



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Level 3 SIP Trunking Service with Avaya Communication Server 1000 Release 7.5, Avaya Aura® Session Manager Release 6.1 and Acme Packet Session Border Controller Release 6.2 – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Level 3 SIP Trunking Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of an Avaya Communication Server 1000 7.5, Avaya Aura® Session Manager 6.1, Acme Packet Session Border Controller 6.2 and various Avaya endpoints. This documented solution does not extend to configurations without Avaya Aura® Session Manager and Acme Packet Session Border Controller.

Level 3 is a member of the Avaya DevConnect Service Provider program. Information in these Application Notes has been obtained through DevConnect compliance testing and additional technical discussions. Testing is conducted via the DevConnect Program at the Avaya Solution and Interoperability Test Lab.

Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing	4
2.2.	Test Results	5
2.3.	Support.....	6
3.	Reference Configuration	7
4.	Equipment and Software Validated	8
5.	Avaya Communication Server 1000 Configuration	8
5.1.	Login to CS1000.....	9
5.1.1.	Login Unified Communications Management (UCM) and Element Manager (EM).....	9
5.1.2.	Login to Call Server Command Line Interface (CLI)	10
5.2.	Administer a Node IP Telephony	11
5.2.1.	Obtain Node IP address	11
5.2.2.	Administer Quality of Service (QoS)	12
5.2.3.	Synchronize the new configuration	12
5.3.	Administer Voice Codec.....	12
5.3.1.	Enable Voice Codec, Node IP Telephony	12
5.3.2.	Administer Voice Codec on Media Gateways.....	14
5.4.	Administer Zones and Bandwidth	15
5.4.1.	Create a zone for IP phones	15
5.4.2.	Create a zone for virtual SIP trunk	16
5.5.	Administer SIP Trunk Gateway.....	17
5.5.1.	Integrated Services Digital Network (ISDN).....	17
5.5.2.	Administer SIP Trunk Gateway to Session Manager	17
5.5.3.	Administer Virtual D-Channel.....	20
5.5.4.	Administer Virtual Super-Loop	22
5.5.5.	Enable Music for Customer Data Block	23
5.5.6.	Administer Virtual SIP Routes	24
5.5.7.	Administer Virtual Trunks.....	28
5.5.8.	Administer Calling Line Identification Entries.....	30
5.5.9.	Enable External Trunk to Trunk Transferring	31
5.5.10.	Enable plug-in 501	32
5.6.	Administer Dialing Plans.....	32
5.6.1.	Define ESN Access Codes and Parameters (ESN).....	32
5.6.2.	Associate NPA and SPN call to ESN Access Code 1.....	34
5.6.3.	Digit Manipulation Block (DMI).....	35
5.6.4.	Route List Block (RLB).....	35
5.6.5.	Incoming Digit Translation (IDC)	36
5.6.6.	Outbound Call - Special Number Configuration	37
5.6.7.	Outbound Call - Numbering Plan Area (NPA).....	38
6.	Configure Avaya Aura® Session Manager	38
6.1.	System Manager Login and Navigation	39
6.2.	Specify SIP Domain.....	40
6.3.	Add Location	40

6.4.	Add SIP Entities.....	41
6.5.	Add Entity Links.....	44
6.6.	Add Routing Policies	45
6.7.	Add Dial Patterns.....	46
6.8.	Add/View Session Manager	48
7.	Configure Acme Packet Net-Net 3800 Session Border Controller	49
7.1.	Acme Packet Command Line Interface	50
7.2.	Physical and Network Interfaces	51
7.3.	Realm	52
7.4.	Session Agent.....	53
7.5.	SIP Configuration	54
7.6.	SIP Interface.....	54
7.7.	SIP Manipulation	55
7.8.	Steering Pools	63
7.9.	Local Policy	64
8.	Level 3 SIP Trunking Service Configuration	65
9.	Verification and Troubleshooting.....	66
9.1.	Verification Steps.....	66
9.2.	Protocol Traces:	66
9.3.	Troubleshooting:	67
10.	Conclusion	72
11.	References	73

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Level 3 SIP Trunking Service (Level 3) and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of an Avaya Communication Server 1000 (CS1000) 7.5, Avaya Aura® Session Manager 6.1, Acme Packet Session Border Controller (Acme SBC) 6.2 and various Avaya endpoints.

