



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring CenturyLink SIP Trunk service with the Avaya Communication Server 1000 Release 7.6, Avaya Aura® Session Manager Release 6.3 and Avaya Session Border Controller for Enterprise Release 6.2 – Issue 1.0

Abstract

These Application Notes describe the procedure for configuration CenturyLink 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 6.2.

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. The calls were placed to and from the PSTN with various Avaya endpoints.

CenturyLink SIP Trunk service provides PSTN access via SIP trunks between the enterprise and CenturyLink'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.....	5
2.	General Test Approach and Test Results.....	5
2.1.	Interoperability Compliance Testing.....	5
2.2.	Test Results	6
2.3.	Support	7
3.	Reference Configuration.....	8
4.	Equipment and Software Validated	9
5.	Configure Avaya Communication Server 1000.....	10
5.1.	Log into Communication Server 1000 System	10
5.1.1.	Log into System Manager and Element Manager (EM).....	10
5.1.2.	Log into the Call Server by using the Overlay Command Line Interface (CLI)	12
5.2.	Administer an IP Telephony Node.....	13
5.2.1.	Obtain Node IP address	13
5.2.2.	Administer Terminal Proxy Server (TPS)	15
5.2.3.	Administer Quality of Service (QoS)	16
5.2.4.	Synchronize New Configuration.....	16
5.3.	Administer Voice Codec	17
5.3.1.	Enable Voice Codec G.711, G.729.....	17
5.3.2.	Enable Voice Codec on Media Gateways.....	18
5.4.	Zones and Bandwidth Management.....	19
5.4.1.	Create a Zone for IP Phones (Zone 10)	19
5.4.2.	Create a 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 Aura® Session Manager.....	22
5.5.3.	Administer Virtual D-Channel.....	24
5.5.4.	Administer Virtual Super-Loop	28
5.5.5.	Administer Virtual SIP Routes	28
5.5.6.	Administer Virtual Trunks.....	30
5.5.7.	Administer Calling Line Identification Entries.....	33
5.5.8.	Enable External Trunk to Trunk Transfer.....	35
5.6.	Administer Dialing Plans	36
5.6.1.	Define ESN Access Codes and Parameters (ESN)	36
5.6.2.	Associate NPA and SPN call to ESN Access Code 1.....	37
5.6.3.	Digit Manipulation Block Index (DMI).....	38

5.6.4.	Route List Block (RLB) (RLB 14)	39
5.6.5.	Inbound Call – Incoming Digit Translation Configuration	41
5.6.6.	Outbound Call - Special Number Configuration	43
5.6.7.	Outbound Call - Numbering Plan Area (NPA)	44
5.7.	Administer a Phone	45
5.7.1.	Phone creation	45
5.7.2.	Enable Privacy for the Phone	46
5.7.3.	Enable Call Forward for Phone	47
5.7.4.	Enable Call Waiting for Phone	49
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.	Add SIP Entities	56
6.4.1.	Configure Session Manager SIP Entity	57
6.4.2.	Configure Communication Server 1000 SIP Entity	58
6.4.3.	Configure Avaya SBCE SIP Entity	59
6.5.	Add Entity Links	59
6.6.	Configure Time Ranges	61
6.7.	Add Routing Policies	61
6.8.	Add Dial Patterns	63
7.	Configure Session Border Controller for Enterprise	66
7.1.	Log into the Avaya SBCE	66
7.2.	Global Profiles	67
7.2.1.	Configure Server Interworking - Avaya site	67
7.2.2.	Configure Server Interworking – CenturyLink site	68
7.2.3.	Configure URI Groups	69
7.2.4.	Configure Routing – Avaya site	69
7.2.5.	Configure Routing – CenturyLink site	70
7.2.6.	Configure Signaling Manipulation	71
7.2.7.	Configure Server – Session Manager	72
7.2.8.	Configure Server – CenturyLink	73
7.2.9.	Configure Topology Hiding – Avaya site	75
7.2.10.	Configure Topology Hiding – CenturyLink site	76
7.3.	Domain Policies	76
7.3.1.	Create Application Rules	77
7.3.2.	Create Border Rules	78

7.3.3.	Create Media Rules.....	79
7.3.4.	Create Security Rules.....	80
7.3.5.	Create Signaling Rules.....	81
7.3.6.	Create Time of Day Rules.....	83
7.3.7.	Create Endpoint Policy Groups	85
7.3.8.	Create Session Policy.....	87
7.4.	Device Specific Settings.....	89
7.4.1.	Manage Network Settings.....	89
7.4.2.	Create Media Interfaces	90
7.4.3.	Create Signaling Interfaces	91
7.4.4.	Configuration Server Flows.....	91
7.4.5.	Create Session Flows	93
8.	CenturyLink SIP Trunking service Configuration.....	94
9.	Verification Steps.....	94
9.1.	General	94
9.2.	Verification of an Active Call on Communication Server 1000.....	94
9.3.	Protocol Trace	97
10.	Conclusion	98
11.	References.....	99

1. Introduction

These Application Notes illustrate a sample configuration using Avaya Communication Server 1000 Release 7.6, Avaya Aura® Session Manager Release 6.3, Avaya Session Border Controller for Enterprise (Avaya SBCE) Release 6.2 with CenturyLink SIP Trunk service. CenturyLink SIP Trunk service provides PSTN access via SIP Trunks between the enterprise and CenturyLink's network as an alternative to legacy analog or digital trunks.

2. General Test Approach and Test Results

The Communication Server 1000 was connected to the Avaya SBCE via SIP Trunks to Session Manager. The Avaya SBCE was connected to CenturyLink's network via SIP trunks. Various call types were made from the Communication Server 1000 to CenturyLink 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 Communication Server 1000 and CenturyLink SIP Trunk service, including the following:
 - Codec/ptime (G.711 u-law/20ms, G.711 a-law/20ms and G.729/20ms), no VAD.
 - Hold/Resume on both ends.
 - Calling Line Identification Display (CLID).
 - Ring-back tone.
 - Speech (audio) path.
 - Dialing plan support (local, long distance, international, outbound toll-free, inbound toll-free, Assisted Operator, 411, and 911).
 - Advanced features (Call on Mute, Call Park, and Call Waiting).
 - Abandoned Call.
- Call redirection verification: all supported methods (blind transfer, consultative transfer, call forward, and conference) including CLID. Call redirection is performed from both ends.
- Response to SIP OPTIONS queries.
- G.711 Pass Through and T.38 fax.
- Inbound and outbound long hold time call stability.
- Caller number/ID presentation.
- Privacy requests (i.e., caller anonymity) and Caller ID restriction for inbound and outbound calls.

- DTMF (RFC2833) in both directions
- SIP Transport UDP, port 5060
- Voice Mail Server Call Pilot (hosted on Avaya system)
- Use SIP UPDATE on Blind Transfer.
- Use SIP CONTACT HEADER on Call Redirection.

The following assumptions were made for the compliance tested configuration:

1. Communication Server 1000 R7.6 software with latest patches.
2. CenturyLink service provides support to setup, configure and troubleshoot on carrier switch during testing execution.

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

1. Calls were checked for the correct call progress tones and cadences.
2. During the ringing state the ring back tone and destination ringing were checked.
3. Calls were checked in both hands-free and handset mode due to internal Avaya requirement.
4. Calls were checked for speech path in both directions using spoken words to ensure clarity of speech.
5. The display(s) of the sets/clients involved were checked for consistent and expected CLID and redirection information both prior to answer and after call establishment.
6. The speech path and messaging system were observed for timely and quality End to End tone audio path generation and application responses.
7. The call server maintenance terminal window was open during the test cases execution for the monitoring of BUG(s), ERROR and AUD messages (See **Session 5.1.2**).
8. Speech path was checked before and after calls were put on/off hold from each end.
9. 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 **Session 9.2** - SIP Trunk monitoring (LD 32)).

2.2. Test Results

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

1. If the Avaya Communication Server 1000 phone holds/resumes an outbound call, the dialed digits are no longer displayed. This is a Communication Server 1000 known issue.
2. CenturyLink provided the inbound toll free number (The inbound call from PSTN to toll free number which terminates the call to Avaya Communication Server 1000 phone number) which is not switched to a POTs number in FROM HEADER. It will be delivered as the 8xx number and CS1000 will use Incoming Digit Translation to convert this number to 303-615-7104.
3. CenturyLink service does not support register and authentication.

CenturyLink agreed that the above observations were not severe enough to fail the test.

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 CenturyLink service, please contact customer service or visit
<http://www.CenturyLink.com>

3. Reference Configuration

Figure 1 illustrates the test configuration used during the compliance test between Communication Server 1000 and CenturyLink 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.

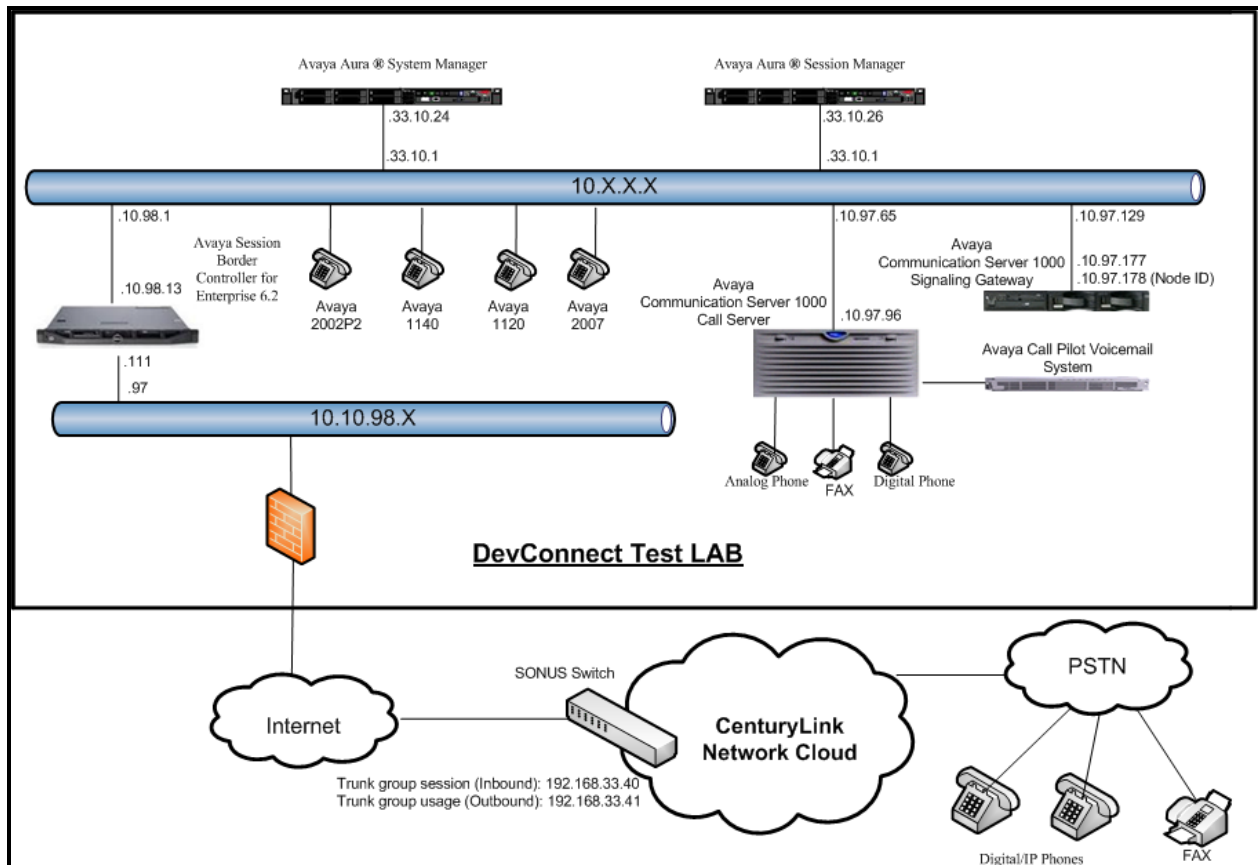


Figure 1- Network diagram for Avaya and CenturyLink SIP Trunk Service

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 S8800 Server	Avaya Aura® Session Manager R6.3.0 – 6.3.0.0.630002-6.3.2.632001
Avaya S8800 Server	Avaya Aura® System Manager R6.3.0 – FP2 6.3.0.8.5682 – 6.3.8.1627 (6.3.2.4.1399)
Avaya Session Border Controller for Enterprise	6.2.0 Q36
Avaya UNISTim Phones: 2002 p2 1140 1120 2007	0604DCO 0625C8Q 0624C8Q 0621C8L
Avaya 3904 Digital Phone	N/A
Analog Phone	N/A
HP Office jet 4500 Fax	N/A

CenturyLink service:

System	Software
SONUS SBC9000	V07.03.07F017

Additional patch lineup for the configuration listed as follows:

Call Server: 7.65 P+ GA plus latest DEPLIST – CPL_7.6_1.zip (X2107.65P)

Signaling Server: 7.65.16 GA plus latest DEPLIST – SP_7.6_1.ntl

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 Special Number (SPN) features to route calls from the Communication Server 1000 to the PSTN, via SIP trunks to CenturyLink.

These application notes assume that the basic Communications Server 1000 configuration has already been administered. For further information on Communications Server 1000, please consult the references in **Section 11**.

The procedures below describe the configuration details for configuring the Communication Server 1000.

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**

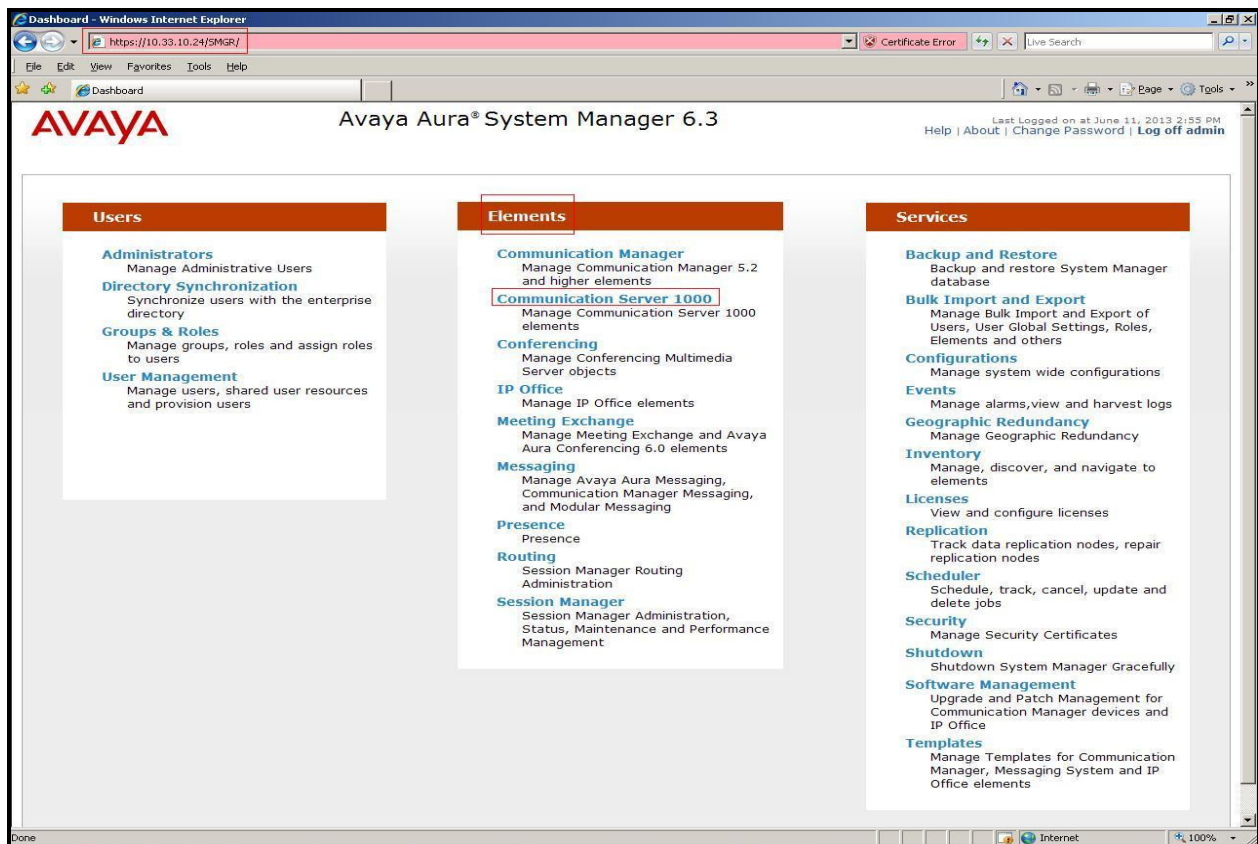
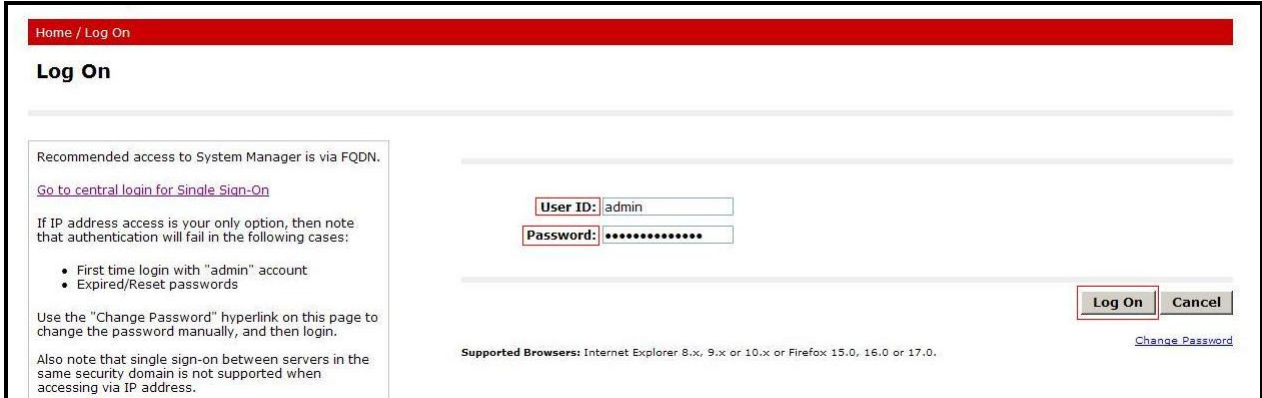


Figure 2 –System Manager Home Screen

Log into the Communication Server 1000 using an appropriate **User ID** and **Password**.



The screenshot shows the 'Log On' page of the Communication Server 1000. At the top is a red header with 'Home / Log On'. Below it, the 'Log On' title is displayed. A text box on the left provides instructions: 'Recommended access to System Manager is via FQDN. Go to [central login for Single Sign-On](#). If IP address access is your only option, then note that authentication will fail in the following cases: First time login with "admin" account, Expired/Reset passwords. Use the "Change Password" hyperlink on this page to change the password manually, and then login. Also note that single sign-on between servers in the same security domain is not supported when accessing via IP address.' To the right of this text are input fields for 'User ID' (containing 'admin') and 'Password' (masked with dots). Below these fields are 'Log On' and 'Cancel' buttons. At the bottom, it lists 'Supported Browsers: Internet Explorer 8.x, 9.x or 10.x or Firefox 15.0, 16.0 or 17.0.' and a 'Change Password' link.

Home / Log On

Log On

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

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

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

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

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

User ID: admin

Password:

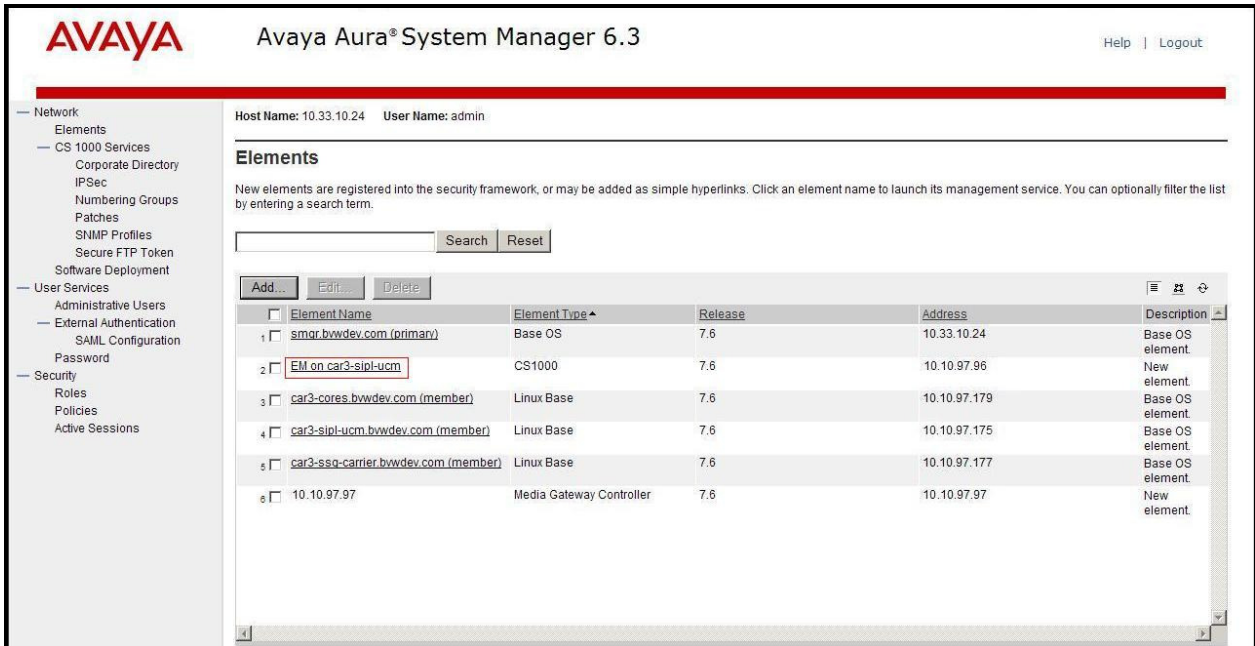
Log On Cancel

Supported Browsers: Internet Explorer 8.x, 9.x or 10.x or Firefox 15.0, 16.0 or 17.0.

