point Flows 1

7.4.4.2 Create End Point Flows – Trunk Flows

From the menu on the left-hand side, select **Device Specific Settings** → **End Point Flows**.

- Select the **Server Flows** tab.
- Select **Add**, enter **Flow Name: SM63_Flow**.
 - **Server Configuration: SM63** (Refer to Section 7.2.4).
 - **URI Group: ***.
 - **Transport: ***.
 - **Remote Subnet: ***.
 - **Received Interface: OutsideUDP1** (refer to Section 7.4.3).
 - **Signaling Interface: InsideUDP1** (refer to Section 7.4.3).
 - **Media Interface: InsideMedia1** (refer to Section 7.4.2).
 - **End Point Policy Group: SM63_SP3_PolicyG** (refer to Section 7.3).
 - **Routing Profile: SM63_To_SP3** (refer to Section 7.2.7).
 - **Topology Hiding Profile: SP3_To_SM63** (refer to Section 7.2.8).
 - Click **Finish** button.

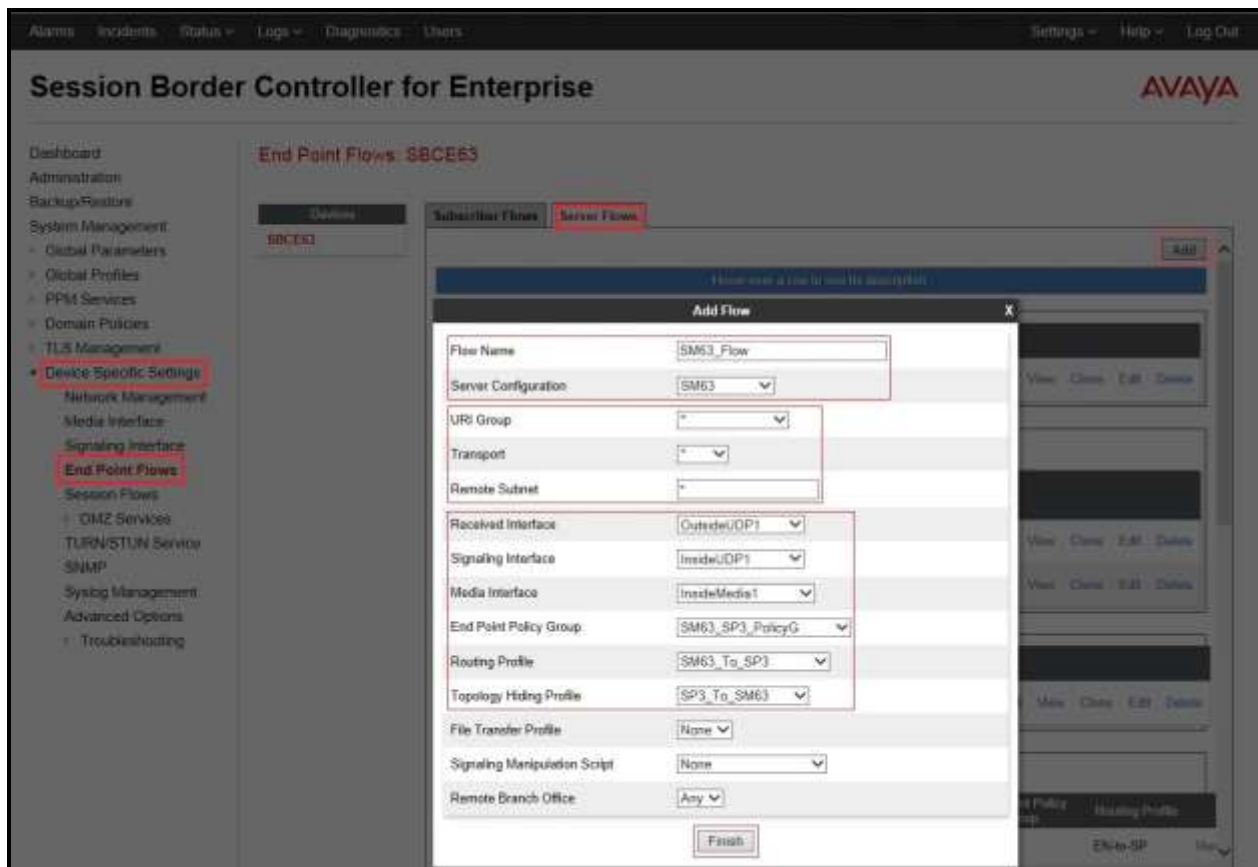


Figure 92 - End Point Flows 2

8. MTS SIP Trunk Service Configuration

MTS is responsible for the network configuration of the MTS SIP Trunk Service. MTS SIP Trunk Service will require that the customer provide the public IP address used to reach the Avaya SBCE public interface at the edge of the enterprise. MTS SIP Trunk Service will provide the IP addresses of MTS's SIP signaling/SBC, IP addresses of media sources and Direct Inward Dialed (DID) numbers assigned to the enterprise. This information is used to complete configurations for CS1000, Session Manager, and Avaya SBCE discussed in the previous sections.