Customers using this Avaya SIP-enabled enterprise solution with Level 3 are able to place and receive PSTN calls via a broadband connection. This converged network solution is an alternative to traditional PSTN trunking such as analog and/or ISDN-PRI.

2. General Test Approach and Test Results

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

Level 3 is a member of the Avaya DevConnect Service Provider program. The general test approach is to connect a simulated enterprise to Level 3 via the public internet and exercise the features and functionality listed in **Section 2.1**.

2.1. Interoperability Compliance Testing

To verify Level 3 SIP Trunking Service interoperability, the following features and functionalities are covered during the compliance test:

- Incoming PSTN call to various phone types including SIP, UNISTim, PC2050 softphone, digital and analog telephone at the enterprise. All inbound calls from PSTN are routed to the enterprise across the SIP trunk from the service provider.
- Outgoing PSTN call from various phone types including SIP, UNISTim, PC2050 softphone, digital and analog telephone at the enterprise. All outbound calls to PSTN are routed from the enterprise across the SIP trunk to the service provider.
- Dialing plans including local, long distance, international, outbound toll-free, operator assisted calls, local directory assistance (411)... etc.
- Proper Codec Negotiation with G.729 and G.711MU codecs.
- Proper Early Media transmission with G.729 and G.711MU codecs.
- Incoming and outgoing fax over IP with T.38 codec.
- DTMF tone transmissions as out-of-band RTP event as per RFC2833.
- Caller ID presentation and Caller ID restriction.
- Response to incomplete call attempts and trunk errors.
- Voicemail navigation for inbound and outbound calls.
- User features such as hold and resume, transfer and conference.

- Off-net call transfer with SIP re-INVITE method.
- Off-net call forward with SIP Diversion method.
- SIP Digest Authentication.

Items are not supported or not tested including the following:

- Inbound toll-free and outbound emergency calls (911) are supported but are not tested as part of the compliance test because Level 3 does not provide the necessary configuration.
- Session Timer refresh is not supported.
- Reliable of Provisional Responses (RFC3262) is not supported.
- Off-net call forwarding using History-Info method is not supported.

2.2. Test Results

Interoperability testing of Level 3 SIP Trunking Service with the Avaya SIP-enabled enterprise solution is completed with successful results for all test cases with the exception of the observations/limitations described below.

1. **Fax over IP using G.711 codec is not recommended.** Transmitting fax over IP using a G.711 codec appears to work for regular fax machines. However, when using an integrated fax modem on a PC, the fax call fails as Level 3 unexpectedly attempts to switch the codec from G.711MU to T.38. This is a known issue on Level 3 SIP Trunking Service but there is no resolution available at this time.
2. **In blind transfer off-net scenario, the calling PSTN does not hear ringback tone when the called PSTN is ringing.** This limitation is encountered when performing a work around to support a blind transfer call without an UPDATE/SDP method. Before completing the transferred call, the CS1000 uses an UPDATE/SDP method to anchor ring back tone on the 2nd leg to the 1st leg. However, Level 3 does not appear to support this method, it rejects the UPDATE/SDP with a “500 Internal Server Error” response. A workaround has been made to eliminate the UPDATE method on inbound signaling, that makes the CS1000 automatically disable UPDATE from being sent to Level 3. This approach is achieved by additional configuration made to the Acme SBC and the CS1000 as described below:
 - On the Acme SBC, create a Header Manipulation Rule (HMR) to delete UPDATE in the Allow header on inbound signaling. For a detailed configuration, please refer to **Section 7.7**, sip-manipulation rule **Level3_To_CS1K**, header-rule **manipAllow**.
 - On the CS1000, enable plug-in 501 in pdt mode. The CS1000 deactivates the blind transfer feature when the far end does not support UPDATE. To reactivate blind transfer functionality, the plug-in 501 has to be enabled. For a detailed configuration, please refer to **Section 5.5.10**.