[Change Password](#)

Figure 3 – Communication Server 1000 Log In Screen

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



The screenshot shows the 'Avaya Aura System Manager 6.3' interface. The top header includes the Avaya logo, the title 'Avaya Aura® System Manager 6.3', and links for 'Help' and 'Logout'. A left-hand navigation menu lists various categories: Network, Elements, CS 1000 Services, User Services, External Authentication, Password, Security, Roles, Policies, and Active Sessions. The main content area is titled 'Elements' and shows a list of registered elements. A search bar with 'Search' and 'Reset' buttons is present. Below the search bar are 'Add...', 'Edit...', and 'Delete' buttons. The table lists elements with columns for 'Element Name', 'Element Type', 'Release', 'Address', and 'Description'. The second row, 'EM on car3-sipl-ucm', is highlighted with a red box around its 'Element Name'.

AVAYA Avaya Aura® System Manager 6.3 Help | Logout

Host Name: 10.33.10.24 User Name: admin

Elements

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

Search Reset

Add... Edit... Delete

	Element Name	Element Type	Release	Address	Description
1	smgr.bvwdev.com (primary)	Base OS	7.6	10.33.10.24	Base OS element.
2	EM on car3-sipl-ucm	CS1000	7.6	10.10.97.96	New element.
3	car3-cores.bvwdev.com (member)	Linux Base	7.6	10.10.97.179	Base OS element.
4	car3-sipl-ucm.bvwdev.com (member)	Linux Base	7.6	10.10.97.175	Base OS element.
5	car3-ssq-carrier.bvwdev.com (member)	Linux Base	7.6	10.10.97.177	Base OS element.
6	10.10.97.97	Media Gateway Controller	7.6	10.10.97.97	New element.

Figure 4 – Communication Server 1000 Management

The Communication Server 1000 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 the Call Server by using the Overlay Command Line Interface (CLI)

Using Putty, SSH to the IP address of the Communication Server 1000 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**

Nortel Networks Linux Base 7.65

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

admin@10.10.97.177's password: <----**enter the password**

Last login: Tue Sep 03 11:20:18 2013 from 10.10.98.78

[admin@car3-ssg-carrier ~]\$ **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 11:39 4/9/2013

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: Leave this screen for monitoring of BUG(s), ERROR and AUD messages.

5.2. Administer an IP Telephony Node

This section describes how to configure an IP Telephony Node on Communication Server 1000.

5.2.1. Obtain Node IP address

These application notes assume that the basic Communication Server 1000 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 Communication Server 1000 IP network to work with CenturyLink SIP Trunk service. For further information on Communications Server 1000, 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**.

The screenshot displays the AVAYA CS1000 Element Manager web interface. The left sidebar contains a navigation tree with the following items: UCM Network Services, Home, Links, Virtual Terminals, System (highlighted), Alarms, Maintenance, Core Equipment, Peripheral Equipment, IP Network (highlighted), Nodes: Servers, Media Cards (highlighted), Maintenance and Reports, Media Gateways, Zones, Host and Route Tables, Network Address Translation (NAT), and QoS Thresholds. The main content area is titled 'CS1000 Element Manager' and shows the 'IP Telephony Nodes' page. At the top, it indicates 'Managing: 10.10.97.96' and 'Username: admin'. Below this, it says 'System » IP Network » IP Telephony Nodes'. The page title is 'IP Telephony Nodes' with a subtitle 'Click the Node ID to view or edit its properties.' There are buttons for 'Add...', 'Import...', 'Export...', and 'Delete', along with 'Print' and 'Refresh'. A table lists the nodes:

Node ID	Components	Enabled Applications	ELAN IP	Node/TLAN IPv4	Node/TLAN IPv6	Status
3000	1	LTPS, Gateway (SIPGw)	-	10.10.97.178		Synchronized
3002	1	SIP Line, LTPS	-	10.10.97.176		Synchronized

At the bottom, there are checkboxes for 'Show: Nodes' (checked), 'Component servers and cards' (unchecked), and 'IPv6 address' (checked).

Figure 6 – IP Telephony Nodes

The **Node Details** screen is displayed in **Figure 7** with the IP address of the Communication Server 1000 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 IP 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. Save Cancel

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 address

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

Figure 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: 10.10.97.96 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 Codecs
- Quality of Service (QoS)
- LAN
- SNTIP
- 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**

<input type="checkbox"/> 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 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: 10.10.97.96 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: 0.0.0.0
Full file path: download/firmware
Server Account/User ID: []
Password: []

DTLS

DTLS policy: Off

Options: ☐ Client authentication
☐ Periodic re-keying

Network Connect Server

* Required Value. **Save** **Cancel**

Note: Changes made on this page will NOT be transmitted until the Node is also 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 navigation tree with categories like 'UCM Network Services', 'System', 'IP Network', 'Interfaces', 'Customers', 'Routes and Trunks', and 'Dialing and Numbering Plans'. The main content area is titled 'Node ID: 3000 - Quality of Service (QoS)'. It features a 'Diffserv Codepoint (DSCP)' section with the following configuration options:

- Enable Avaya automatic QoS: ☐
- Control packets: (0-63)
- Voice packets: (0-63)
- VLAN tagging: ☐ 802.1Q support
- 802.1Q bits value (802.1P): (0-7)

At the bottom of the configuration area, there is a note: 'Note: Changes made on this page will NOT be transmitted until the Node is also saved.' Below this note are 'Save' and 'Cancel' buttons. The 'Save' button is highlighted with a red box.

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** (not shown). The **Synchronize Configuration Files (Node ID <3000>)** screen is displayed (not shown). Check the **Signaling Server** checkbox and click on **Start Sync** (not shown). When the synchronization completes, check the **Signaling Server** checkbox and click on the **Restart Applications** (not shown).

5.3. Administer Voice Codec

5.3.1. Enable Voice Codec G.711, G.729

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 Communication Server 1000 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**. CenturyLink supports **G.711/time 20ms** and **G.729/time 20ms** with **Voice Activity Detection (VAD)** checkbox unchecked. Click on the **Save** button.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left pane contains a navigation tree with categories like UCM Network Services, Home, Links, 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, Unicom 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 pane displays the 'Node ID: 3000 - Voice Gateway (VGW) and Codecs' configuration page. The page has tabs for General, Voice Codes, and Fax. The 'Voice Codes' tab is active, showing a list of voice codecs. The 'Voice Codes' section contains the following settings:

- Codec G.711:** ☒ Enabled (required). Voice payload size: 20 (milliseconds per frame). Voice playback (jitter buffer) delay: 40 (Nominal) to 80 (Maximum) milliseconds. A note states: 'Maximum delay may be automatically adjusted based on nominal settings.'
- Voice Activity Detection (VAD):** ☐ Unchecked.
- Codec G.722:** ☐ Not Enabled. Voice payload size: 20 (milliseconds per frame). Voice playback (jitter buffer) delay: 40 (Nominal) to 80 (Maximum) milliseconds. A note states: 'Maximum delay may be automatically adjusted based on nominal settings.'
- Codec G.729:** ☒ Enabled. Voice payload size: 20 (milliseconds per frame).

At the bottom of the page, 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 11 – 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 11**, 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 G.711** and **Codec G.729A** and uncheck **VAD** as shown in **Figure 12**. Scroll down to the bottom of the page and click on the **Save** button (not shown).

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

D-Channels

Digital Trunk Interface

Dialing and Numbering Plans

Electronic Switched Network

Flexible Code Restriction

Incoming Digit Translation

Phones

Templates

Reports

Views

Lists

Properties

Migration

Tools

Backup and Restore

Date and Time

Logs and reports

Security

Passwords

Policies

Login Options

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 9600 (bps)

FAX playout nominal delay 100 (0 - 300 milliseconds)

FAX no activity timeout 20 (10 - 32000 milliseconds)

FAX packet size 30

Codec G.711 Select ☒

Codec name G.711

Voice payload size 20 (ms/frame)

Voice playout (jitter buffer) nominal delay 40

Modifications may cause changes to dependent settings

Voice playout (jitter buffer) maximum delay 80

Modifications may cause changes to dependent settings

VAD ☐

Codec G.729A Select ☒

Codec name G.729A

Voice payload size 20 (ms/frame)

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

Figure 12 – 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 sets, and zone 255 for the SIP Trunk.

5.4.1. Create a Zone for IP Phones (Zone 10)

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

Select **IP Network** → **Zones** configuration from the left pane (not shown), click on **Bandwidth Zones** as shown in **Figure 13**.

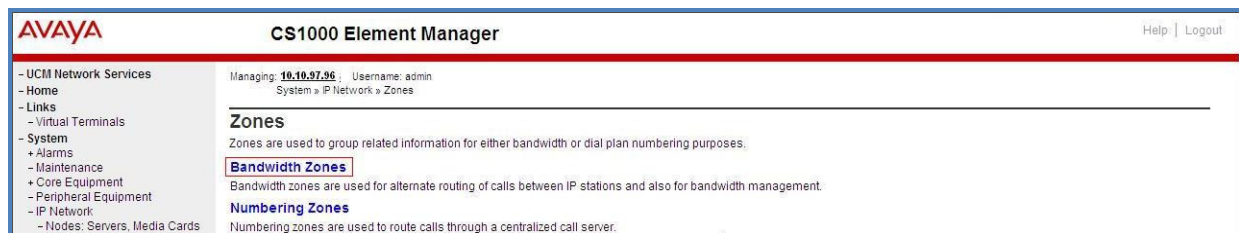


Figure 13 – Zones Page

The **Bandwidth Zones** screen is displayed as shown in **Figure 14**. Click **Add** to create new zone for IP Phones.

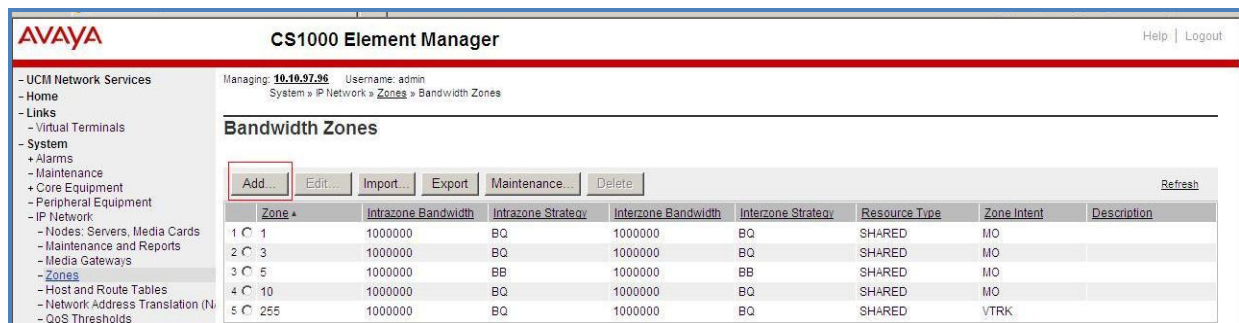


Figure 14 – Bandwidth Zones

Select and input the values as shown below (in the red boxes) in **Figure 15**, and click on the **Submit** button.

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

Managing: 10.10.97.96 Username: admin
System » IP Network » Zones » Bandwidth Zones » Bandwidth Zones 10 » Edit Bandwidth Zone » Zone Basic Property and Bandwidth Management

Zone Basic Property and Bandwidth Management

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

Submit Refresh Cancel

Figure 15 –Bandwidth Management Configuration Details – IP phone

5.4.2. Create a 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 16** and then click on the **Submit** button.

Managing: 10.10.97.96 Username: admin
System » IP Network » Zones » Bandwidth Zones » Bandwidth Zones 255 » Edit Bandwidth Zone » Zone Basic Property and Bandwidth Management

Zone Basic Property and Bandwidth Management

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

Submit Refresh Cancel

Figure 16 –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 (not shown). The **Customers** screen is displayed. Click on the link associated with the appropriate customer, in this case **00**. The system can support more than one customer with different network settings and options. The **Customer 00 Edit** page will appear (not shown). Select the **Feature Packages** option from **Customer 00 Edit** page. The screen is updated with a listing of available **Feature Packages** (not all features are shown in **Figure 17** 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 Help | Logout

Package: 145

- Integrated Services Digital Network

+ 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 17 –Customer – ISDN Configuration

5.5.2. Administer SIP Trunk Gateway to Avaya Aura® Session Manager

Select **IP Network** → **Nodes: Servers, Media Cards** configuration from the left pane. In the **IP Telephony Nodes** screen displayed (not shown), select the **Node ID** of the Communication Server 1000 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 18**. The **SIP domain name** and **Local SIP port** should be matched in the configuration of Session Manager (in **Sections 6.2 and 6.5**).

AVAYA CS1000 Element Manager

Managing: 10.10.97.96 Username: admin
System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration

Node ID: 3000 - Virtual Trunk Gateway Configuration Details

General | SIP Gateway Settings | SIP Gateway Services

Vtrk gateway application: ☒ Enable gateway service on this node

General

Vtrk gateway application: SIP Gateway (SIPGw)
SIP domain name: bwdev7.com
Local SIP port: 5060 *(1 - 65535)
Gateway endpoint name: car3-sng-carrier
Gateway password:
Application node ID: 3000 *(0-9999)
Enable failsafe NRS: ☐

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

Virtual Trunk Network Health Monitor

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

Monitor IP:
Add

Monitor addresses:
Remove

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

Save Cancel

Figure 18 – Virtual Trunk Gateway Configuration Details

Click on the **SIP Gateway Settings** tab, under **Proxy or Redirect Server**, and enter the following values (highlighted in red boxes) for the specified fields, retaining the default values for the remaining fields as shown in **Figure 19**. Enter the IP address of Session Manager in the **Primary TLAN IP address** field (This IP address is defined in **Session 6.4.1**). Enter **Port: 5060** and **Transport protocol: UDP**. Uncheck **Support registration** checkbox.

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a navigation tree with categories like UCM Network Services, Links, System, and Customers. The main content area is titled 'Node ID: 3000 - Virtual Trunk Gateway Configuration Details'. It has three tabs: 'General', 'SIP Gateway Settings', and 'SIP Gateway Services'. The 'SIP Gateway Services' tab is active. Under the 'Proxy Or Redirect Server' section, the 'Primary TLAN IP address' is set to 10.33.10.26, the 'Port' is 5060, and the 'Transport protocol' is UDP. The 'Support registration' checkbox is unchecked. The 'Secondary TLAN IP address' is set to 0.0.0.0, and its 'Transport protocol' is 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 19 – Virtual Trunk Gateway Configuration Details

On the same page as shown in **Figure 19**, scroll down to the **SIP URI Map** section.

Under the **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 the **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 20**. Then click on the **Save** button.

Figure 20 – 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 21**. Click the **to Add** button.

Figure 21 – D-Channels

The **D-Channels 100 Property Configuration** screen is displayed next, as shown in **Figure 22**. 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 22**. Other fields are left as default.

AVAYA CS1000 Element Manager

Help | Logout

- Basic Configuration

Input Description	Input Value
Action Device And Number (ADAN):	DCH
D channel Card Type:	DCIP
Designator:	VoIP
Recovery to Primary:	<input type="checkbox"/>
PRI loop number for Backup D-channel:	
User:	Integrated Services Signaling Link Dedicated (ISLD)
Interface type for D-channel:	Meridian Meridian1 (SL1)
Country:	ETS 300 =102 basic protocol (ETSI)
D-Channel PRI loop number:	
Primary Rate Interface:	more PRI
Secondary PRI2 loops:	
Meridian 1 node type:	Slave to the controller (USR)
Release ID of the switch at the far end:	25
Central Office switch type:	100% compatible with Bellcore standard (STD)
Integrated Services Signaling Link Maximum:	4000 Range: 1 - 4000
Signalling server resource capacity:	1800 Range: 0 - 3700

+ Basic options (BSCOPT)

- Advanced options (ADVOPT)

- Layer 3 call control message count per 5 second time interval: 300 Range: 60 - 350

- Number of Status Enquiry Messages sent within 128 ms: 1

- Map channel number to timeslots on a PRI2 loop: ☒

- H323 Overlap Signaling Settings (H323)

- Overlap Receiving: ☐

- Overlap Sending: ☐

--Overlap Timer:

- Multilocation Business Group Allowed: ☐

- Network Attendant Service Allowed: ☒

+ Link Access Protocol for D-channel (LAPD)

+ Feature Packages

Copyright © 2002-2013 Avaya Inc. All rights reserved.

Figure 22 – D-Channels Configuration Details

Click on the **Basic Options (BSCOPT)** and click on the **Edit** button on the **Remote Capabilities** field as shown in **Figures 23**.

AVAYA CS1000 Element Manager Help | Logout

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

- Basic options (BSCOPT)

Action Device And Number (ADAN): DCH

D channel Card Type: DCIP

Designator: VoIP

Recovery to Primary: ☐

PRI loop number for Backup D-channel:

User: Integrated Services Signaling Link Dedicated (ISLD)

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

Country: ETS 300 =102 basic protocol (ETSI)

D-Channel PRI loop number:

Primary Rate Interface: more PRI

Secondary PRI2 loops:

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

Release ID of the switch at the far end: 25

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

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

Signalling server resource capacity: 1800 Range: 0 - 3700

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

- PINX customer number:

- Progress signal:

- Calling Line Identification:

- Output request Buffers: 32

- D-channel transmission Rate: 56 kb/s when LCMT is AMI (56K)

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

- Remote Capabilities: **Edit**

- B channel Service messaging: ☐

+ - Change protocol timer value (TIMR)

+ Advanced options (ADVOPT)

+ Feature Packages

Submit Refresh Delete Cancel

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

Figure 23 – D-Channel Configuration Details

The **Remote Capabilities Configuration** page appears as shown in **Figures 24**. Check on the **ND2** and the **MWI** checkboxes.

AVAYA CS1000 Element Manager

Managing: 10.10.37.36 Username: admin
Routes and Trunks » D-Channels » D-Channels 100 Property Configuration » Remote 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 QSIG 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 QSIG 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"/>
Malicious call identification (MCID)	<input type="checkbox"/>
MCDN QSIG conversion (MQC)	<input type="checkbox"/>
Remote D-channel is on a MSDL 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 © 2002-2011 Avaya Inc. All rights reserved.

Figure 24 – Remote Capabilities Configuration Details

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 25**. In this example, Superloop 4, 96, 100, and 124 have been added and are being used.

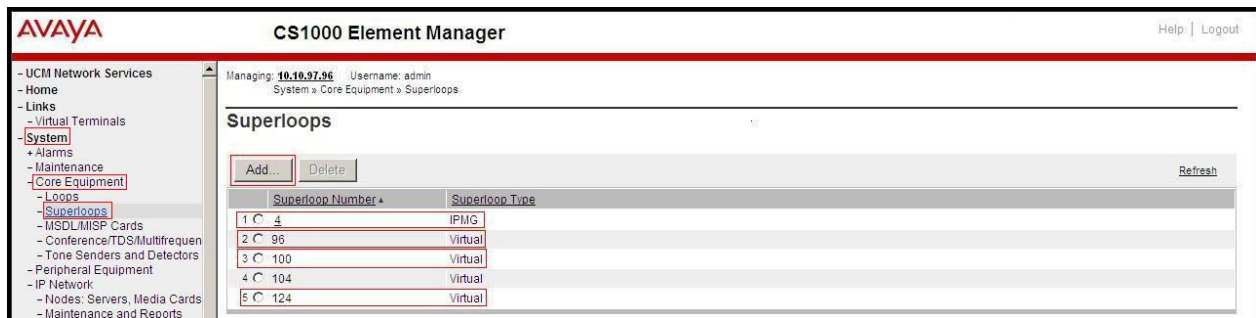


Figure 25 – Administer Virtual Super-Loop Page

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 26**.

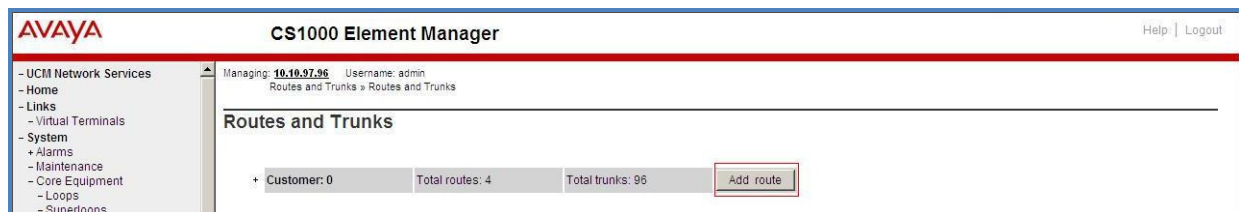


Figure 26 – Add route

The **Customer 0**, New **Route Configuration** screen is displayed next (not shown). The **Basic Configuration** section is displayed to put 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 27**.

- **Route number (ROUT):** Select 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**)
 - **Network calling name allowed (NCNA):** Check the field.
 - **Network call redirection (NCRD):** Check the field.
 - **Insert ESN access code (INAC):** Check the field.