The configuration between MTS SIP Trunk Service and the enterprise is a static IP configuration. There is an authentication of the SIP trunk from enterprise users to the MTS's network.

9. Verification Steps

The following steps may be used to verify the configuration.

9.1. General

Place an inbound call from a PSTN phone to an internal Avaya phone, answer the call, and verify that two-way speech path exists. Verify that the call remains stable for several minutes and disconnects properly.

9.2. Verification of an Active Call on Communication Server 1000

Active Call Trace (ld 80)

The following is an example of one of the commands available on the CS1000 to trace the DN for which the call is in progress or idle (4610). The call scenario involved PSTN phone number 1303XXX9042 calling 204XXX4610 (which is translated to phone 4610).

- Login into CS1000 Signaling Server 10.10.97.177 with admin account and password.
- Issue a command “cslogin” to login on to the CS1000 Call Server.
- Log in to the Overlay command prompt, issue the command **ld 80** and then **trace 0 4610**.
- After the call is released, issue command **trac 0 4610** again to see if the DN is released back to idle state.

Below is the actual output of the CS1000 Call Server Command Line mode when the **4610** is in call state:

```
>ld 80
TRA000
.trac 0 4610

ACTIVE VTN 096 0 00 02

ORIG VTN 100 0 01 00 VTRK IPTI RMBR 101 1 INCOMING VOIP GW CALL
FAR-END SIP SIGNALLING IP: 10.10.98.13
FAR-END MEDIA ENDPOINT IP: 10.10.98.13 PORT: 36194
FAR-END VendorID: AVAYA-SM-6.3.13.631303
TERM VTN 096 0 00 02 KEY 0 SCR MARP CUST 0 DN 4610 TYPE 2002P2
SIGNALLING ENCRYPTION: INSEC
MEDIA ENDPOINT IP: 10.33.5.23 PORT: 5200
MEDIA PROFILE: CODEC G.711 MU-LAW PAYLOAD 20 ms VAD OFF
RFC2833: RXPT 101 TXPT 101 DIAL DN 4610
MAIN_PM ESTD
TALKSLOT ORIG 6 TERM 11
EES_DATA:
NONE
QUEU NONE
CALL ID 501 80

---- ISDN ISL CALL (ORIG) ----
CALL REF # = 385
BEARER CAP = VOICE
HLC =
```

```
CALL STATE = 10  ACTIVE
CALLING NO = 1303XXX9042 NUM_PLAN:UNKNOWN  TON:UNKNOWN  ESN:UNKNOWN
CALLED NO = 204XXX4610 NUM_PLAN:UNKNOWN  TON:UNKNOWN  ESN:UNKNOWN
```

And this is the example after the call to 4610 is finished.

```
>ld 80
TRA000
.trac 0 4610
IDLE VTN 96 0 00 02  MARP
```

SIP Trunk monitoring (ld 32)

Place a call inbound from PSTN (1303XXX9042) to an internal device (204XXX4610). Then check the SIP trunk status by using ld 32, one trunk is BUSY.

```
>ld 32
NPR000
.stat 100 0
091 UNIT(S) IDLE
001 UNIT(S) BUSY
000 UNIT(S) DSBL
000 UNIT(S) MBSY
```

After the call is released, check that SIP trunk status changed to the IDLE state.

```
>ld 32
NPR000
.stat 100 0
092 UNIT(S) IDLE
000 UNIT(S) BUSY
000 UNIT(S) DSBL
000 UNIT(S) MBSY
```

9.3. Protocol Trace

Below is a wireshark trace of the same call scenario described in **Section 9.2**.