Note: The CS1000 requires support of UPDATE, but Level3 does not support this method. Not supporting UPDATE may result in significant service degradation and feature breakage.
3. **Off-net call transfer, the calling party name and number is not updated to calling PSTN party** When the CS1000 transfers an incoming call off-net to the PSTN, it sends a 200OK with the true connected calling party name and number in Remote-Party-ID

header to the calling PSTN. However, the calling party name and number are not updated; the calling PSTN party still displays the calling party number of the CS1000. This is a known issue on Level 3 SIP Trunking Service. It is recommended that Level 3 should support the calling party information update. The feature also needs to be supported by the service provider hosting the calling PSTN party. This issue has low user impact, it is listed here simply as an observation.

4. **CS1000 SIP phone transfer off-net to the PSTN is not successful with Music On Hold enabled.** In an inbound or outbound call between a CS1000 SIP phone and PSTN_1, the CS1000 SIP phone performs an off-net transfer back to PSTN_2. The transfer fails. PSTN_1 continues to hear ringing after the call has been answered by PSTN_2. This call scenario is successful with other endpoints .e.g. UNISim or digital phones. The issue does not happen when Music On Hold is disabled. An internal tracking number wi01017194 has been created. This issue is simply listed here as a limitation.
5. **CS1000 phone holds and retrieves an outbound call causing the calling party number to be changed.** After retrieving a call, the calling party number previously displayed on CS1000 phone will be replaced by Route ACOD – Trunk Channel ID. This is a known issue on the CS1000 but there is no resolution available at this time. This issue has low user impact, it is listed here simply as an observation.
6. **CS1000 SIP phone calls a local UNISim phone then blind transfers to PSTN causing the calling party number to be changed.** The call is successfully transferred. However, the UNISim phone displays Route ACOD – Trunk Channel ID instead of displaying the PSTN calling party name and number. This is a known issue on the CS1000 but there is no resolution available at this time. This issue has low user impact, it is listed here simply as an observation.
7. **Digest Authentication on inbound call is corrected and works properly.** When the CS1000 holds an inbound call, the re-INVITE from the CS1000 is challenged by a 401 from Level 3 to do Digest Authentication. However, the CS1000 does not resend another re-INVITE with Authorization header as expected. The issue has been corrected by applying patch cs1000-vtrk-7.50.17.16-30.i386.000 to the CS1000 SIP Trunk Gateway.

2.3. Support

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

For technical support on Level 3 SIP Trunking Service, please contact Level 3 technical support at:

- Phone: 1-877-453-8353)
- Website: <http://www.level3.com/en/contact-us/>

3. Reference Configuration

Figure 1 illustrates the sample Avaya SIP-enabled enterprise solution connected to the Level 3 SIP Trunking Service (Vendor Validation circuit) through a public Internet WAN connection.

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

Located at the edge of the enterprise network is an Acme SBC. It has a public side that connects to Level 3 via the internet and a private side that connects to the enterprise network. All SIP and RTP traffic entering or leaving the enterprise network flows through the Acme SBC which can protect the enterprise against any outside SIP-based attacks. The Acme SBC provides network address translation at both the IP and SIP layers. The transport protocol between the Acme SBC and Level 3 across the public network is UDP; the transport protocol between the Acme SBC and Session Manager across the enterprise network is TCP. In the compliance testing, the Avaya CPE environment is configured with SIP domain **level3.com** for the enterprise. The Acme SBC is used to adapt the enterprise SIP domain to the IP address based URI-Host known to Level 3. **Figure 1** below illustrates the network diagram for the enterprise.