Figure 27 – Route Configuration Details

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 28**. Click on the **Submit** button.

AVAYA CS1000 Element Manager

Help | Logout

UCM Network Services

- Home
- Links
- Virtual Terminals
- System
 - Alarms
 - Maintenance
 - Core Equipment
 - Loops
 - Superloops
 - MSDL/MISP Cards
 - Conference/TDS/Multifrequen
 - Tone Senders and Detectors
 - Peripheral Equipment
- IP Network
 - Nodes: Servers, Media Cards
 - Maintenance and Reports
 - Media Gateways
 - Zones
 - Host and Route Tables
 - Network: Address Translation
 - QoS Thresholds
 - Personal Directories
 - Unicode Name Directory
- Interfaces
 - Engineered Values
 - Emergency Services
 - Geographic Redundancy
 - Software
- Customers
 - Routes and Trunks
 - Routes and Trunks
 - D-Channels
 - Digital Trunk Interface
 - 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

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

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

Basic Route Options

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

Billing number required (BLN): ☐

Call detail recording (CDR): ☒

CDR records generated on incoming calls (INC): ☒

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

Time to answer output in CDR (TTA): ☐

CDR ACC Q initial connection records to be generated (QREC): ☒

CDR on outgoing calls (OAL): ☒

CDR on outgoing toll calls (OTL): ☐

Answered call identification allowed (AIA): ☒

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

Outpulsed digits in CDR (OPD): ☒

Number of digits printed (NDP): EXC 0

North American toll scheme (NATL): ☒

Controls or timers (CNTL): ☐

Conventional (Tie trunk only) (CNVT): ☐

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

Day IDC tree number (DCNO): 1 (0 - 254)

Night IDC tree number (NDNO): 1 (0 - 254)

Display external dialed digits (DEXT): ☐

Multifrequency compelled or MFC signaling (MFC): No MFC (NO)

Process notification networked calls (PNNC): ☐

Network Options

General Options

Advanced Configurations

Submit Refresh Delete Cancel

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

Figure 28 – Route Configuration Details

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 29**.

AVAYA CS1000 Element Manager

Help | Logout

Managing: 10.10.97.96 Username: admin

Routes and Trunks → Routes and Trunks

Routes and Trunks

Customer	Total routes	Total trunks	
Customer: 0	Total routes: 4	Total trunks: 96	Add route
+ Route: 11	Type: TIE	Description: SIPL	Edit Add trunk
+ Route: 100	Type: TIE	Description: 100	Edit Add trunk

Figure 29 – Routes and Trunks Page

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. The 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 30**.

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

Figure 30 – New Trunk Configuration Details

For **Media Security**, select **Media Security Never (MSNV)**. Enter the values for the specified fields as shown in **Figure 31**. Scroll down to the bottom of the screen and click **Return Class of Service** and click on the **Save** button (shown in **Figure 30**).

AVAYA CS1000 Element Manager

Help | Logout

- Class of Service

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:	
- Busy Tone Supervised COT:	
- Calling Line Identification:	
- Calling party:	Calling party Denied (CND)
- Central Office Ringback:	
- Centrex Switchhook Flash:	Centrex 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 M911P:	
- Polarity:	
- Priority:	Low Priority (LPR)
- Restriction level:	Unrestricted (UNR)
- Reversed Ear Piece:	Reversed Ear Piece denied (XREP)
- Short or long line:	
- Transmission Class of Service:	Non-Transmission Compensated (NTC)
- Warning Tone:	Warning Tone Allowed (WTA)
- Reversed Ear Piece:	Reversed Ear Piece denied (XREP)
- ARF Supervised COT:	

Return Class of Service Cancel

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

Figure 31 – Class of Service Configuration Details Page

5.5.7. Administer Calling Line Identification Entries

Select **Customers** → **00** → **ISDN and ESN Networking** on the left pane. Click on **Calling Line Identification Entries** as shown in Figure 32.

AVAYA CS1000 Element Manager

Managing: 10.10.97.96 Username: admin
Customers > 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: (0 - 9999)

Code for processing the called number

National access code:

International access code:

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

Network option: ☒ Coordinated dialing plan routing

Integrated services digital network: ☒

Microsoft converged office dialing plan:

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

Calling Line Identification

Information for incoming/outgoing calls:

Size: (0 - 4000)

Country code: (0 - 9999)

Code displayed as part of calling number

Calling Line Identification Entries

Save Cancel

Figure 32 – ISDN and ESN Networking

Click on **Add** as shown in Figure 33.

AVAYA CS1000 Element Manager

Managing: 10.10.97.96 Username: admin
Customers > Customer 00 > Customer Details > ISDN and ESN Networking > Calling Line Identification Entries

Calling Line Identification Entries

Search for CLID

Start range:

End range:

'End range' should not exceed the CLID size specified

Search

Calling Line Identification Entries

Add Delete Refresh

Figure 33 – Calling Line Identification Entries

The add entry **0** screen is displayed to put the following values for the specified fields and retain the default values for the remaining fields. The Edit Calling Line Identification of existing entry 0 is displayed as shown in **Figure 34**:

- **National Code**: leave it blank.
- **Local Code**: input prefix digits assigned by CenturyLink, in this case it is 6 digits – **303615**. This **Local Code** will be used for call display purpose for Call Type = Unknown.
- **Home Location Code**: input prefix digits assigned by CenturyLink, in this case it is 6 digits - **303615**. This **Home Location Code** will be used for call display purpose for Call Type = National (NPA).
- **Local Steering Code**: input prefix digits assigned by CenturyLink, in this case it is 6 digits - **303615**. 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 for **Roman characters**.

Click on the **Save** button as shown in **Figure 34**

AVAYA CS1000 Element Manager Help | Logout

Managing: **10.10.97.96** Username: admin
 Customers » Customer 00 » Customer Details » ISDN and ESN Networking » Calling Line Identification Entries » Edit Calling Line Identification 0

Edit Calling Line Identification 0

General Properties

National Code: (0 - 999999)
Code for national home number

Local Code: (1-12 digits)
Code for home local number or listed DN

Home Location Code: (1-7 digits)

Local Steering Code: (1-7 digits)

Use DN as DID:

Emergency Services Access

Emergency Local Code: (1-12 digits)
Code for home local number during Emergency calls

Emergency Options: ☐ Home national number for emergency services access calls
☒ Append the originating directory number for emergency services access calls

Calling Party Name Display

Roman characters: ☐

CPND Name:
first name; last name

Expected Length:

Display Format:

Figure 34 – 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 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 35**.

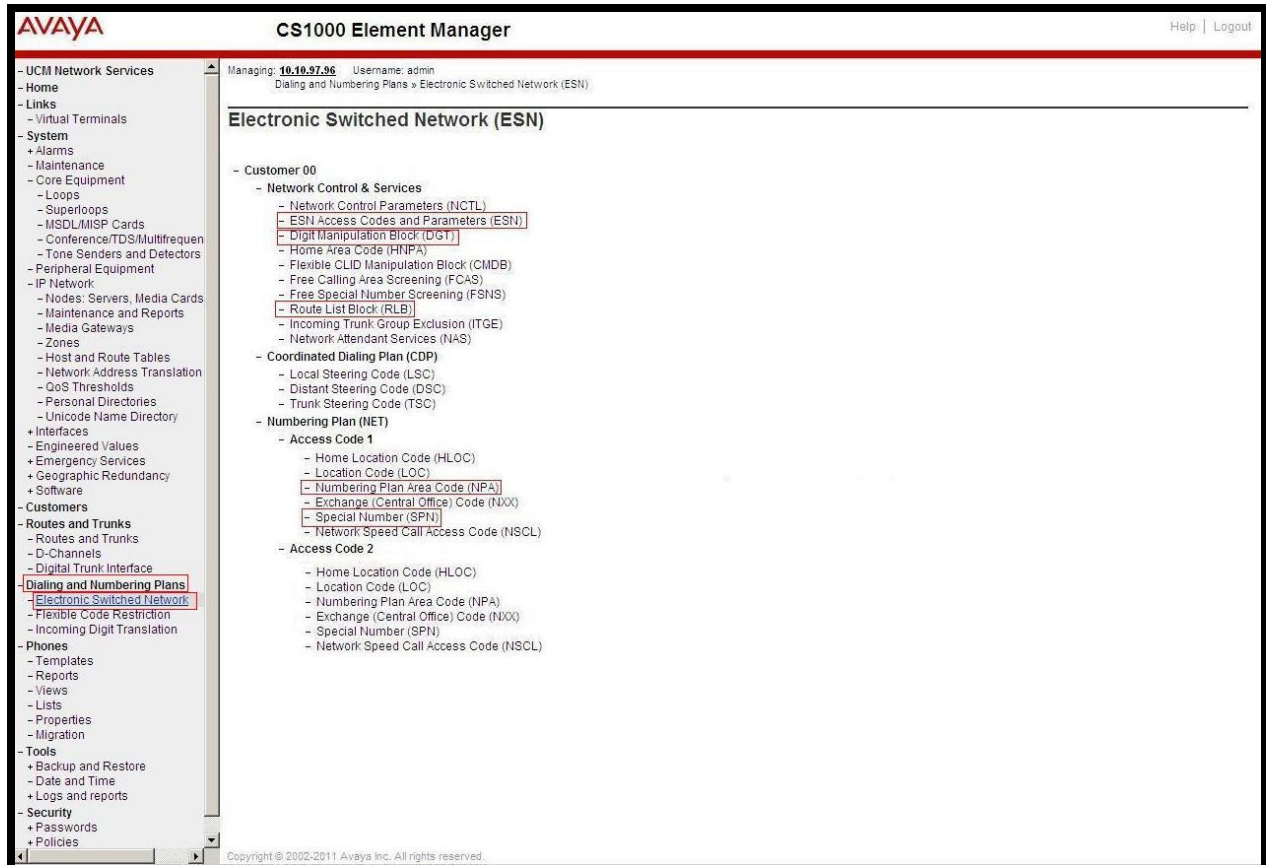


Figure 35 –ESN Configuration Details

Select **ESN Access Codes and Basic Parameters** to define **NARS/BARS Access Code 1** as shown in **Figure 36**.

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

Figure 36 – ESN Access Codes and Basic Parameters

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

Log in 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 35**. Select **Digit Manipulation Block (DGT)**. The **Digit Manipulation Block List** is displayed as shown in **Figure 37**. 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 37 – Add a DMI

The DMI_14 screen will open. In this testing, it is not supposed to delete any number of leading digits, therefore enter **0** for the **Number of leading digits to be deleted** field and select **NPA (Numbering Plan Area)** for the **Call Type to be used by the manipulated digits** and then click on **Submit** button as shown in **Figure 38**.

Figure 38 – DMI_14 Configuration Details

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 35**. 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 39**. The screen shown in **Figure 40** will open.

Figure 39 – Add a Route List Block.

Enter the following values for the specified fields, and retain the default values for the remaining fields (**Figure 40**). 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**)

Figure 40 – RLB_14 Route List Block Configuration Details

5.6.5. Inbound Call – Incoming Digit Translation Configuration

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

Select **Dialing and Numbering Plans** → **Incoming Digit Translation** (not shown) from the left pane to display the **Incoming Digit Translation** screen. Click on the **Edit IDC** button as shown in **Figure 41**.

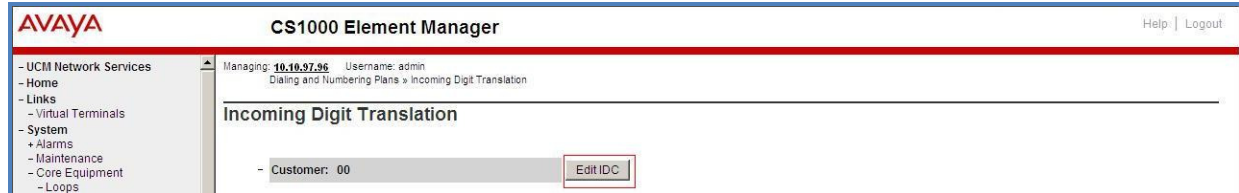


Figure 41 – Incoming Digit Translation

Click on the **New DCNO** to create the digit translation mechanism. In this example, Digit Conversion Tree Number 1 has been created as shown in **Figure 42**.



Figure 42 – Incoming Digit Conversion Property

Detail configuration of the Digit Conversion Tree Configuration is shown in **Figure 43**. The **Incoming Digits** can be added to map to the Converted Digits which would be the associated Communication Server 1000 system phone DN. This **DCNO** has been assigned to route 100 as shown in **Figure 27**.

In the following configuration, the incoming call from PSTN with DID with prefix 303615 will be translated to the associated DN with 4 digits. The DID number 3036157108 is translated to 1700 for Voicemail accessing purpose. The DID number 8553275224 is translated to 7104 for inbound toll free call purpose.

	Incoming Digits	Converted Digits	CPND Name	CPND Language
1	3036157104	7104		Roman characters
2	3036157105	7105		Roman characters
3	3036157106	7106		Roman characters
4	3036157107	7107		Roman characters
5	3036157108	1700		Roman characters
6	8553275224	7104		Roman characters

Figure 43 – 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, 1877, 411, 911 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 35**. Select **Special Number (SPN)**. Enter a SPN number and then click on **to Add** button. **Figure 44** shows all the special numbers used for this testing.

The screenshot displays the AVAYA CS1000 Element Manager web interface. The left-hand navigation pane shows a tree structure with categories like UCM Network Services, Home, Links, System, Customers, Routes and Trunks, Dialing and Numbering Plans (highlighted), Phones, Tools, and Security. Under 'Dialing and Numbering Plans', 'Electronic Switched Network' is selected. The main content area is titled 'Special Number List'. At the top, it shows the managing IP (10.10.97.96) and username (admin). Below this, a breadcrumb trail indicates the path: Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 00 » Numbering Plan (NET) » Access Code 1 » Special Number List. A form for adding a new special number is visible, with a text input field labeled 'Please enter a Special Number' and a 'to Add' button. Below this, a list of existing special numbers is shown, each with an 'Edit' button. The listed numbers are 0, 1877, 411, and 911. For each number, details such as 'Flexible length', 'Inhibit time-out handler', 'Type of call that is defined by the special number', and 'Route list index' are provided.

Special Number	Flexible length	Inhibit time-out handler	Type of call that is defined by the special number	Route list index
Special Number -- 0	14	NO	NONE	14
Special Number -- 1877	11	NO	NONE	14
Special Number -- 411	3	NO	NONE	14
Special Number -- 911	3	NO	NONE	14

Figure 44 – Add a SPN

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 35**. Enter the area code desired in the textbox and click on the **to Add** button. The 1469, 1613, and 303 area codes were used in this configuration as shown in **Figure 45**.

The screenshot displays the AVAYA CS1000 Element Manager web interface. The left-hand navigation pane shows a tree structure with 'Dialing and Numbering Plans' and 'Electronic Switched Network' highlighted. The main content area is titled 'Numbering Plan Area Code List'. At the top, it shows the managing IP (10.10.97.96) and username (admin). Below this, a breadcrumb trail indicates the current path: 'Dialing and Numbering Plans > Electronic Switched Network (ESN) > Customer 00 > Numbering Plan (NET) > Access Code 1 > Numbering Plan Area Code List'. The main section contains a form with the label 'Please enter an area code' and a 'to Add' button. Below the form, there is a list of three existing area codes: 1469, 1613, and 303. Each entry includes an 'Edit' button and details such as 'Route List Index: 14' and 'Incoming Trunk group Exclusion Index: NONE'.

Numbering Plan Area Code	Route List Index	Incoming Trunk group Exclusion Index
1469	14	NONE
1613	14	NONE
303	14	NONE

Figure 45 – Numbering Plan Area Code List

5.7. Administer a Phone

This section describes the creation of Communication Server 1000 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 phone. Refer to **Section 5.4.1** to create a bandwidth zone - **10** for IP phone. 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:

```
REQ: prt
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 FBD WTA LPR MTD FND HTD TDD CRPD
    MWD LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
    POD SLKD CCSD SWD LNA CNDA
    CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBD
    ICDD CDMD LLCN MCTD CLBD AUTU
    GPUD DPUD DNDD CFXD 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 CCBD RTDD RBDD RBHD PGND OCBD 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 7104 0   MARP < --- Set the position of DN 7104 to display on key 0 of the phone
    CPND
    CPND_LANG ROMAN
    NAME Cent1 < --- 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) and 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** to **ddgd**. Communication Server 1000 will include “Privacy:id” in the SIP message header before sending it to CenturyLink.

```

>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**. Communication Server 1000 will not send the Privacy header to CenturyLink.

```
>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 46**.

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

The screenshot displays the 'AVAYA CS1000 Element Manager' interface. On the left is a navigation tree with categories like 'UCM Network Services', 'System', 'Interfaces', 'Customers', 'Routes and Trunks', 'Dialing and Numbering Plans', 'Phones', 'Tools', 'Security', and 'Login Options'. The 'Customers' section is expanded, showing '00' as the selected customer. The main content area is titled 'Call redirection by day:' and contains several configuration sections:

- Call redirection by day:** Includes input fields for 'Days for day option 0', 'Days for day option 1', 'Days for day option 2', and 'Days for day option 3'.
- Redirection Holidays:** Includes a checkbox for 'Do not disturb hunting:'.
- Total redirection count limit:** A dropdown menu set to '0'.
- Options:** A list of checkboxes for 'Call forward reminder tone for 500/2500 sets', 'CFNA treatment for call waiting calls on a DN', 'DID call to second degree busy treatment', 'Message center' (checked), and 'Prevention of reciprocal call forward' (checked).
- Call forward:** Radio buttons for 'Originating' (selected) and 'Forwarding'.
- Number of normal ringing cycles for CFNA:** Three dropdown menus for 'Option 0', 'Option 1', and 'Option 2', all set to '3'.
- Number of distinctive ringing cycles for CFNA:** Three dropdown menus for 'Option 0', 'Option 1', and 'Option 2', all set to '3'.
- Calls routed to message center:** Includes checkboxes for 'No answer DID calls:', 'No answer non-DID calls:', and 'DID calls to busy telephones:'.

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

Figure 46 – Call Redirection

To enable **Call Forward All Call (CFAC)** for a phone over a 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 616139675205.

```
ld 11
REQ: chg
TYPE: 2007
TN 96 0 0 4

ECHG yes
ITEM cls CFXA SFA
ITEM key 19 CFW 16 616139675205
```

To enable **Call Forward Busy (CFB)** for phone over trunk by using **LD 11**, change its **CLS** to **FBA**, **HTA**, and **SFA**, then program the forward number as **HUNT** and **FDN**. Following is the configuration of a phone has **CFB** enabled with forward number is 616139675205.

```
ld 11
REQ: chg
TYPE: 2007
TN 96 0 0 4
ECHG yes
ITEM cls FBA HTA SFA
ITEM hunt 616139675205
ITEM fdn 616139675205
```

To enable **Call Forward No Answer (CFNA)** for a phone over a trunk by using **LD 11**, change its **CLS** to **FNA**, and **SFA**, then program the forward number as **HUNT** and **FDN**. Following is the configuration of a phone that has CFNA enabled with forward number 616139675205.

```
ld 11
REQ: chg
TYPE: 2007
TN 96 0 0 4
ECHG yes
ITEM cls FNA SFA
ITEM hunt 616139675205
ITEM fdn 616139675205
```

5.7.4. Enable Call Waiting for Phone

This section shows how to configure the Call Waiting feature at the phone level.

Log in to the Call Server CLI (please refer to **Section 5.1.2** for more details), configure Call Waiting feature for phone by using **LD 11** to change **CLS** to **HTD**, and **SWA** and adding a **CWT** key.