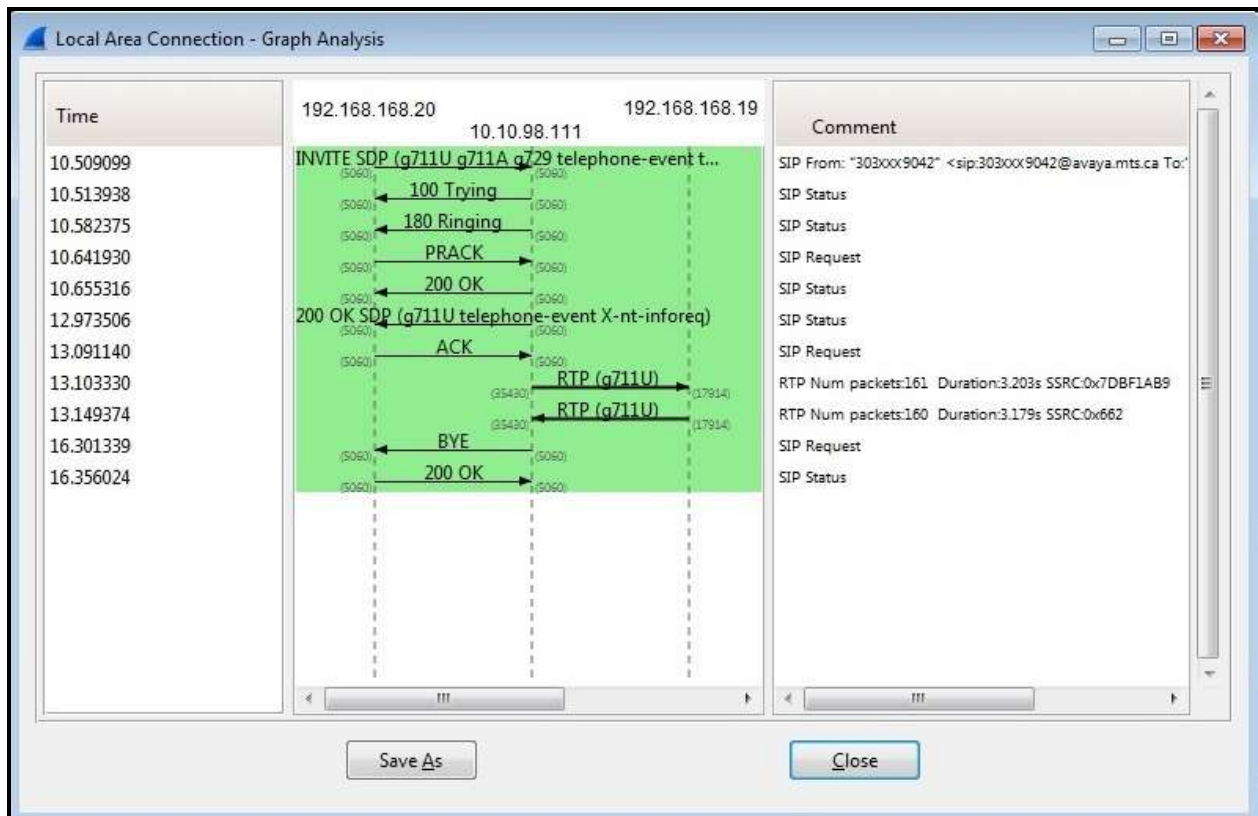


Figure 93 – SIP Call Trace

10. Conclusion

All of the test cases have been executed. Despite observations seen during the testing, as noted in **Section 2.2**, the test met the objectives outlined in **Section 2.1**. The MTS SIP Trunk Service is considered compliant with Avaya Communication Server 1000 Release 7.6, Avaya Aura[®] Session Manager Release 6.3 and Avaya Session Border Controller for Enterprise Release 6.3.

11. References

This section references the documentation relevant to these Application Notes.

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

Avaya Communication Server 1000

- [1] *Network Routing Service Fundamentals*, Avaya Communication Server 1000, Release 7.6, Document Number NN43001-130, Issue 04.01, March 2013
- [2] *IP Peer Networking Installation and Commissioning*, Avaya Communication Server 1000, Release 7.6, Document Number NN43001-313, Issue 06.01, March 2013
- [3] *Communication Server 1000E Overview*, Avaya Communication Server 1000, Release 7.6, Document Number NN43041-110, Issue 06.01, March 2013
- [4] *Unified Communications Management Common Services Fundamentals*, Avaya Communication Server 1000, Release 7.6, Document Number NN43001-116, Issue 06.01, March 2013
- [5] *Dialing Plans Reference*, Avaya Communication Server 1000, Release 7.6, Document Number NN43001-283, Issue 06.01, March 2013.
- [6] *Product Compatibility Reference*, Avaya Communication Server 1000, Release 7.6, Document Number NN43001-256, Issue 06.01 Standard, March 2013

Avaya Aura[®] Session Manager/System Manager

- [7] *Administering Avaya Aura[®] Session Manager*, Release 6.3, Issue 7, Sep 2014
- [8] *Maintaining and Troubleshooting Avaya Aura[®] Session Manager*, Release 6.3, Issue 7, Mar 2015
- [9] *Administering Avaya Aura[®] System Manager for Release 6.3.13*, Release 6.3, Issue 8, Jul 2015

Avaya Session Border Controller for Enterprise

- [10] *Avaya Session Border Controller for Enterprise Overview and Specification*, Release 6.3, Issue 3, October 2014