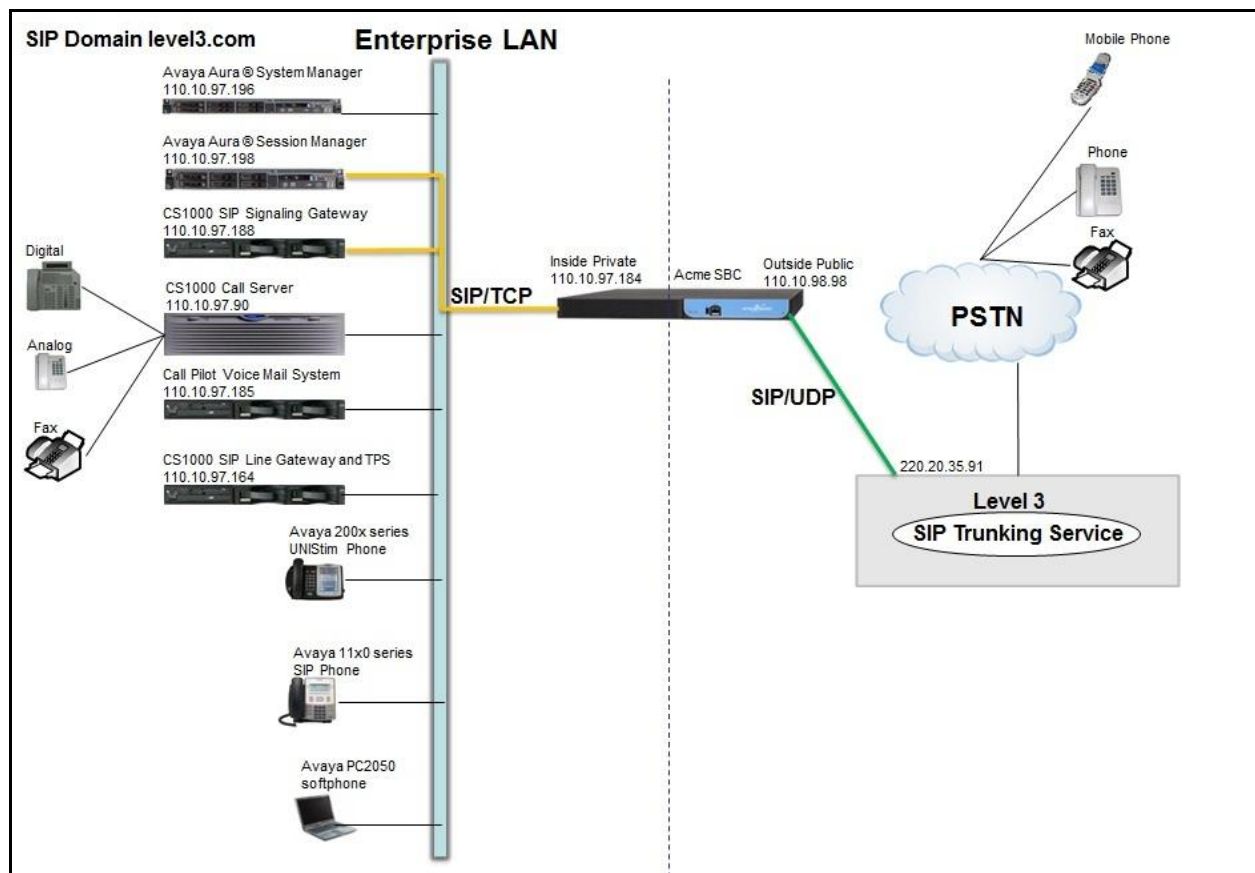


Figure 1: Avaya IP Telephony Network connecting to Level 3 SIP Trunking Service

4. Equipment and Software Validated

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

Avaya IP Telephony Solution Components	
Component	Release
Avaya CS1000 7.5 (CPPM)	<ul style="list-style-type: none">• Call Server: 7.50 Q GA plus latest DEPLIST – Issue: 01 Release: x2107.50, 2012-05-16 12:51:18 (est)• SSG Server: 7.50.17 GA plus latest Service_Pack_Linux_7.50_17_20120516.ntl• SLG Server: 7.50.17 GA plus latest Service_Pack_Linux_7.50_17_20120516.ntl
Avaya Aura® System Manager running on Avaya S8800 Server	<ul style="list-style-type: none">• 6.1.5.0 Build number 6.1.0.0.7345 Patch 6.1.5.9
Avaya Aura® Session Manager running on Avaya S8800 Server	<ul style="list-style-type: none">• 6.1.1.0.611023
Avaya IP Telephone	<ul style="list-style-type: none">• 2002 p2: 0604DCJ (UNISim)• 2004 p2: 0604DCJ (UNISim)• 1140: 0625C6O (UNISim)• 1120: 0624C6O (UNISim)• 2007: 0621C6M (UNISim)• 1220: 062AC6O (UNISim)• SIP 1120, 1140: SIP12x0e04.00.04.00• SIP 1220,1240: SIP12x0e04.00.04.00
Avaya CallPilot	05.00.41.141
Avaya 2050PC softphone	3.4
Avaya Digital Telephone	n/a
Avaya Analog Telephone	n/a
Acme Packet Session Border Controller 3800	Net-Net 3800 Firmware SCX6.2.0 MR-9 GA
Level 3 SIP Trunking Service Components	
Component	Release
Level 3 Enterprise Edge	Version 1