```
ld 11
REQ: chg
TYPE: 2002p2
TN 96 0 0 2
ECHG yes
ITEM cls HTD SWA
ITEM key 2 cwt
```

...

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.
- SIP Entities corresponding to Communication Server 1000, 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.

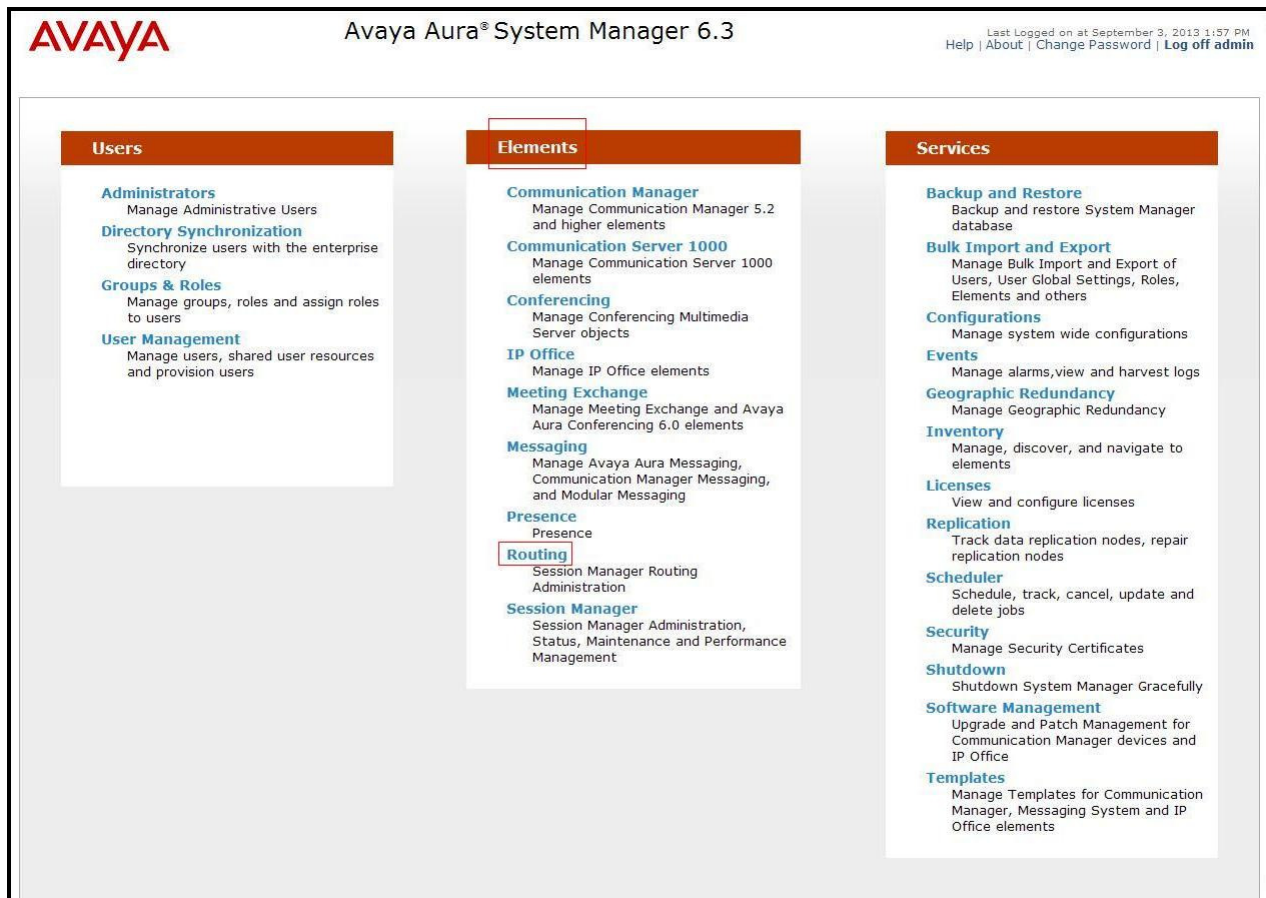


Figure 47 – System Manager Home Screen

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.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The top header includes the Avaya logo, the product name 'Avaya Aura® System Manager 6.3', and a user status bar indicating 'Last Logged on at September 3, 2013 1:57 PM' with links for 'Help', 'About', 'Change Password', and 'Log off admin'. The interface is divided into three main sections: a left-hand navigation tree, a top breadcrumb bar, and a main content area.

The left-hand navigation tree is expanded to show the 'Routing' section, which includes sub-items: Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The top breadcrumb bar shows the path 'Home / Elements / Routing'. The main content area is titled 'Introduction to Network Routing Policy' and contains the following text:

Network Routing Policy consists of several routing applications like "Domains", "Locations", "SIP Entities", etc.
 The recommended order to use the routing applications (that means the overall routing workflow) to configure your network configuration is as follows:

- Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).
- Step 2: Create "Locations"
- Step 3: Create "Adaptations"
- Step 4: Create "SIP Entities"
 - SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
 - Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)
 - Assign the appropriate "Locations", "Adaptations" and "Outbound Proxies"
- Step 5: Create the "Entity Links"
 - Between Session Managers
 - Between Session Managers and "other SIP Entities"
- Step 6: Create "Time Ranges"
 - Align with the tariff information received from the Service Providers
- Step 7: Create "Routing Policies"
 - Assign the appropriate "Routing Destination" and "Time Of Day"
 (Time Of Day = assign the appropriate "Time Range" and define the "Ranking")
- Step 8: Create "Dial Patterns"
 - Assign the appropriate "Locations" and "Routing Policies" to the "Dial Patterns"
- Step 9: Create "Regular Expressions"

Figure 48 – 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 **bvwdev7.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.
- **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.

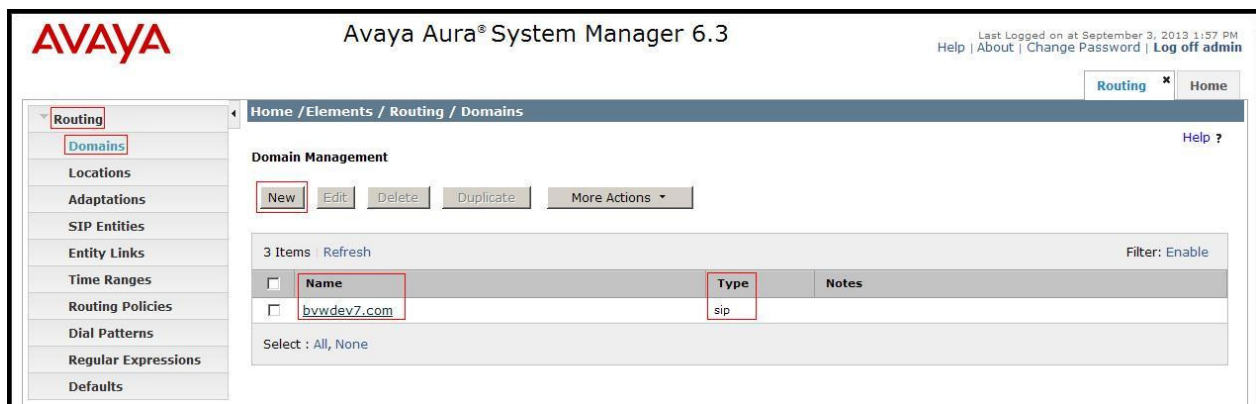


Figure 49 – Domain Management

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 Communication Server 1000, 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 Avaya Aura® System Manager 6.3 Last Logged on at September 3, 2013 1:57 PM
Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Locations Help ?

Location Details Commit Cancel

General

* Name:

Notes:

Dial Plan Transparency in Survivable Mode

Enabled: ☐

Listed Directory Number:

Associated CM SIP Entity:

Overall Managed Bandwidth

Managed Bandwidth Units:

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

Per-Call Bandwidth Parameters

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

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

* Minimum Multimedia Bandwidth: Kbit/Sec

* Default Audio Bandwidth: Kbit/sec

Alarm Threshold

Overall Alarm Threshold: %

Figure 50 – 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

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.33.*	<input type="text"/>
<input type="checkbox"/>	* 10.10.97.*	<input type="text"/>
<input type="checkbox"/>	* 10.10.98.*	<input type="text"/>

Select : All, None

Commit Cancel

Figure 51 – IP Ranges Configuration

Click **Commit** to save.

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

6.4. Add SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to Session Manager which includes Communication Server 1000 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 Communications Server 1000 and the 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
- Session Border Controller for Enterprise SIP Entity

6.4.1. 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 is entered for **FQDN or IP Address** **10.33.10.26**. 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 top navigation bar includes the Avaya logo, the title 'Avaya Aura® System Manager 6.3', and a user status bar indicating 'Last Logged on at September 3, 2013 1:57 PM' with links for 'Help', 'About', 'Change Password', and 'Log off admin'. A breadcrumb trail shows 'Home / Elements / Routing / SIP Entities'. The left sidebar contains a menu with 'Routing' selected, and sub-items: Domains, 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 several input fields: 'Name' (SM63), 'FQDN or IP Address' (10.33.10.26), 'Type' (Session Manager), 'Notes' (SM R6.3), 'Location' (Belleville), 'Outbound Proxy' (empty), 'Time Zone' (America/Toronto), and 'Credential name' (empty). 'Commit' and 'Cancel' buttons are at the top right. At the bottom, there is a 'SIP Link Monitoring' section with a dropdown set to 'Use Session Manager Configuration'.

Figure 52 – 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 **Commit** (not shown) to save.

The compliance test used port **5060** with **UDP** for connecting to Communication Server 1000 and Avaya SBCE.

Other entries defined for other projects as shown in the screen were not used.

Port

TCP Failover port:

TLS Failover port:

2 Items Refresh Filter: Enable

<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	5060	UDP	bvwdev7.com	

Select : All, None

Figure 53 – Session Manager SIP Entity Port

6.4.2. Configure Communication Server 1000 SIP Entity

The following screen shows the addition of the Communication Server 1000 SIP Entity named **car3-ssg-carrier**. In order for Session Manager to send SIP service provider traffic on a separate Entity Link to Communication Server 1000, it is necessary to create a separate SIP Entity for Communication Server 1000, 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 Communication Server 1000 signaling Node **10.10.97.178**. The **Location** field is set to **Belleville** which is the Location that includes the subnet where Communication Server 1000 resides. Select **Time Zone** as **America/Toronto** and **Type** as **Other**.

AVAYA Avaya Aura® System Manager 6.3 Last Logged on at September 3, 2013 1:57 PM
Help | About | [Change Password](#) | [Log off admin](#)

Routing * Home

Home / Elements / Routing / SIP Entities Help ?

SIP Entity Details

General

* **Name:** car3-ssg-carrier

* **FQDN or IP Address:** 10.10.97.178

Type: Other

Notes: For CenturyLink

Adaptation:

Location: Belleville

Time Zone: America/Toronto

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

CommProfile Type Preference:

Figure 54 – Communication Server 1000 SIP Entity

6.4.3. Configure Avaya SBCE SIP Entity

The following screen shows the addition of Avaya SBCE SIP entity named **SBCE**. The **FQDN or IP Address** field is set to the IP address of the SBC's private network interface **10.10.98.13**. The **Location** field is set to **Belleville** which includes the subnet where the Avaya SBCE resides. Select **Time Zone** as **America/Toronto** and **Type** as **Other**.

The screenshot displays the Avaya Aura System Manager 6.3 web interface. The left-hand navigation pane shows the 'Routing' menu expanded, with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and 'General'. The form contains the following fields and values:

- Name:** SBCE
- FQDN or IP Address:** 10.10.98.13
- Type:** Other (selected from a dropdown)
- Notes:** SBCE R6.2
- Adaptation:** (empty dropdown)
- Location:** Belleville (selected from a dropdown)
- Time Zone:** America/Toronto (selected from a dropdown)
- Override Port & Transport with DNS SRV:** ☐
- * 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)

Buttons for 'Commit' and 'Cancel' are visible at the top right of the form area. The top of the page shows the Avaya logo, the title 'Avaya Aura® System Manager 6.3', and a user status bar indicating 'Last Logged on at September 3, 2013 1:57 PM' with links for 'Help', 'About', 'Change Password', and 'Log off admin'.

Figure 55 – Avaya SBCE SIP Entity

6.5. 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 Communication Server 1000 and one to the Avaya SBCE.

To add an Entity Link, navigate to **Routing → Entity Links** in the left-hand navigation pane and click on the **New** button in the right pane (not shown). 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 6.4**.
- **Port:** Port number on which the other system receives SIP requests from the Session Manager. For the Communication Server 1000 Entity Link, this must match the **port** defined on the Communication Server 1000 in **Section 5.5.2**.

- **Trusted:** Check this box. Note: If this box is not checked, calls from the associated SIP Entity specified in **Section 6.4** will be denied.

Click **Commit** to save.

The following screens illustrate the Entity Link to the Communication Server 1000. The protocol and ports defined here must match the values used for the Communication Server 1000 signaling in **Section 5.5.2**.

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar contains a navigation menu with options: Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links (highlighted), Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Entity Links' and includes a 'Commit' button and a 'Cancel' button. Below these is a table with the following columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Connection Policy, Deny New Service, and Notes. A single row is displayed with the following values: Name: SM63_car3-ssg-car, SIP Entity 1: SM63, Protocol: UDP, Port: 5060, SIP Entity 2: car3-ssg-carrier, Port: 5060, Connection Policy: trusted, Deny New Service: (checkbox), and Notes: (text field). The table is filtered by 'Enable'.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service	Notes
* SM63_car3-ssg-car	* SM63	UDP	* 5060	* car3-ssg-carrier	* 5060	trusted	<input type="checkbox"/>	

Figure 56 – Communication Server 1000 Entity Link

The following screens illustrate the Entity Links to the Avaya SBCE. The protocol and ports defined here must match the values used for the Avaya SBCE mentioned in **Section 7.2.7**