12. Appendix

Additional patch lineup for the configuration is listed as follows:

Call Server: 7.65 P+ GA plus latest DEPLIST – CPM_7.6_6.zip (X2107.65P)

Signaling Server: 7.65.16 GA plus latest DEPLIST – SP_7.6_6.ntl (7.65.16.00)

CS1000 Signaling Server patch list:

[admin@car3-cores ~]\$ pstat

Product Release: 7.65.16.00

In system patches: 5

PATCH#	NAME	IN_SERVICE	DATE	SPECINS	TYPE	RPM
38	p31484_1	Yes	20/02/14	NO	FRU	cs1000-shared-general-7.65.16-00.i386
47	p33125_1	Yes	23/12/14	NO	FRU	cs1000-OS-1.00.00.00-00.noarch
48	p33274_1	Yes	23/12/14	YES	FRU	initscripts-8.45.25-1.el5.i386
49	p33331_1	Yes	23/12/14	YES	FRU	cs1000-OS-1.00.00.00-00.noarch
50	p33384_1	Yes	23/12/14	NO	FRU	cs1000-OS-1.00.00.00-00.noarch

In System service updates: 31

PATCH#	IN_SERVICE	DATE	SPECINS	REMOVABLE	NAME
0	Yes	23/12/14	YES	YES	cs1000-linuxbase-7.65.16.23-3.i386.000
1	Yes	23/12/14	NO	YES	cs1000-Jboss-Quantum-7.65.16.23-3.i386.000
2	Yes	23/12/14	YES	YES	cs1000-patchWeb-7.65.16.22-4.i386.000
3	Yes	23/12/14	YES	YES	cs1000-dmWeb-7.65.16.23-1.i386.000
4	Yes	23/12/14	YES	YES	cs1000-csoneksvrMgr-7.65.16.22-5.i386.000
5	Yes	23/12/14	YES	YES	cs1000-baseWeb-7.65.16.22-4.i386.000
6	Yes	23/12/14	YES	YES	cs1000-oam-logging-7.65.16.22-4.i386.000
7	Yes	23/12/14	YES	YES	cs1000-csv-7.65.16.22-2.i386.000
8	Yes	23/12/14	YES	YES	cs1000-mscTone-7.65.16.22-2.i386.000
9	Yes	23/12/14	YES	YES	cs1000-mscMusc-7.65.16.22-4.i386.000
10	Yes	23/12/14	YES	YES	cs1000-mscConf-7.65.16.22-2.i386.000
11	Yes	23/12/14	YES	YES	cs1000-mscAnnc-7.65.16.22-2.i386.000
12	Yes	23/12/14	YES	YES	cs1000-mscAttn-7.65.16.22-2.i386.000
13	Yes	23/12/14	NO	YES	cs1000-gk-7.65.16.22-1.i386.000
14	Yes	23/12/14	YES	YES	cs1000-shared-pbx-7.65.16.22-3.i386.000
15	Yes	20/02/14	NO	YES	cs1000-pd-7.65.16.21-00.i386.000
16	Yes	20/02/14	NO	YES	cs1000-shared-carIdtct-7.65.16.21-01.i386.000
17	Yes	20/02/14	NO	YES	cs1000-shared-tpselect-7.65.16.21-01.i386.000
18	Yes	20/02/14	NO	yes	cs1000-dbcom-7.65.16.21-00.i386.000
26	Yes	20/02/14	NO	YES	cs1000-snmp-7.65.16.21-00.i686.000
31	Yes	20/02/14	NO	YES	cs1000-shared-omm-7.65.16.21-2.i386.000
34	Yes	20/02/14	YES	YES	cs1000-ipsec-7.65.16.22-1.i386.000
36	Yes	20/02/14	NO	YES	cs1000-cppmUtil-7.65.16.22-1.i686.000
39	Yes	23/12/14	YES	YES	cs1000-shared-xmsg-7.65.16.22-1.i386.000
40	Yes	23/12/14	NO	YES	cs1000-sps-7.65.16.23-1.i386.000
41	Yes	23/12/14	YES	YES	jdk-1.6.0_81-fcs.i586.000
42	Yes	23/12/14	YES	YES	cs1000-cs-7.65.P.100-03.i386.000

43	Yes	23/12/14	NO	YES	bash-3.2-33.el5_11.4.i386.000
44	Yes	23/12/14	NO	YES	tzdata-2014g-1.el5.i386.000
45	Yes	23/12/14	YES	YES	cs1000-tps-7.65.16.23-7.i386.000
46	Yes	23/12/14	YES	YES	cs1000-vtrk-7.65.16.23-24.i386.000

©2015 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.