The screenshot shows the Avaya Aura System Manager 6.3 interface. The left sidebar contains a navigation menu with options: Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links (highlighted), Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Entity Links' and includes a 'Commit' button and a 'Cancel' button. Below these is a table with the following columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Connection Policy, Deny New Service, and Notes. A single row is displayed with the following values: Name: SM63_SBCE_5060, SIP Entity 1: SM63, Protocol: UDP, Port: 5060, SIP Entity 2: SBCE, Port: 5060, Connection Policy: trusted, Deny New Service: (checkbox), and Notes: (text field). The table is filtered by 'Enable'.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Deny New Service	Notes
* SM63_SBCE_5060	* SM63	UDP	* 5060	* SBCE	* 5060	trusted	<input type="checkbox"/>	

Figure 57 – Avaya SBCE Entity Link

6.6. Configure Time Ranges

Time Ranges are configured for time-based-routing. In order to add Time Ranges, select **Routing** → **Time Ranges** and then click **New** button. The Routing Policies shown subsequently will use the **24/7** range since time-based routing was not the focus of these Application Notes.

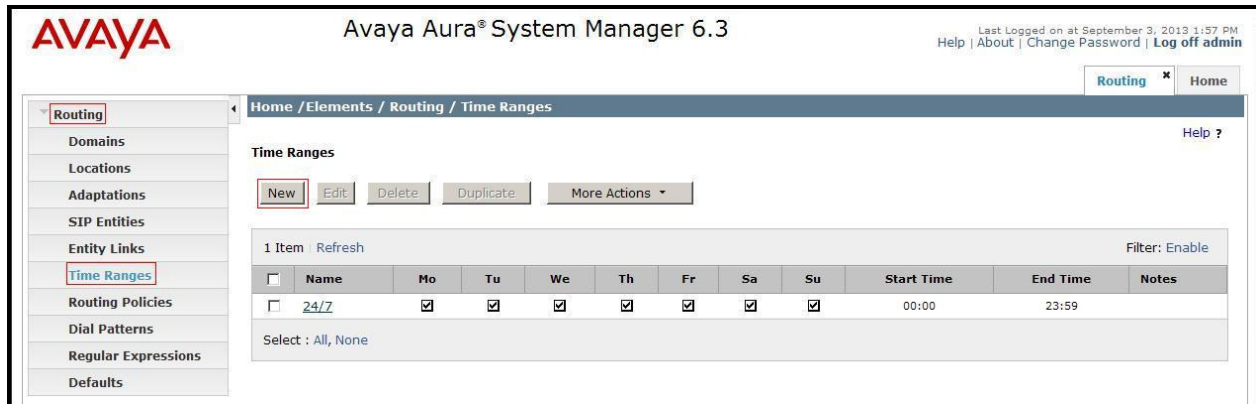


Figure 58 – Time Ranges

6.7. Add Routing Policies

Routing Policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.4**. Two Routing Policies must be added: one for the Communication Server 1000 and one for the 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 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.
- **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 **To car3-ssg-carrier** associated with incoming PSTN calls from CenturyLink to the Communication Server 1000. Observe the **SIP Entity as Destination** is the entity named **car3-ssg-carrier**.

Avaya Aura® System Manager 6.3

Last Logged on at September 3, 2013 1:57 PM
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing Policy Details

Commit Cancel

General

Name: To car3-scg-carrier

Disabled: ☐

Retries: 0

Notes: To car3-scg-carrier

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
car3-scg-carrier	10.10.97.178	Other	For CenturyLink

Figure 59 – Routing to Communication Server 1000

The following screen shows the **Routing Policy Details** for the policy named **To_CenturyLink**. This is associated with outgoing calls from the Communication Server 1000 to the PSTN via CenturyLink, through the Avaya SBCE. Observe the **SIP Entity as Destination** is the entity named **SBCE**.

Avaya Aura® System Manager 6.3

Last Logged on at September 5, 2013 10:51 AM
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing Policy Details

Commit Cancel

General

Name: To_CenturyLink

Disabled: ☐

Retries: 0

Notes: For CenturyLink

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
SBCE	10.10.98.13	Other	SBCE R6.2

Figure 60 – Routing to CenturyLink

6.8. 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 Communication Server 1000 to CenturyLink 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., 1877 Toll free call, 411, etc.) were similarly defined.

The first example shows that outbound 11-digit dialed numbers that begin with **1613** and have a destination SIP Domain of **bvwddev7.com** uses the **SBCE** Routing Policy as defined in **Section 6.7**.

AVAYA

Avaya Aura® System Manager 6.3

Last Logged on at September 5, 2013 10:51 AM

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

Routing

Home

Home / Elements / Routing / Dial Patterns

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

Dial Pattern Details

Commit

Cancel

Help ?

General

Pattern: 1613

Min: 11

Max: 11

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: bvwddev7.com

Notes: CenturyLink Outbound Calls

Originating Locations and Routing Policies

Add

Remove

1 Item

Refresh

Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Belleville	GSSCP Belleville	To_CenturyLink	0	<input type="checkbox"/>	SBCE	For CenturyLink

Select : All, None

Figure 61 – Dial Pattern_1613

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

The second example shows that inbound 10-digit numbers that start with **303** uses Routing Policy **car3-ssg-carrier** as defined in **Section 6.7**. This Dial Pattern matches the DID numbers assigned to the enterprise by CenturyLink.

Avaya Aura® System Manager 6.3

Last Logged on at September 5, 2013 10:51 AM
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing | Home

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

General

* **Pattern:** 303

* **Min:** 10

* **Max:** 10

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: bvwddev7.com

Notes: CenturyLink Inbound Calls

Originating Locations and Routing Policies

Add **Remove**

1 Item [Refresh](#) Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Belleville	GSSCP Belleville	To car3-ssg-carrier	0	<input type="checkbox"/>	car3-ssg-carrier	To car3-ssg-carrier

Select : All, None

Figure 62 – Dial Pattern_303

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

Avaya Aura® System Manager 6.3

Last Logged on at September 5, 2013 10:51 AM
[Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

Routing | Home

Home / Elements / Routing / Dial Patterns

Dial Patterns

New **Edit** **Delete** **Duplicate** **More Actions**

27 Items [Refresh](#) Filter: Enable

<input type="checkbox"/>	Pattern	Min	Max	Emergency Call	Emergency Type	Emergency Priority	SIP Domain	Notes
<input type="checkbox"/>	0	1	14	<input type="checkbox"/>			bvwddev7.com	CenturyLink Outbound Calls
<input type="checkbox"/>	1469	11	11	<input type="checkbox"/>			bvwddev7.com	CenturyLink Outbound Calls
<input type="checkbox"/>	1613	11	11	<input type="checkbox"/>			bvwddev7.com	CenturyLink Outbound Calls
<input type="checkbox"/>	1877	11	11	<input type="checkbox"/>			bvwddev7.com	CenturyLink Outbound Toll Free Calls
<input type="checkbox"/>	303	10	10	<input type="checkbox"/>			bvwddev7.com	CenturyLink Inbound Calls
<input type="checkbox"/>	3034	10	10	<input type="checkbox"/>			bvwddev7.com	CenturyLink Outbound Local Calls
<input type="checkbox"/>	411	3	3	<input type="checkbox"/>			bvwddev7.com	CenturyLink 411 Outbound Calls
<input type="checkbox"/>	855	10	10	<input type="checkbox"/>			bvwddev7.com	CenturyLink Inbound Toll Free Calls
<input type="checkbox"/>	911	3	3	<input type="checkbox"/>			bvwddev7.com	CenturyLink 911 Outbound Calls

Select : All, None < Previous Page 1 of 2 Next >

Figure 63 – Dial Pattern List

7. Configure Session Border Controller for Enterprise

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

Avaya elements reside on the Private side and the CenturyLink SIP Trunk service reside 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 **Section 11** of these Application Notes.

7.1. Log into the Avaya 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**.



AVAYA

Log In

Username:

Password:

**Session Border Controller
for Enterprise**

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.

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

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

© 2011 - 2013 Avaya Inc. All rights reserved.

Figure 64 - 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 one 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** → **Add**

- Enter Profile name: **SM63**
- Check **T.38 Support** as **Yes**.
- All other options on the **General** Tab 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 is shown that Session Manager server interworking (named: **SM63**) was added.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header shows the title "Session Border Controller for Enterprise" and the Avaya logo. On the left, a sidebar menu lists various configuration areas, with "Global Profiles" expanded and "Server Interworking" highlighted. The main content area is titled "Interworking Profiles: SM63" and features an "Add" button. Below this, a list of existing profiles is shown, including "cs2100", "avaya-ru", "OCS-Edge-Server", "cisco-ccm", "cups", "OCS-FrontEnd-Server", and "SM63". The "SM63" profile is selected, and its configuration is displayed in a tabbed interface. The "General" tab is active, showing a table of parameters and their values. The "T.38 Support" parameter is highlighted with a red box and set to "Yes". Other parameters include "Hold Support" (NONE), "180 Handling" (None), "181 Handling" (None), "182 Handling" (None), "183 Handling" (None), "Refer Handling" (No), "3xx Handling" (No), "Diversion Header Support" (No), "Delayed SDP Handling" (No), "URI Scheme" (SIP), and "Via Header Format" (RFC3261). The "Privacy" section shows "Privacy Enabled" (No), "User Name", "P-Asserted-Identity" (No), "P-Preferred-Identity" (No), and "Privacy Header". The "DTMF" section is also visible at the bottom.

General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
T.38 Support	Yes
URI Scheme	SIP
Via Header Format	RFC3261

Privacy	
Privacy Enabled	No
User Name	
P-Asserted-Identity	No
P-Preferred-Identity	No
Privacy Header	

DTMF

Figure 65 - Server Interworking – Avaya site

7.2.2. Configure Server Interworking – CenturyLink site

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

- Enter Profile name: **CenturyLink**
- Check **T.38 Support** as **Yes**.
- All other options on the **General** Tab 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 is shown that CenturyLink server interworking (named: **CenturyLink**) was added.

The screenshot displays the Avaya Session Border Controller for Enterprise web interface. The left-hand navigation menu is expanded, showing the path: **Global Profiles** → **Server Interworking**. The main content area is titled "Interworking Profiles: CenturyLink" and features an "Add" button. Below this, a list of existing profiles is shown, including "cs2100", "avaya-ru", "OCS-Edge-Server", "cisco-ccm", "cups", "OCS-FrontEnd-Server", "SM63", and "CenturyLink". The "CenturyLink" profile is selected. The configuration tabs are "General", "Timers", "URI Manipulation", "Header Manipulation", and "Advanced". The "General" tab is active, showing a table of configuration options. The "T.38 Support" option is highlighted with a red box and set to "Yes".

General	
Hold Support	NONE
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
T.38 Support	Yes
URI Scheme	SIP
Via Header Format	RFC3261

Privacy	
Privacy Enabled	No
User Name	
P-Asserted-Identity	No
P-Preferred-Identity	No
Privacy Header	

DTMF	
------	--

Figure 66 - Server Interworking – CenturyLink site

7.2.3. Configure URI Groups

The URI Group feature allows administrator to create any number of logical URI groups that are comprised of individual SIP subscribers located in that particular domain or group.

The following URI Group configuration is used for this specific testing in DevConnect Lab environment. The URI-Group named **CenturyLink** was used to match the “From” and “To” headers in a SIP call dialog received from both Enterprise and CenturyLink SIP Trunk service. If there is a match, the Avaya SBCE will apply the appropriate Routing profile (see **Section 7.2.4, 7.2.5**), Server Flow (see **Section 7.4.4**), and Session Flow (see **section 7.4.5**) to route incoming and outgoing calls to the right destinations. In production environment, there is not a requirement to define this URI.

From the menu on the left-hand side, select **Global Profiles → URI Groups**. Select **Add**.

- Enter Group Name: **CenturyLink**.
- Edit the URI Type: **Regular Expression** (not shown).
- **Add URI**: **.*10\10\98\111** (Avaya SBCE public interface IP address), **.*10\10\98\13** (Avaya SBCE internal interface IP address), **.*10\10\33\26** (Session Manager IP address), **.*192\168\33\40** (CenturyLink Session SIP Signaling server IP address), **.*192\168\33\41** (CenturyLink Usage SIP Signaling IP address), **.*anonymous\invalid** (Anonymous URI), **.*bywdev7\com** (Enterprise domain).
- Click **Finish** (not shown))

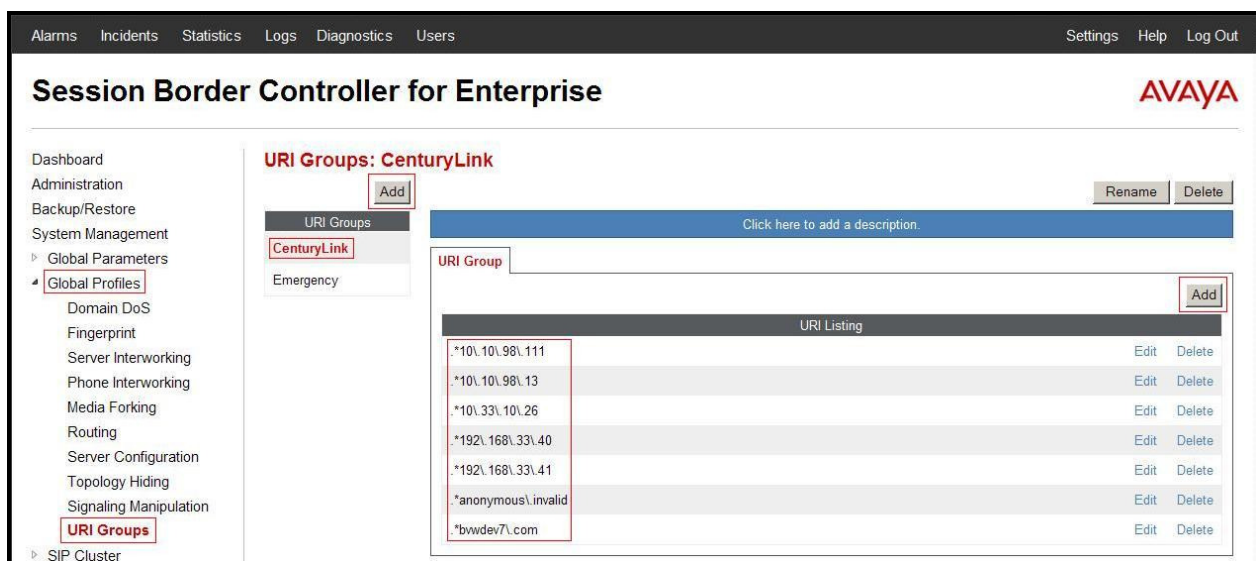


Figure 67 - URI Group

7.2.4. 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 → Add**

Enter Profile Name: **CenturyLink_To_SM63**

- **URI Group: CenturyLink**
- **Next Hop Server 1: 10.33.10.26:5060** (Session Manager IP address)
- Check **Routing Priority based on Next Hop Server** (not shown)
- **Outgoing Transport: UDP** (not shown)
- Click **Finish** (not shown).

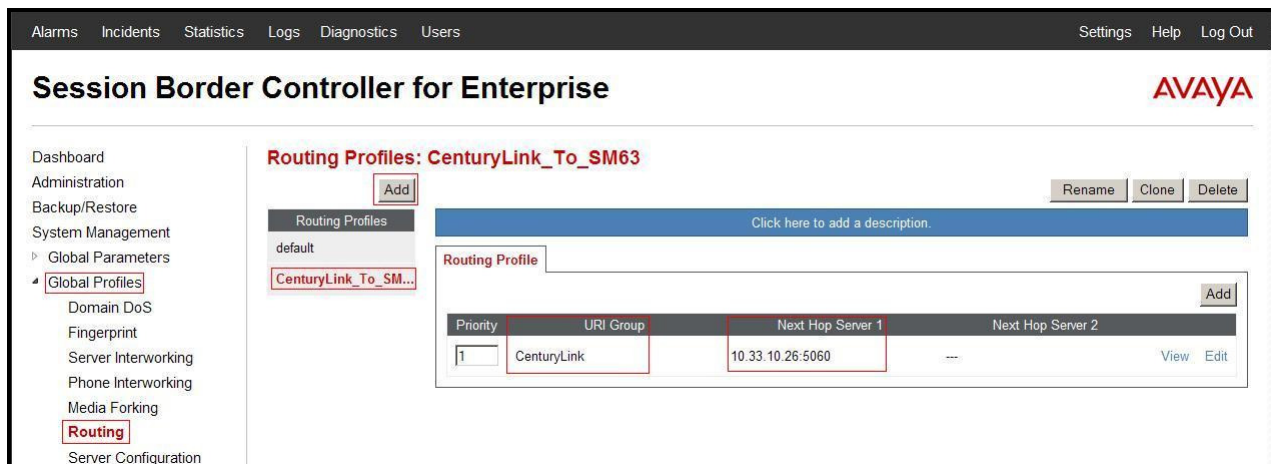


Figure 68 - Routing to Avaya

7.2.5. Configure Routing – CenturyLink 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 → Add**

Enter Profile Name: **SM63_To_CenturyLink**

- **URI Group: CenturyLink**
- **Next Hop Server 1: 192.168.33.41** (CenturyLink Usage SIP Signaling server IP address)
- Check **Routing Priority based on Next Hop Server** (not shown)
- **Outgoing Transport: UDP** (not shown)
- Click **Finish** (not shown).

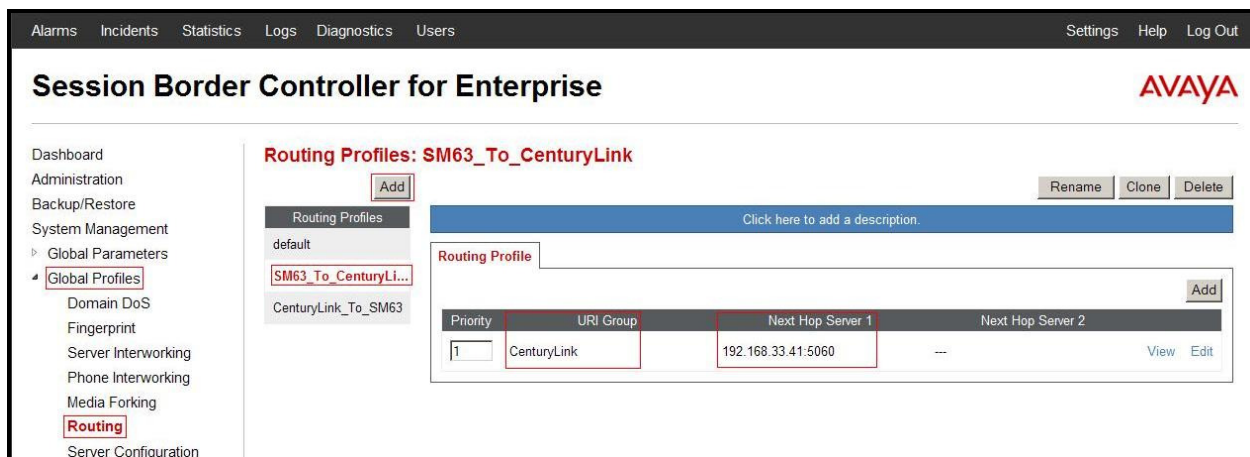


Figure 69 - Routing to CenturyLink

7.2.6. Configure Signaling Manipulation

The Avaya's SIP signaling header manipulation feature is used for the Avaya SBCE product. This 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: **CenturyLink**
 - Edit the script to replace MIME from the body of SIP message
 - Edit the script to remove unwanted parameters in body of SIP message
 - Edit the script to remove unwanted SIP headers
 - Click **Save** (not shown)

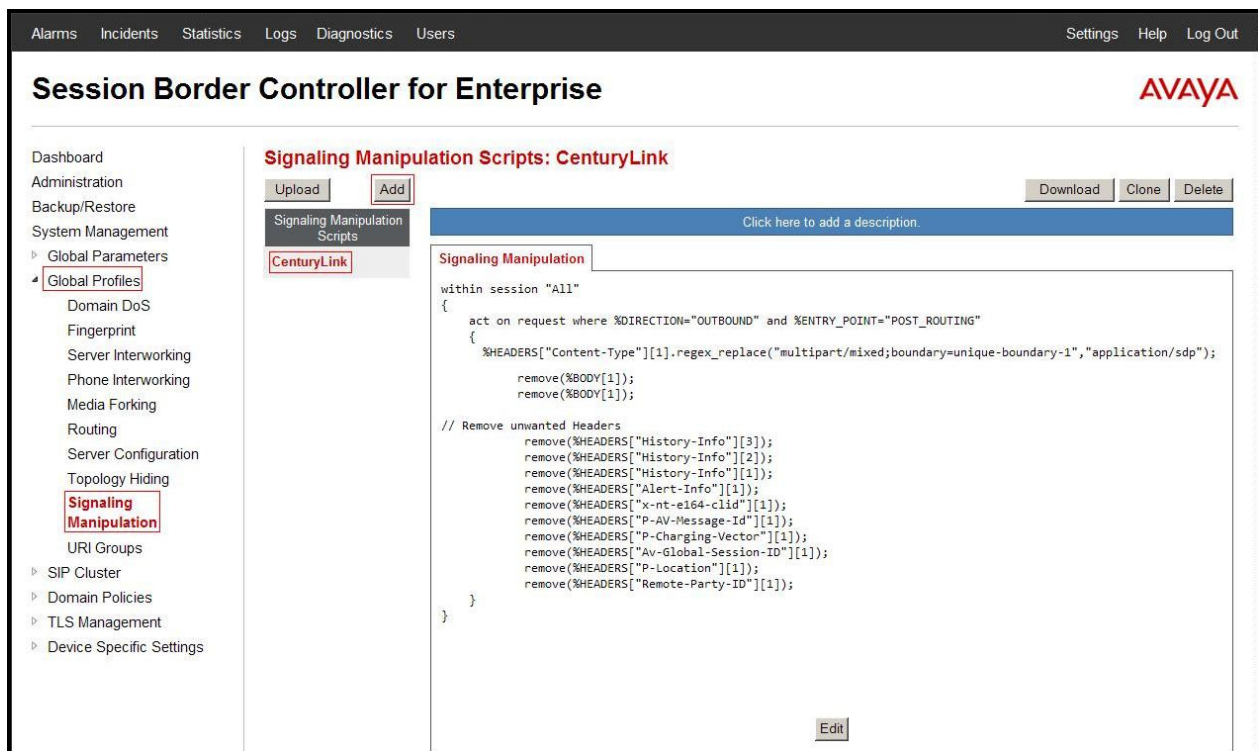


Figure 70 – Signaling Manipulation CenturyLink

7.2.7. 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** → **Add**.

Enter profile name: **SM63**

On **General** tab enter the following:

- **Server Type:** Select **Call Server**
- **IP Address/FQDNs:** **10.33.10.26** (Session Manager IP Address)
- **Supported Transports:** **UDP**
- **UDP Port:** **5060**

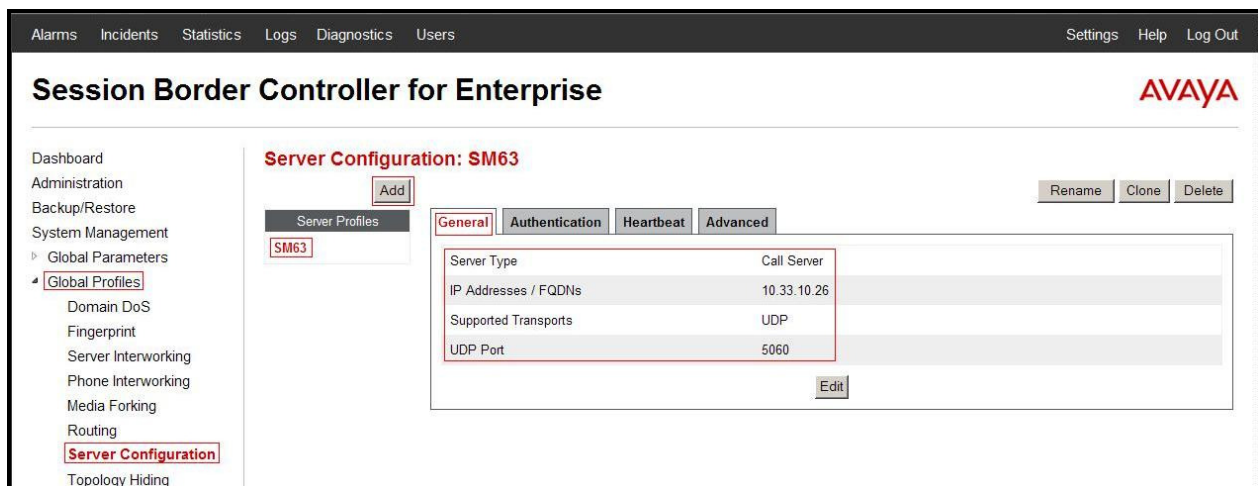


Figure 71 - Session Manager General Server Configuration

On the **Advanced** tab:

- Select **SM63** for **Interworking Profile**.

Click **Finish** (not shown).

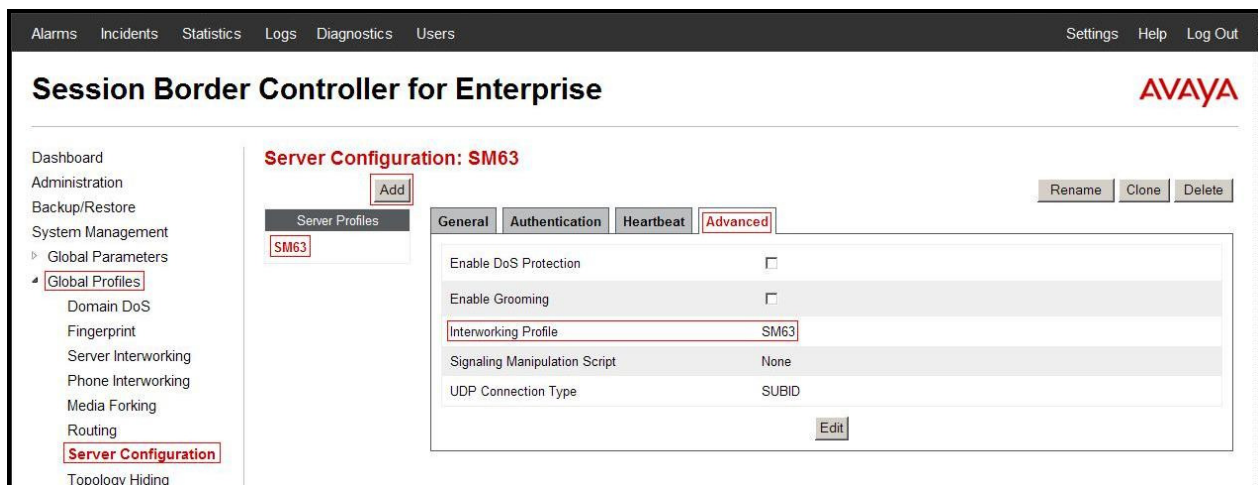


Figure 72 - Session Manager Advanced Server Configuration

7.2.8. Configure Server – CenturyLink

From the menu on the left-hand side, select **Global Profiles** → **Server Configuration** → **Add**.

Enter profile name: **CenturyLink**

On **General** tab enter the following:

- **Server Type:** Select **Trunk Server**

- **IP Address: 192.168.33.40** (CenturyLink Session Signaling server IP Address) and **192.168.33.41** (CenturyLink Usage Signaling server IP Address)
- **Supported Transports: UDP**
- **UDP Port: 5060**

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left sidebar contains a navigation menu with items like Dashboard, Administration, Backup/Restore, System Management, Global Parameters, Global Profiles, Domain DoS, Fingerprint, Server Interworking, Phone Interworking, Media Forking, Routing, Server Configuration (highlighted), and Topology Hiding. The main content area is titled "Server Configuration: CenturyLink" and has tabs for General, Authentication, Heartbeat, and Advanced. The General tab is active, showing a table with the following configuration:

Server Type	Trunk Server
IP Addresses / FQDNs	192.168.33.40, 192.168.33.41
Supported Transports	UDP
UDP Port	5060

Buttons for "Add", "Rename", "Clone", "Delete", and "Edit" are visible.

Figure 73 - CenturyLink General Server Configuration

On the **Advanced** tab enter the following:

- **Interworking Profile:** select **CenturyLink**
- **Signaling Manipulation Script:** select **CenturyLink**

Click **Finish** (not shown).

The screenshot shows the Avaya Session Border Controller for Enterprise web interface, specifically the Advanced tab of the CenturyLink Server Configuration. The configuration table is as follows:

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	CenturyLink
Signaling Manipulation Script	CenturyLink
UDP Connection Type	SUBID

Buttons for "Add", "Rename", "Clone", "Delete", and "Edit" are visible.

Figure 74 - CenturyLink Advanced Server Configuration

7.2.9. 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 **Add**, enter Profile Name: **CenturyLink_To_SM63**.

- For the Header **From**,
 - In the **Criteria** column select **IP/Domain**
 - In the **Replace Action** column select: **Overwrite**
 - In the **Overwrite Value** column: **bwdev7.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: **bwdev7.com**
- For the Header **To**,
 - In the **Criteria** column select **IP/Domain**
 - In the **Replace Action** column select: **Overwrite**
 - In the **Overwrite Value** column: **bwdev7.com**

Click **Finish** (not shown).

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Settings, Help, and Log Out. The main header displays 'Session Border Controller for Enterprise' and the Avaya logo. On the left, a sidebar menu lists various system management options, with 'Global Profiles' expanded to show 'Topology Hiding' selected. The main content area is titled 'Topology Hiding Profiles: CenturyLink_To_SM63'. It features an 'Add' button, a 'Rename' button, a 'Clone' button, and a 'Delete' button. Below these is a table with the following data:

Header	Criteria	Replace Action	Overwrite Value
From	IP/Domain	Overwrite	bwdev7.com
Request-Line	IP/Domain	Overwrite	bwdev7.com
To	IP/Domain	Overwrite	bwdev7.com

An 'Edit' button is located below the table.

Figure 75 - Topology Hiding Session Manager

7.2.10. Configure Topology Hiding – CenturyLink site

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

Select **Add Profile**, enter Profile Name: **SM63_To_CenturyLink**.

- For the Header **From**,
 - In the **Criteria** column select **IP/Domain**
 - In the **Replace Action** column select: **Overwrite**
 - In the **Overwrite Value** column: **10.10.98.111**
- For the Header **Request-Line**,
 - In the **Criteria** column select **IP/Domain**
 - In the **Replace Action** column select: **Overwrite**
 - In the **Overwrite Value** column: **192.168.33.41**
- For the Header **To**,
 - In the **Criteria** column select **IP/Domain**
 - In the **Replace Action** column select: **Overwrite**
 - In the **Overwrite Value** column: **192.168.33.41**

Click **Finish** (not shown).

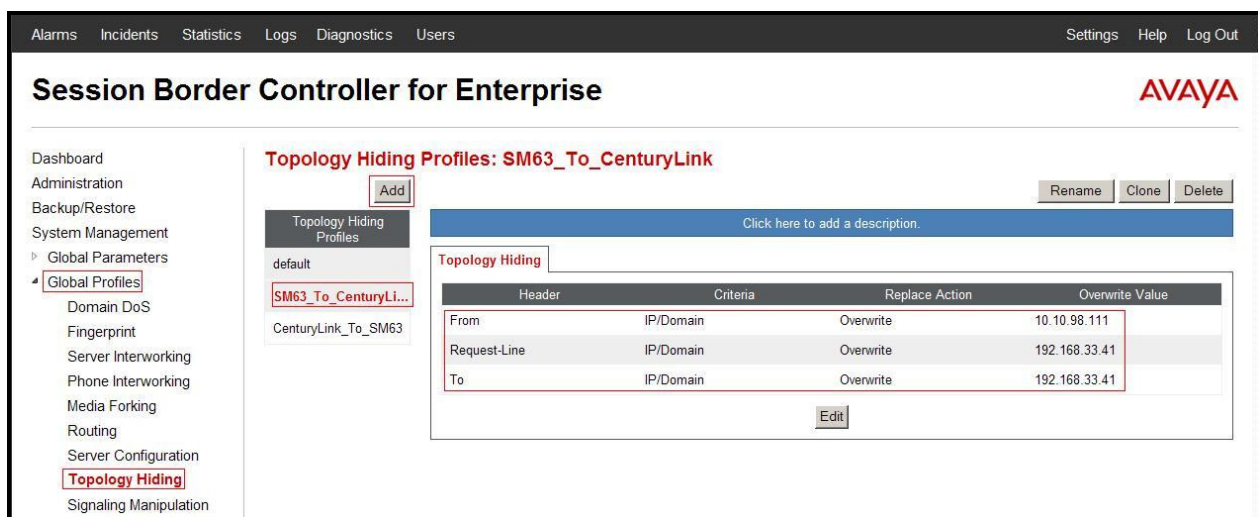


Figure 76 - Topology Hiding CenturyLink

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.

7.3.1. Create Application Rules

Application Rules allow one to define which types of SIP-based Unified Communications (UC) applications the Avaya SBCE security device will protect: voice, video, and/or Instant Messaging (IM). In addition, one can determine the maximum number of concurrent voice and video sessions so that the network will process to prevent resource exhaustion.

From the menu on the left-hand side, select **Domain Policies** → **Application Rules**.

- Select the **default** Rule
- Select **Clone** button
 - Name: **SM63_Cent_AppR**
 - Click **Finish** (not shown).

The screenshot shows the Avaya Session Border Controller for Enterprise web interface. The left-hand navigation menu is expanded, showing 'Domain Policies' and 'Application Rules' highlighted. The main content area displays the configuration for 'Application Rules: SM63_Cent_AppR'. At the top, there are buttons for 'Add', 'Filter By Device...', 'Rename', 'Clone', and 'Delete'. Below this is a table with columns: Application Type, In, Out, Maximum Concurrent Sessions, and Maximum Sessions Per Endpoint. The table has three rows: Voice, Video, and IM. The 'Voice' row has checkboxes for 'In' and 'Out' both checked, and values of 1000 for both 'Maximum Concurrent Sessions' and 'Maximum Sessions Per Endpoint'. The 'Video' and 'IM' rows have checkboxes for 'In' and 'Out' both unchecked. Below the table is a 'Miscellaneous' section with two rows: 'CDR Support' with a value of 'None', and 'RTCP Keep-Alive' with a value of 'No'. There is an 'Edit' button at the bottom right of the configuration area.

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

Miscellaneous	
CDR Support	None
RTCP Keep-Alive	No

Figure 77 - Session Manager Application Rule

From the menu on the left-hand side, select **Domain Policies** → **Application Rules**.

- Select the **default** Rule
- Select **Clone** button
 - Name: **CenturyLink_AppR**
 - Click **Finish** (not shown).

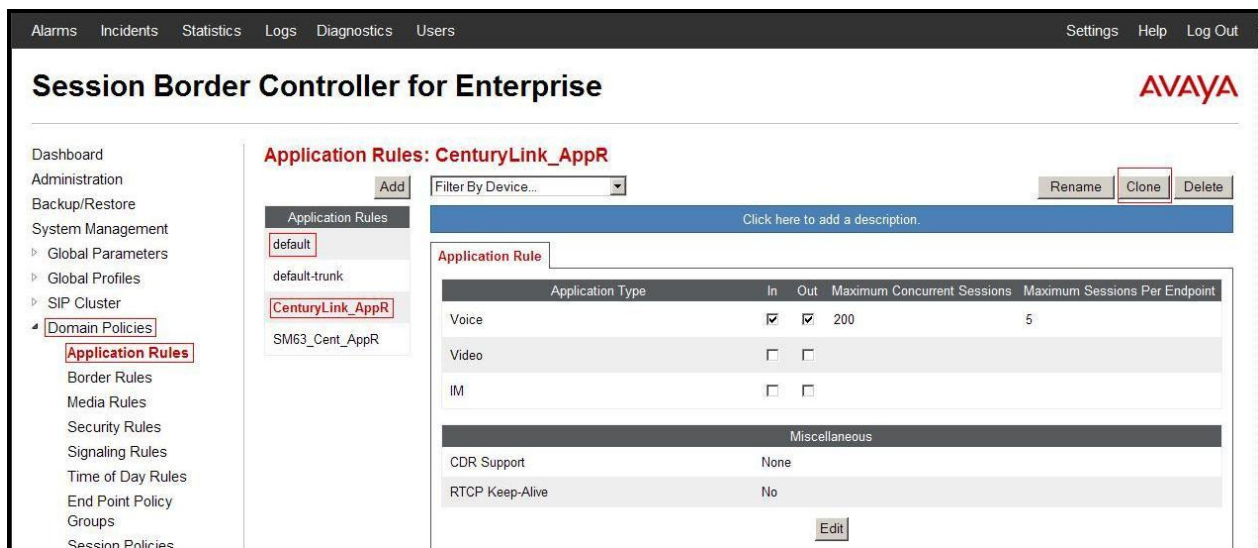


Figure 78 - CenturyLink Application Rule

7.3.2. Create Border Rules

Border Rules allow one to control NAT Traversal. The NAT Traversal feature allows one to determine whether or not call flow through the DMZ needs to traverse a firewall and the manner in which pinholes will be kept open in the firewall to accommodate traffic.

From the menu on the left-hand side, select **Domain Policies** → **Border Rules**.

- Select the **default** Rule
- Select **Clone** button
 - Enter Clone Name: **SM63_Cent_BorderR**
 - Click **Finish** (not shown).

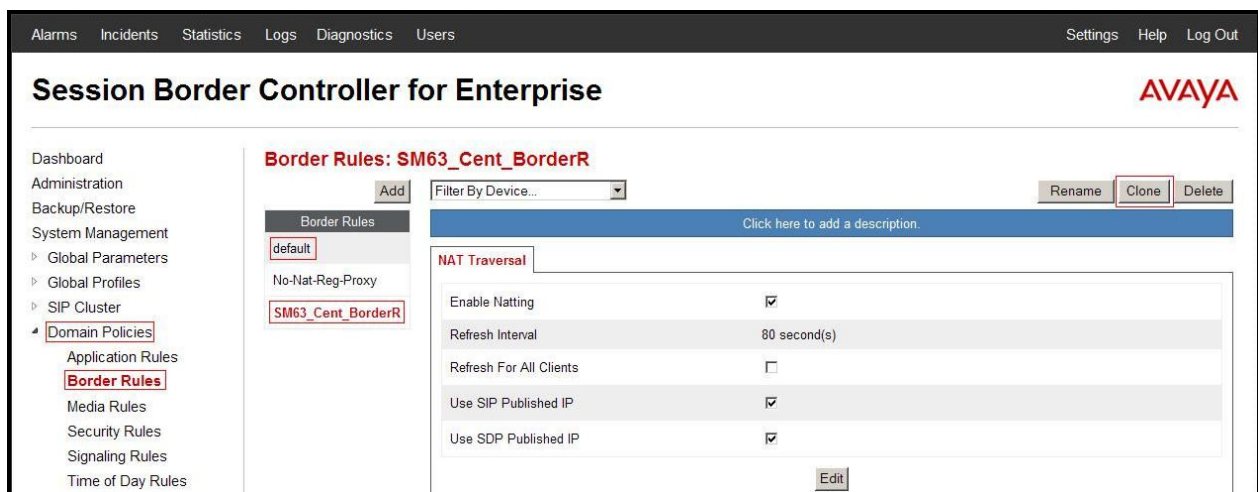


Figure 79 - Session Manager Border Rule

From the menu on the left-hand side, select **Domain Policies** → **Border Rules**.

- Select the **default** Rule
- Select **Clone** button
 - Enter Clone Name: **CenturyLink_BorderR**
 - Click **Finish** (not shown).

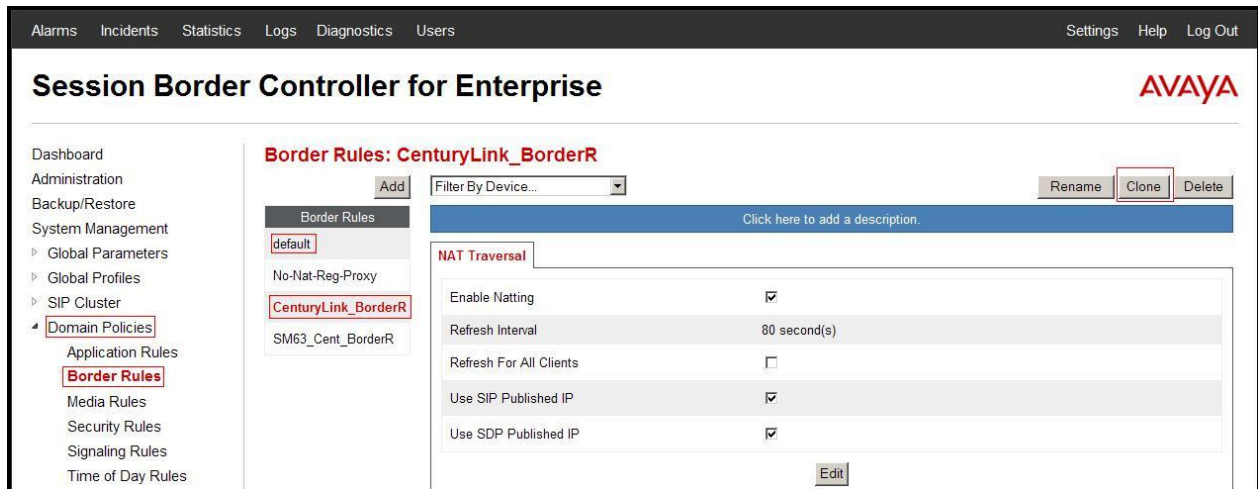


Figure 80 - CenturyLink Border Rule

7.3.3. Create Media Rules

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

From the menu on the left-hand side, select **Domain Policies** → **Media Rules**.

- Select the **default-low-med** Rule
- Select **Clone** button
 - Enter Clone Name: **SM63_Cent_MediaR**
 - Click **Finish** (not shown).



Figure 81 - Session Manager Media Rule

From the menu on the left-hand side, select **Domain Policies** → **Media Rules**.

- Select the **default-low-med** Rule
- Select **Clone** button
 - Enter Clone Name: **CenturyLink_MediaR**
 - Click **Finish** (not shown).

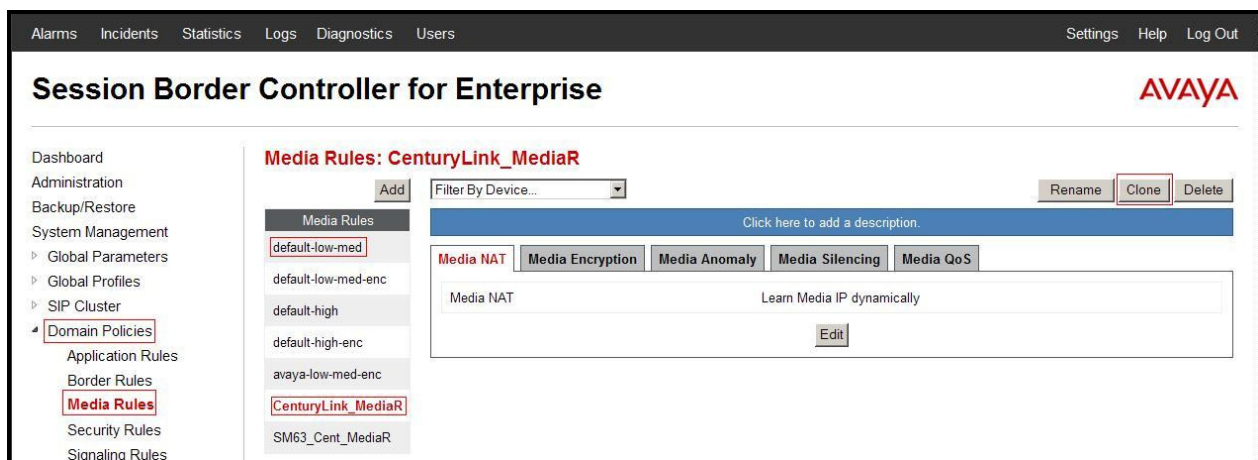


Figure 82 – CenturyLink Media Rule

7.3.4. Create Security Rules

Security Rules allow one to define which enterprise-wide VoIP and Instant Message (IM) security features will be applied to a particular call flow. Security Rules allows one to configure Authentication, Compliance, Fingerprinting, Scrubber, and Domain DoS. In addition to determining which combination of security features are applied, one can also define the security feature profile, so that the feature is applied in a specific manner to a specific situation.

From the menu on the left-hand side, select **Domain Policies** → **Security Rules**.

- Select the **default-med** Rule
- Select **Clone** button

- Enter Clone Name: **SM63_Cent_SecR**
- Click **Finish** (not shown).

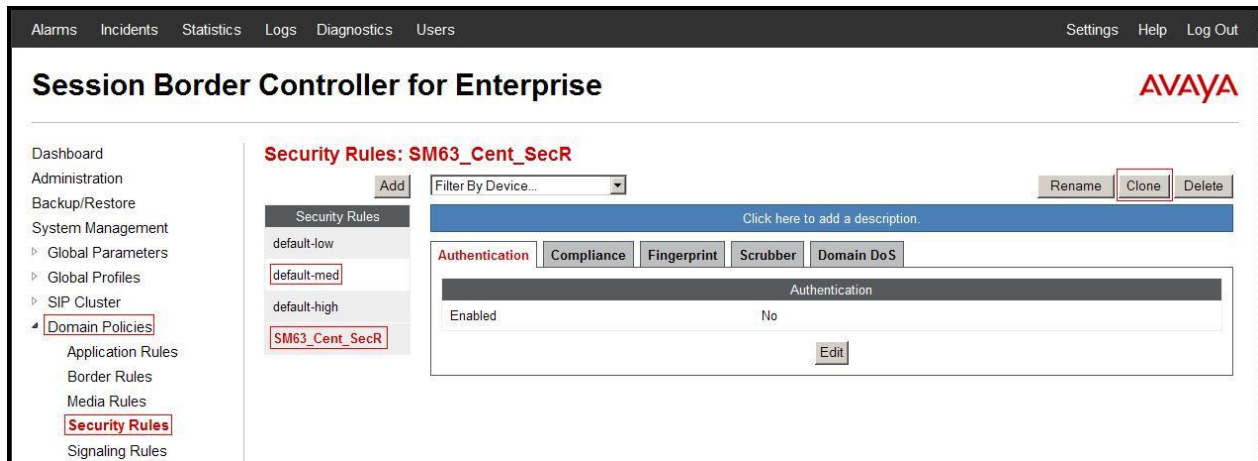


Figure 83 - Session Manager Security Rule

From the menu on the left-hand side, select **Domain Policies** → **Security Rules**.

- Select the **default-med** Rule
- Select **Clone** button
 - Enter Clone Name: **CenturyLink_SecR**
 - Click **Finish** (not shown).

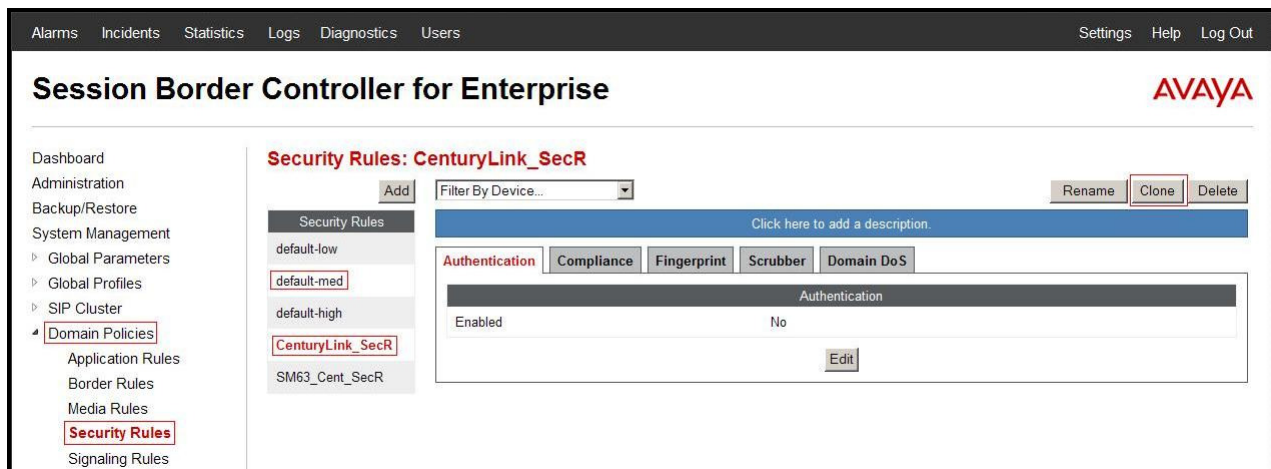


Figure 84 - CenturyLink Security Rule

7.3.5. Create Signaling Rules

Signaling Rules allow one to define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. When SIP signaling packets are received by the Avaya SBCE, they are parsed and “pattern matched” against the

particular signaling criteria defined by these rules. Packets matching the criteria defined by the Signaling Rules are tagged for further policy matching.

From the menu on the left-hand side, select **Domain Policies** → **Signaling Rules**.

- Select the **default** Rule
- Select **Clone** button
 - Enter Clone Name: **SM63_Cent_SigR**
 - Click **Finish** (not shown).

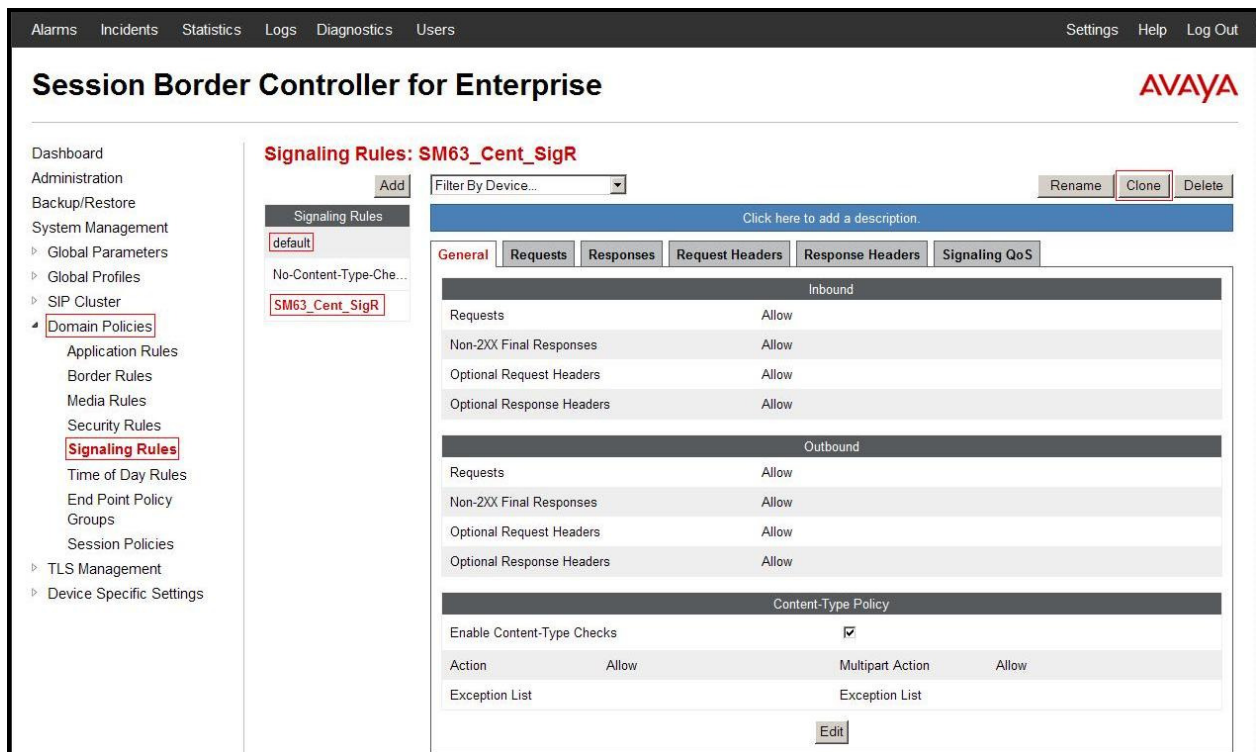


Figure 85 - Session Manager Signaling Rule

From the menu on the left-hand side, select **Domain Policies** → **Signaling Rules**.

- Select the **default** Rule
- Select **Clone** button
 - Enter Clone Name: **CenturyLink_SigR**
 - Click **Finish** (not shown).

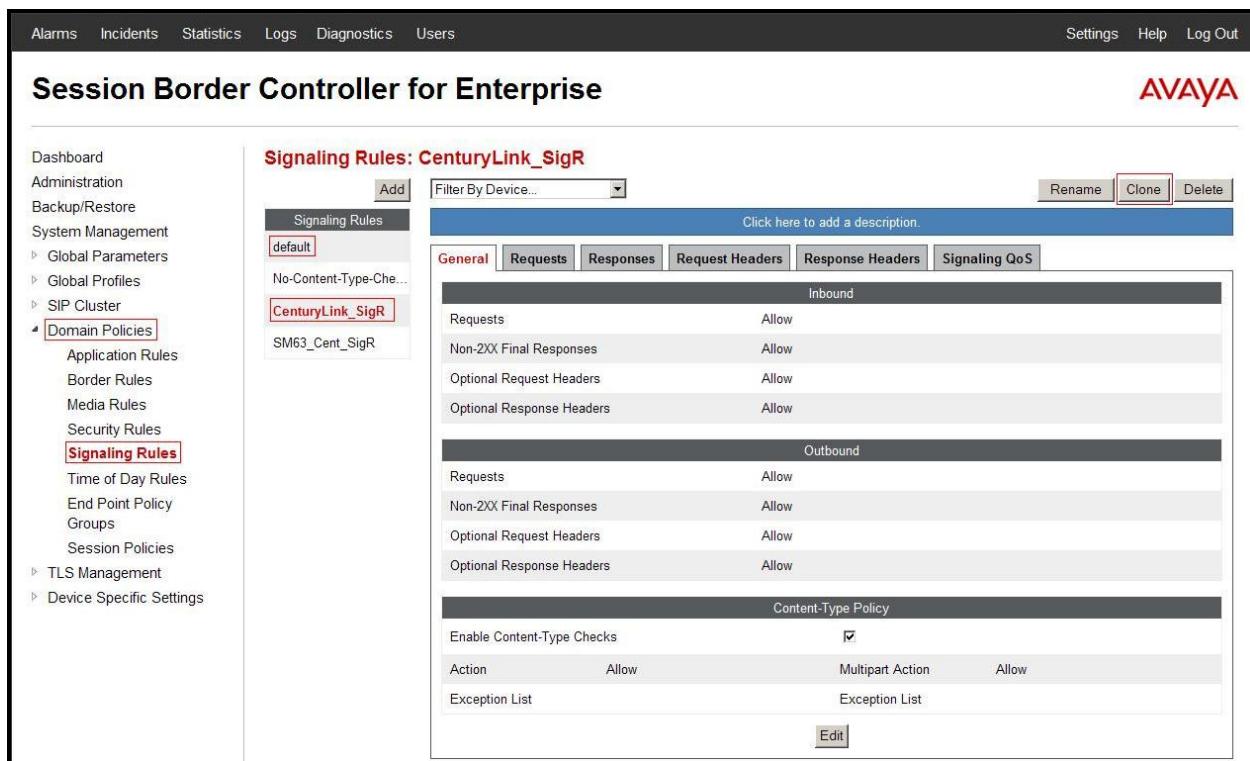


Figure 86 - CenturyLink Signaling Rule

7.3.6. Create Time of Day Rules

A Time-of-day (ToD) Rule allows one to determine when the domain policy which is assigned to will be in effect. ToD Rules provide complete flexibility to fully accommodate the enterprise by, not only determining when a particular domain policy will be in effect, but also to whom it will apply, and for how long it will remain in effect.

From the menu on the left-hand side, select **Domain Policies → Time of Day Rules**.

- Select the **default** Rule
- Select **Clone** button
 - Enter Clone Name: **SM63_Cent_ToDR**
 - Click **Finish** (not shown).

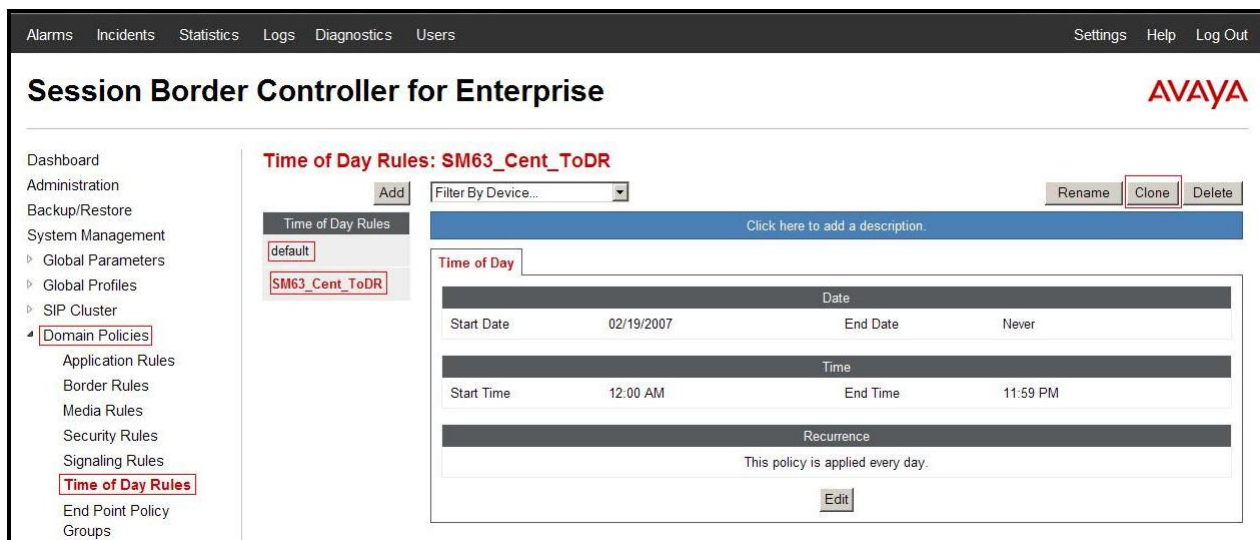


Figure 87 - Session Manager Time of Day Rule

From the menu on the left-hand side, select **Domain Policies** → **Time of Day Rules**.

- Select the **default** Rule
- Select **Clone** button
 - Enter Clone Name: **CenturyLink_ToDR**
 - Click **Finish** (not shown).

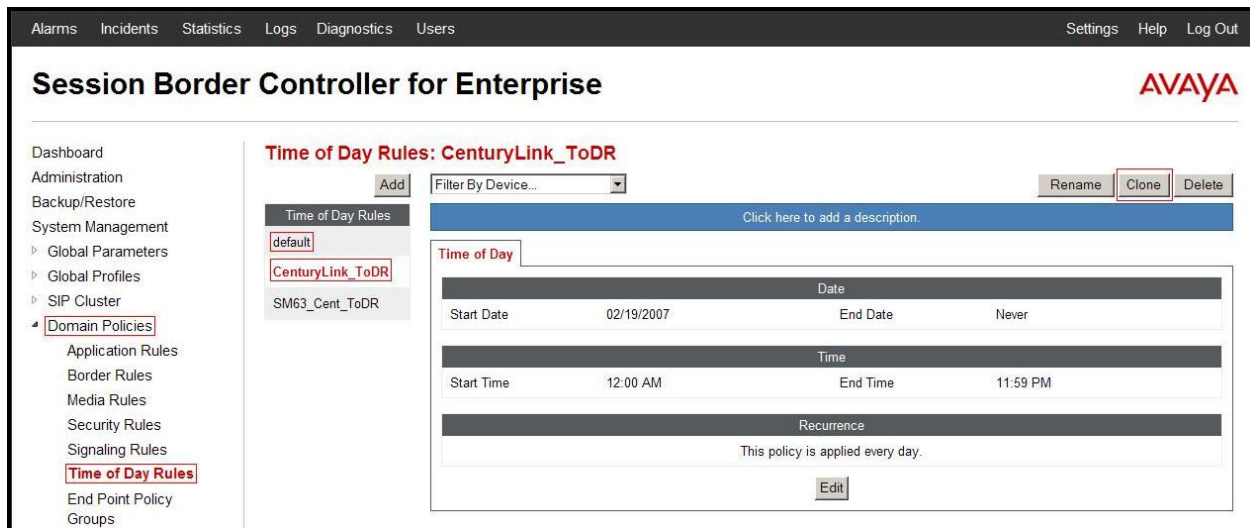


Figure 88 - CenturyLink Time of Day Rule

7.3.7. Create Endpoint 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 Avaya 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_Cent_PolicyG**
 - **Application Rule: SM63_Cent_AppR**
 - **Border Rule: SM63_Cent_BorderR**
 - **Media Rule: SM63_Cent_MediaR**
 - **Security Rule: SM63_Cent_SecR**
 - **Signaling Rule: SM63_Cent_SigR**
 - **Time of Day: SM63_Cent_ToDR**
- Select **Finish** (not shown).

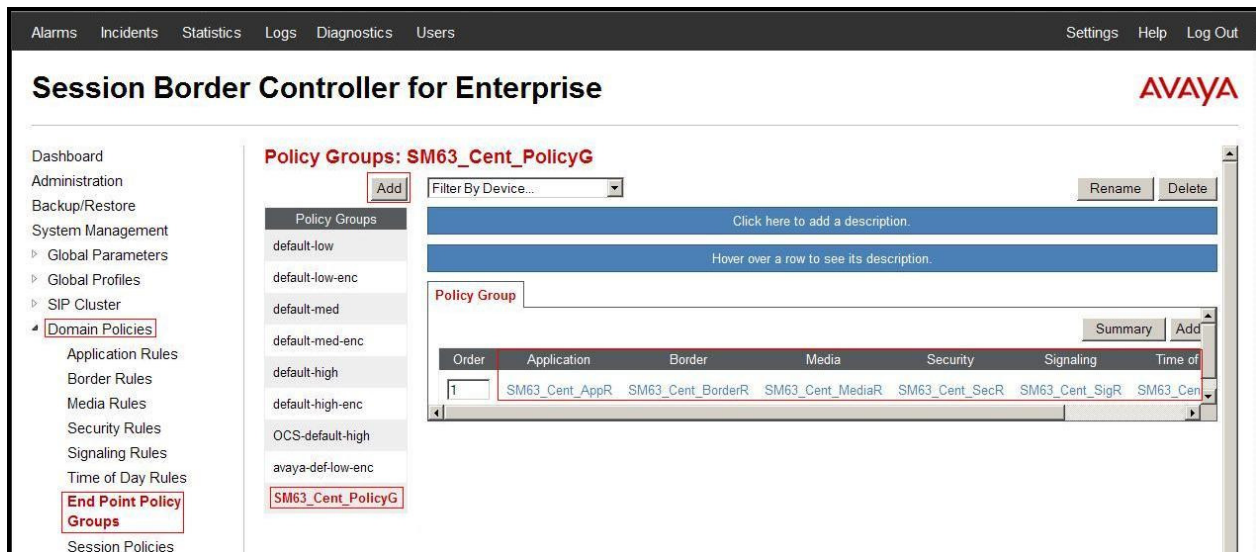


Figure 89 - Session Manager End Point Policy Group

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

- Select **Add**
- Enter **Group Name: CenturyLink_PolicyG**
 - **Application Rule: CenturyLink_AppR**
 - **Border Rule: CenturyLink_BorderR**
 - **Media Rule: CenturyLink_MediaR**

- **Security Rule: CenturyLink_SecR**
- **Signaling Rule: CenturyLink_SigR**
- **Time of Day: CenturyLink_ToDR**
- Select **Finish** (not shown).

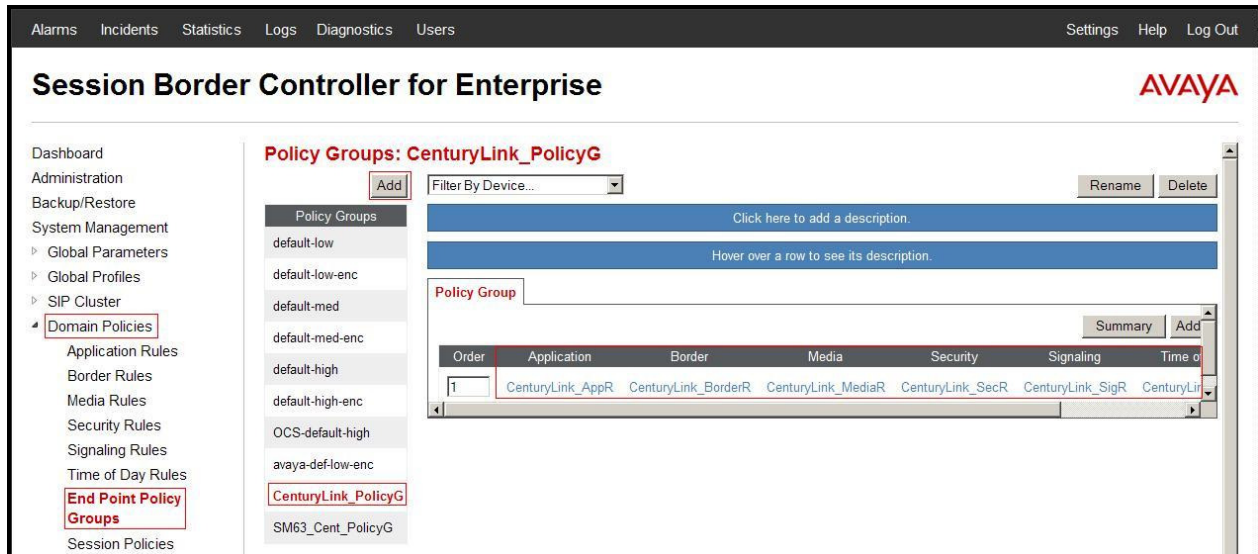


Figure 90 - CenturyLink End Point Policy Group

7.3.8. Create Session Policy

Session Policies allow users to define RTP media packet parameters such as codec types (both audio and video) and codec matching priority. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criterion will be handled by the Avaya SBCE security product.

- From the menu on the left-hand side, select **Domain Policies → Session Policies**.
- Select the **default** policy
- Select **Clone** button
 - Enter Clone Name: **CenturyLink**
 - Click **Finish** (not shown).
- Click **Edit** button on **Codec Prioritization** tab
 - Check **Codec Prioritization**
 - Set **Preferred Codec #1: PCMU (0)**
 - Set **Preferred Codec #2: PCMA (8)**
 - Set **Preferred Codec #3: G729 (18)**
 - Select **Finish** (not shown)

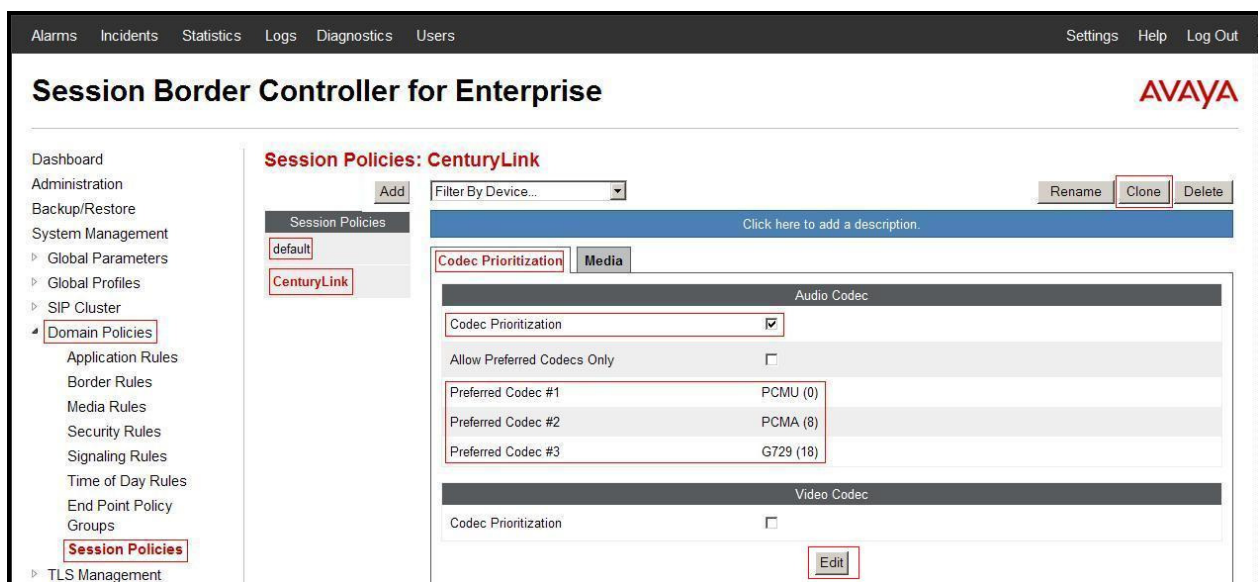


Figure 91 - CenturyLink Session Policy

- Click **Edit** button on **Media** tab
 - Check **Media Anchoring**
 - Select **Finish** (not shown)

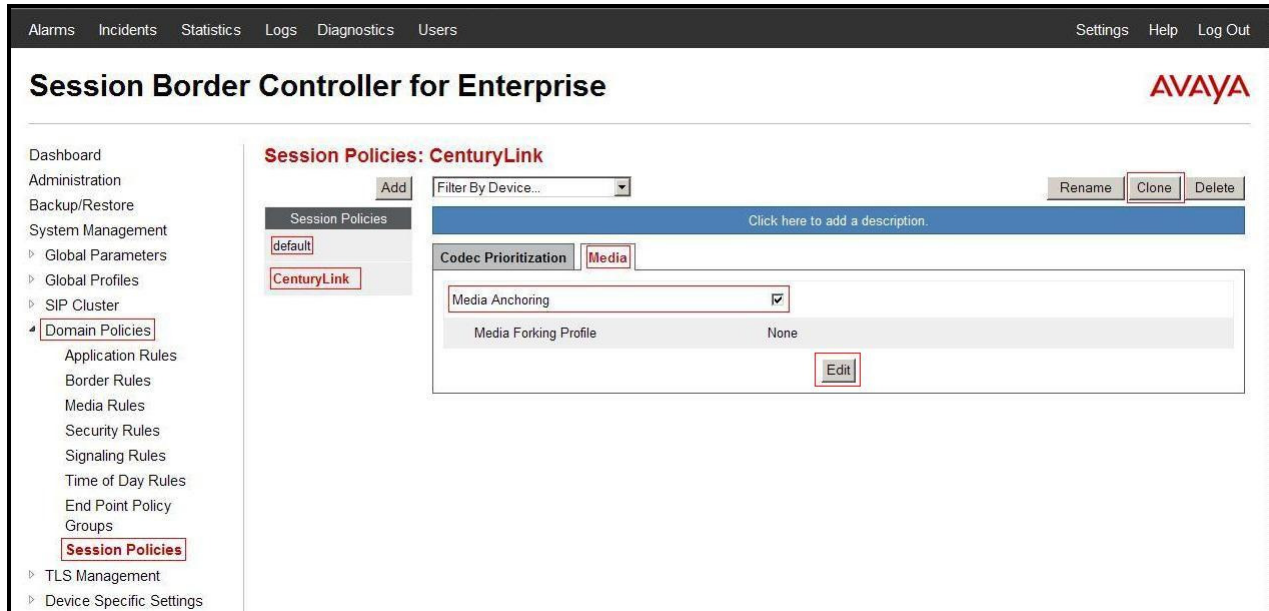


Figure 92 - CenturyLink Session Policy – Anchoring Media

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**.

- Enter the **IP Address** and **Gateway Address** for both the Inside and the Outside interfaces:
 - **IP Address** for Inside interface: **10.10.98.13**; **Gateway: 10.10.98.1**
 - **IP Address** for Outside interface: **10.10.98.111**; **Gateway: 10.10.98.97**
- Select the physical interface used in the Interface column:
 - **Inside Interface: A1**
 - **Outside Interface: B1.**

IP Address	Public IP	Gateway	Interface	
10.10.98.13		10.10.98.1	A1	Delete
10.10.98.111		10.10.98.97	B1	Delete

Figure 93 - Network Management

- Select the **Interface Configuration** Tab.
- Toggle the State of the physical interfaces being used to **Enabled**.

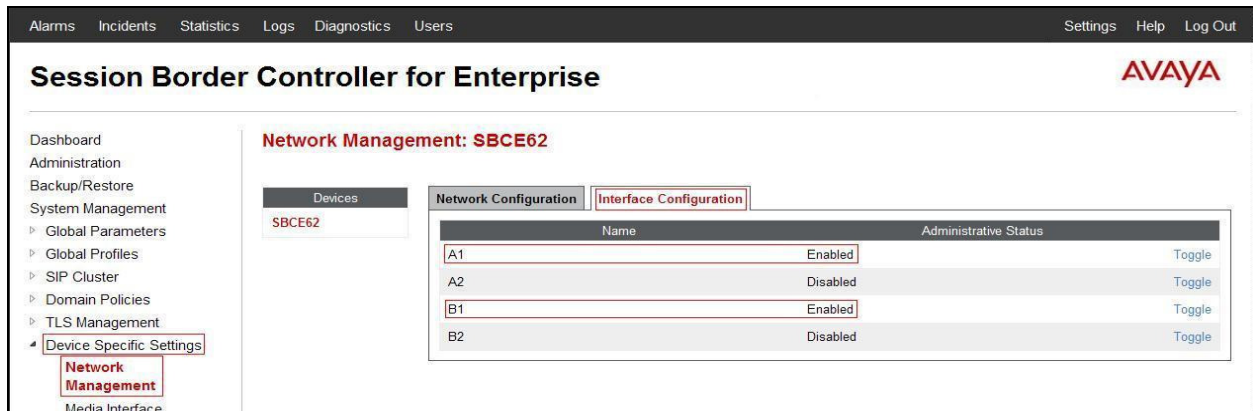


Figure 94 - Network Interface Status

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, **Device Specific Settings** → **Media Interface**.

- Select **Add**
 - **Name: InsideMedia**
 - **Media IP: 10.10.98.13** (Internal IP Address toward Session Manager)
 - **Port Range: 35000 - 40000**
 - Click **Finish** (not shown)
- Select **Add**
 - **Name: OutsideMedia**
 - **Media IP: 10.10.98.111** (External IP Address toward CenturyLink trunk)
 - **Port Range: 35000 - 40000**
 - Click **Finish** (not shown).



Figure 95 - 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: InsideUDP**
 - **Media IP: 10.10.98.13** (Internal IP Address toward Session Manager)
 - **UDP Port: 5060**
 - Click **Finish** (not shown).

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

- Select **Add**
 - **Name: OutsideUDP**
 - **Media IP: 10.10.98.111** (External IP Address toward CenturyLink trunk)
 - **UDP Port: 5060**
 - Click **Finish** (not shown).

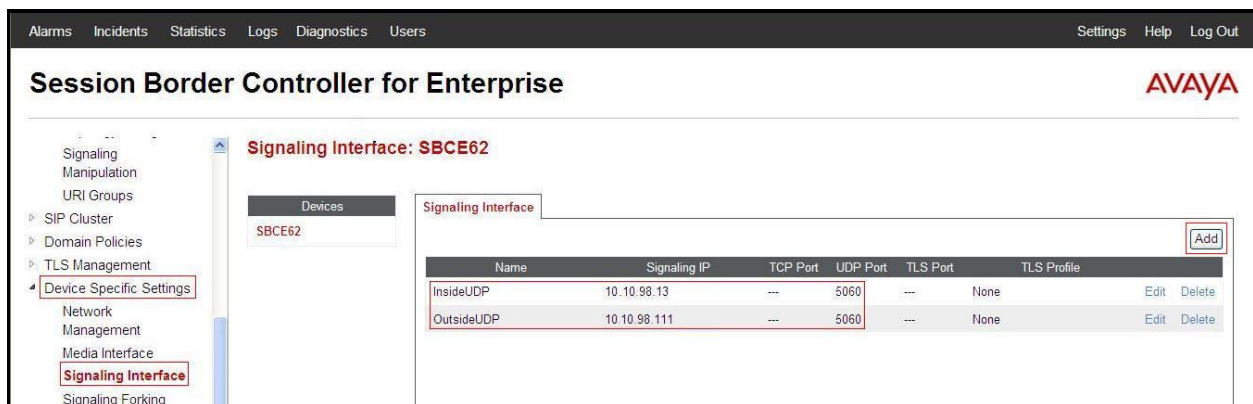


Figure 96 - Signaling Interface

7.4.4. Configuration Server Flows

Server Flows allow to categorize trunk-side signaling and apply a policy.

7.4.4.1 Create End Point Flows – From CenturyLink

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: From CenturyLink**
 - **Server Configuration: CenturyLink**
 - **URI Group: CenturyLink**
 - **Transport: ***
 - **Remote Subnet: ***
 - **Received Interface: InsideUDP**
 - **Signaling Interface: OutsideUDP**
 - **Media Interface: OutsideMedia**

- **End Point Policy Group: CenturyLink_PolicyG**
- **Routing Profile: CenturyLink_To_SM63**
- **Topology Hiding Profile: SM63_To_CenturyLink**
- Click **Finish** (not shown).

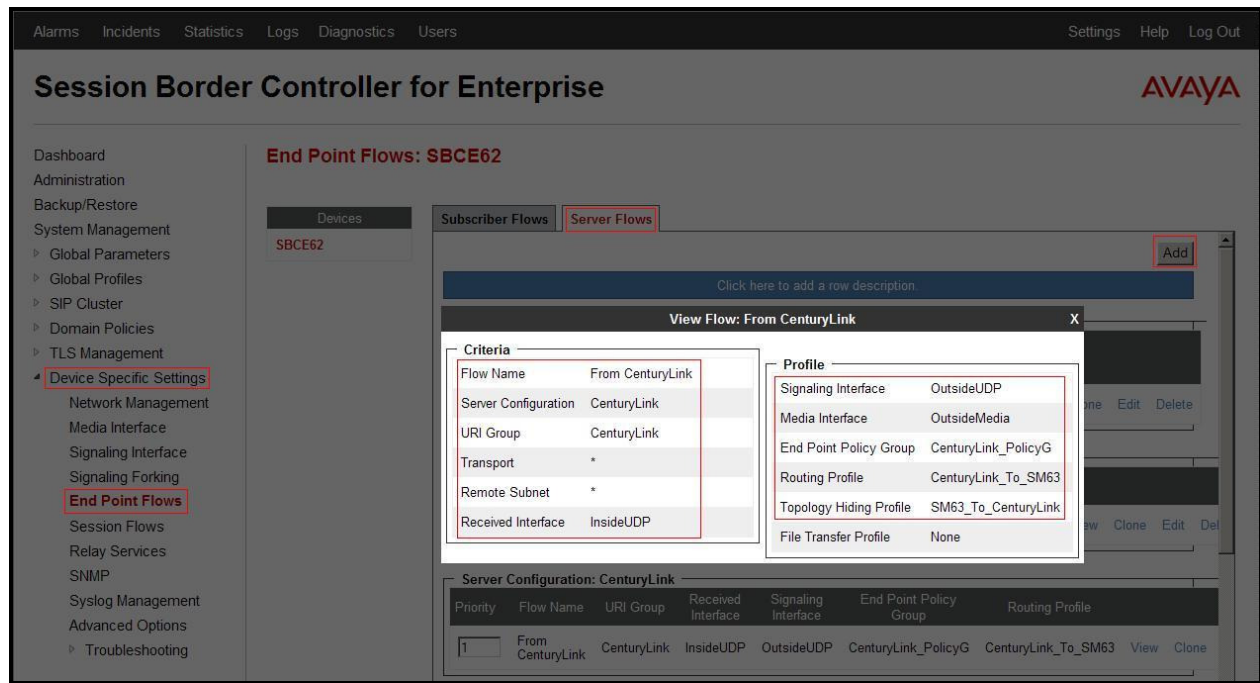


Figure 97 - End Point Flows 1

7.4.4.2 Create End Point Flows – To CenturyLink

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: To CenturyLink**
 - **Server Configuration: SM63**
 - **URI Group: CenturyLink**
 - **Transport: ***
 - **Remote Subnet: ***
 - **Received Interface: OutsideUDP**
 - **Signaling Interface: InsideUDP**
 - **Media Interface: InsideMedia**
 - **End Point Policy Group: SM63_Cent_PolicyG**
 - **Routing Profile: SM63_To_CenturyLink**
 - **Topology Hiding Profile: CenturyLink_To_SM63**
 - Click **Finish** (not shown).

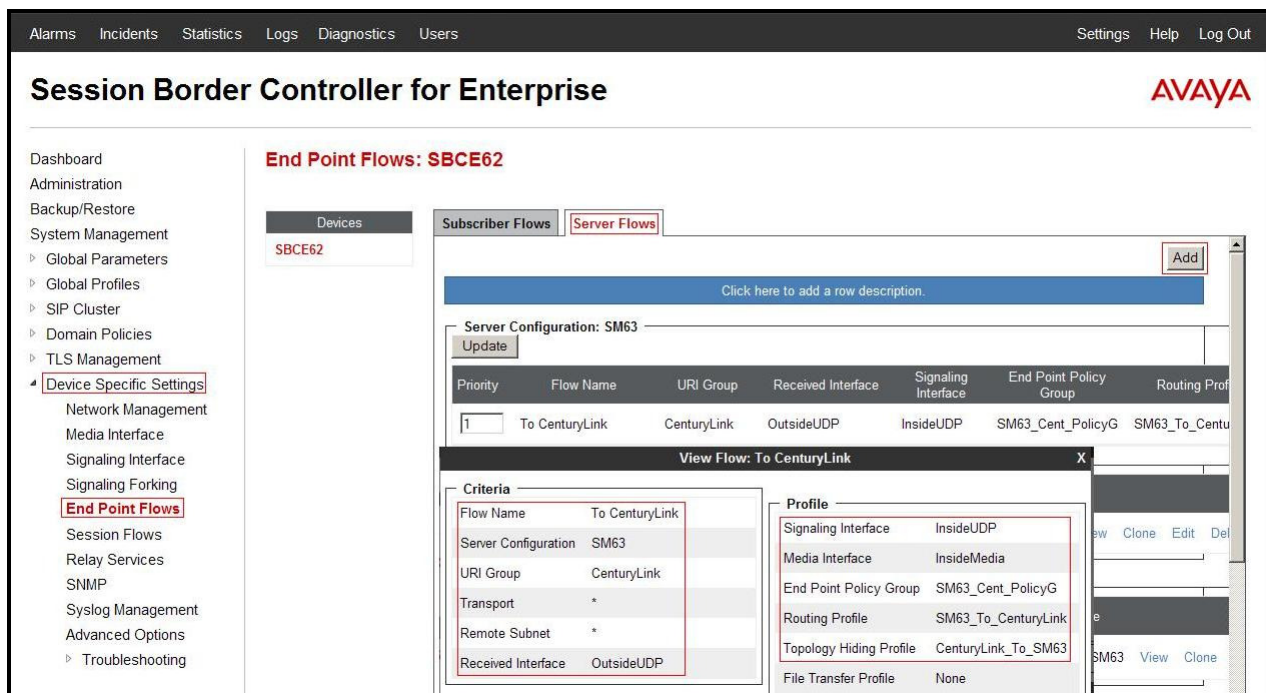


Figure 98 - End Point Flows 2

7.4.5. Create Session Flows

Session Flow determines the media (audio/video) sessions in order to apply the appropriate session policy.

- Select **Device Specific Settings** from the menu on the left-hand side
- Select the **Session Flows**
- Select **Add**
- Enter **Flow Name: CenturyLink**
 - **URI Group#1: CenturyLink**
 - **URI Group#2: CenturyLink**
 - **Session Policy: CenturyLink**
- Select **Finish** (not shown)

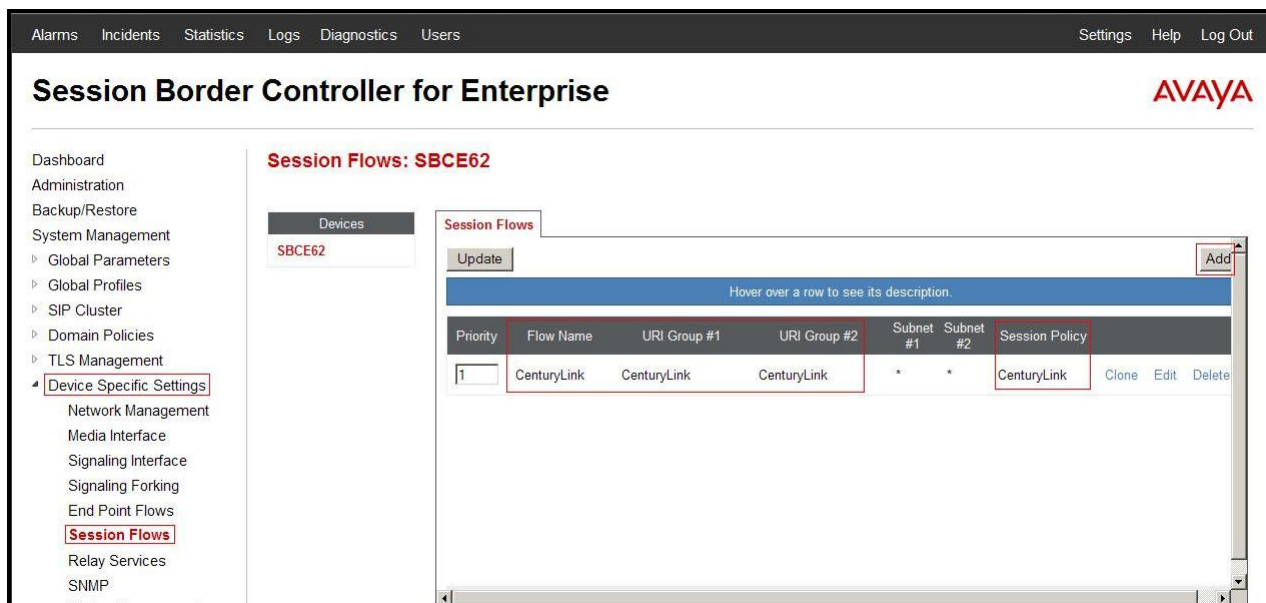


Figure 99 – Session Flows

8. CenturyLink SIP Trunking service Configuration

CenturyLink is responsible for the network configuration of the CenturyLink SIP Trunking service. CenturyLink will require that the customer provide the public IP address used to reach the Avaya SBCE public interface at the edge of the enterprise. CenturyLink will provide the IP address of CenturyLink's SIP proxy/SBC, IP addresses of media sources and Direct Inward Dialed (DID) numbers assigned to the enterprise. This information is used to complete configurations for Communication Server 1000, Session Manager, and the Avaya SBCE discussed in the previous sections.

The configuration between CenturyLink and the enterprise is a static configuration. There is no registration of the SIP trunk or enterprise users to the CenturyLink'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 Communication Server 1000 to trace the DN for which the call is in progress or idle (7104). The call scenario involved PSTN phone number 6139675206 calling 3036157104 (which is translated to phone 7104).

- Login into Communication Server 1000 Signaling Server 10.10.97.177 with admin account and password.
- Issue a command “cslogin” to login on to the Communication Server 1000 Call Server.
- Log in to the Overlay command prompt, issue the command **LD 80** and then **trace 0 7104**.
- After the call is released, issue command **trac 0 7104** again to see if the DN is released back to idle state.

Below is the actual output of the Communication Server 1000 Call Server Command Line mode when the 7104 is in call state:

```
>ld 80
TRA000
.trac 0 7104

ACTIVE VTN 096 0 00 02

ORIG VTN 100 0 00 00 VTRK IPTI RMBR 100 1 INCOMING VOIP GW CALL
FAR-END SIP SIGNALLING IP: 10.10.98.13
FAR-END MEDIA ENDPOINT IP: 10.10.98.13 PORT: 37996
FAR-END VendorID: AVAYA-SM-6.3.2.0.632023
TERM VTN 096 0 00 02 KEY 0 SCR MARP CUST 0 DN 7104 TYPE 2002P2
SIGNALLING ENCRYPTION: INSEC
MEDIA ENDPOINT IP: 10.33.5.16 PORT: 5200
MEDIA PROFILE: CODEC G.711 MU-LAW PAYLOAD 20 ms VAD OFF
RFC2833: RXPT 101 TXPT N/A DIAL DN 7104
MAIN_PM ESTD
TALKSLOT ORIG 12 TERM 17
EES_DATA:
NONE
QUEUE NONE
CALL ID 501 29

---- ISDN ISL CALL (ORIG) ----
CALL REF # = 484
BEARER CAP = VOICE
HLC =
CALL STATE = 10 ACTIVE
CALLING NO = 6139675206 NUM_PLAN:UNKNOWN TON:UNKNOWN ESN:UNKNOWN
CALLED NO = 3036157104 NUM_PLAN:UNKNOWN TON:UNKNOWN ESN:UNKNOWN
```

And this is the example after the call to 7104 is finished.

```
>ld 80
TRA000
.trac 0 7104
IDLE VTN 96 0 00 02 MARP
```

SIP Trunk monitoring (LD 32)

Place a call inbound from PSTN (6139675206) to an internal device (3036157104). Then check the SIP trunk status by using LD 32, one trunk is BUSY.

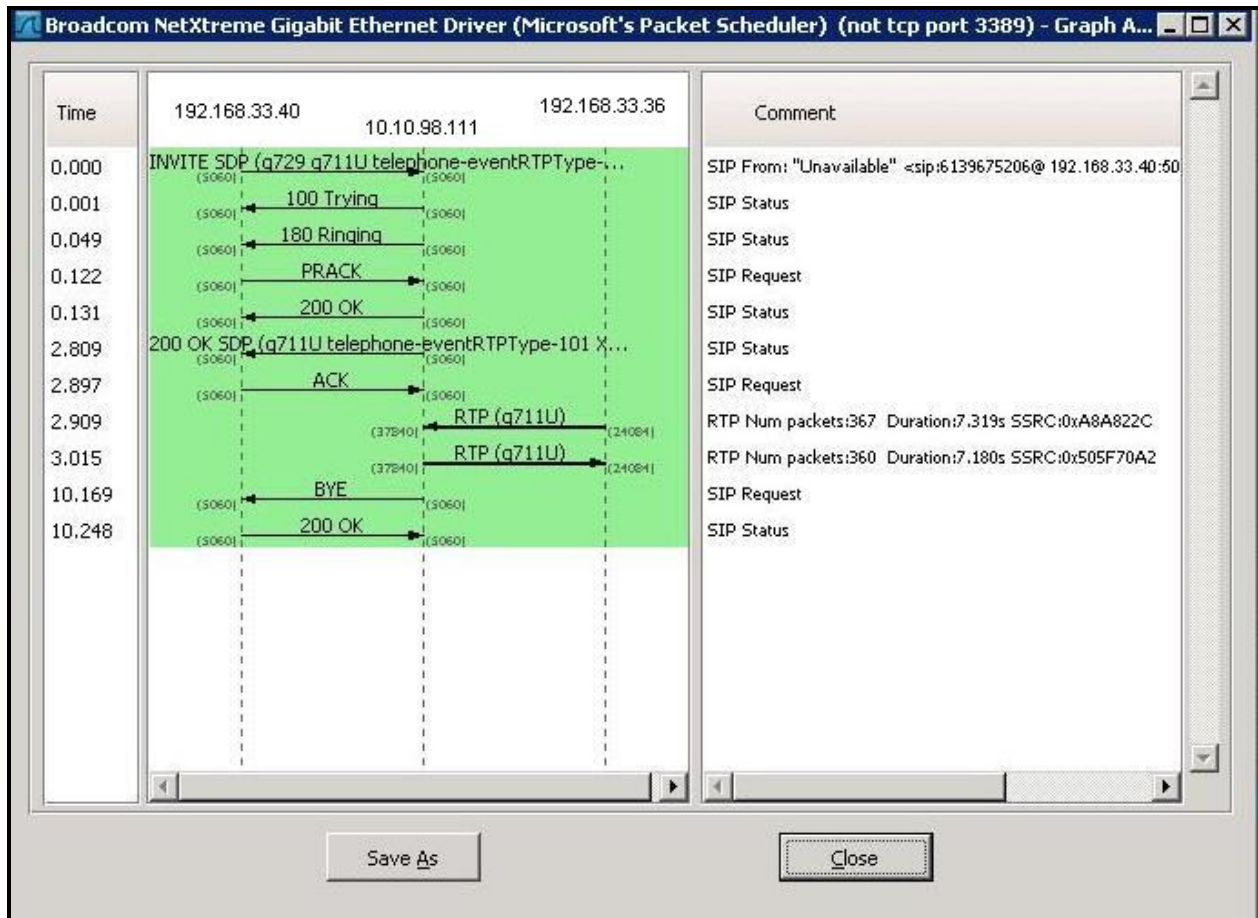
```
>ld 32
NPR000
.stat 100 0
091 UNIT(S) IDLE
001 UNIT(S) BUSY
000 UNIT(S) DSBL
000 UNIT(S) MBSY
```

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.



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 CenturyLink SIP Trunk service is considered **compliant** with Avaya Communication Server 1000 Release 7.6, Avaya Aura® Session Manager Release 6.3 FP2 and Avaya Session Border Controller for Enterprise Release 6.2.0 Q36

11. References

This section references the documentation relevant to these Application Notes.

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

[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.

[7] Avaya Aura® System Manager Overview and Specification, Release 6.3, Issue 2, May 2013.

[8] Administering Avaya Aura® Session Manager, Release 6.3, Issue 2, June 2013.

[9] Maintaining and Troubleshooting Avaya Aura® Session Manager, Release 6.3, Issue 2, May 2013.

[10] Administering Avaya Session Border Controller for Enterprise, Release 6.2, Issue 2, May 2013.

[11] Installing Avaya Session Border Controller for Enterprise, Release 6.2, Issue 3, June 2013.

[12] Upgrading Avaya Session Border Controller for Enterprise, Release 6.2, Issue 3, July 2013.

Other resources:

[13] RFC 3261 SIP: Session Initiation Protocol, <http://www.ietf.org/>

[14] RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals,
<http://www.ietf.org/>

Appendix A: SigMa Script

The following is the Signaling Manipulation script used in the configuration of the Avaya SBCE, **Section 7.2.6:**

```
within session "All"
{
    act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
    {
        %HEADERS["Content-Type"][1].regex_replace("multipart/mixed;boundary=unique-boundary-1", "application/sdp");

        remove(%BODY[1]);
        remove(%BODY[1]);

        // Remove unwanted Headers
        remove(%HEADERS["History-Info"][3]);
        remove(%HEADERS["History-Info"][2]);
        remove(%HEADERS["History-Info"][1]);
        remove(%HEADERS["Alert-Info"][1]);
        remove(%HEADERS["x-nt-e164-clid"][1]);
        remove(%HEADERS["P-AV-Message-Id"][1]);
        remove(%HEADERS["P-Charging-Vector"][1]);
        remove(%HEADERS["Av-Global-Session-ID"][1]);
        remove(%HEADERS["P-Location"][1]);
        remove(%HEADERS["Remote-Party-ID"][1]);
    }
}
```

©2013 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.