Table 1: Equipment and Software Tested

5. Avaya Communication Server 1000 Configuration

This section describes the procedure for configuring the CS1000 for inter-operating with the Level 3.

A two-way SIP trunk is created between the CS1000 and Session Manager to carry traffic to and from the service provider. For an inbound call, the call flows from Level 3 to the Acme SBC to the CS1000 via Session Manager. Once the call arrives at the CS1000, further incoming call

treatment, such as incoming digit translations and class of service restrictions may be performed. Outbound calls to the PSTN are first processed by the CS1000 for outbound feature treatment such as route selection and class of service. Once the CS1000 has selected the proper SIP trunk, the call is routed to Session Manager and then on toward the Acme SBC for egress to the Level 3.


For the compliance test, CS1000 sends 11 digits in the destination headers (e.g., Request-URI and To) and sends 10 digit in the source headers (e.g., From, Contact, and P-Asserted-Identity (PAI)). Level 3 sends 10 digits in destination headers and sends 10 digits in source headers.

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

5.1. Login to CS1000

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

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



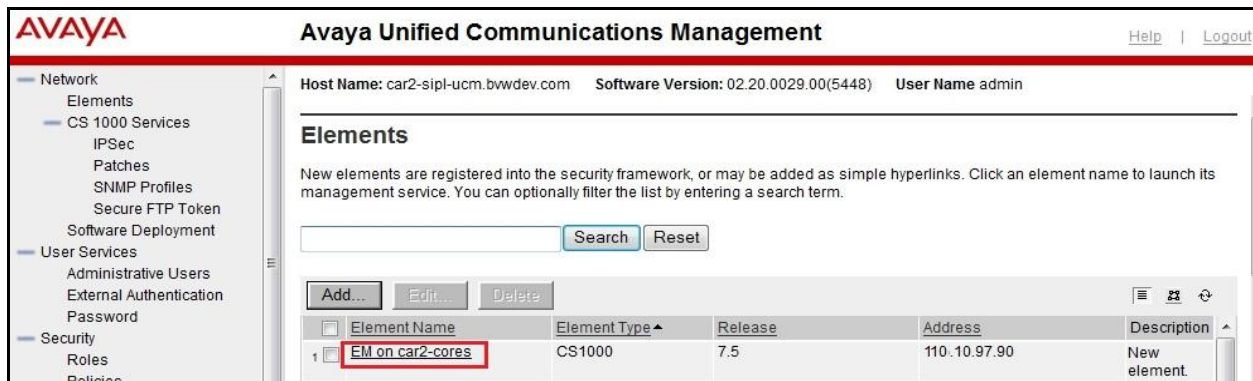
This computer system and network is PRIVATE and PROPRIETARY of [company name] and may only be accessed by authorized users. Unauthorized use of this computer system or network is strictly prohibited and may be subject to criminal prosecution, employee discipline up to and including discharge, or the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

User ID:

Password:

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

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



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



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

- Using Putty, SSH to the IP address of the SSG Server with the admin account.
- Run the command "cslogin" and login with the appropriate admin account and password.
- Here are the logs.

```
login as: admin

Avaya Inc. Linux Base 7.50
The software and data stored on this system are the property of,
or licensed to, Avaya Inc. and are lawfully available only
to authorized users for approved purposes. Unauthorized access
to any software or data on this system is strictly prohibited and
punishable under appropriate laws. If you are not an authorized
user then do not try to login. This system may be monitored for
operational purposes at any time.

admin@110.10.97.172's password:
Last login: Wed Nov 2 11:32:26 2011 from 110.10.98.105

[admin@car2-sps ~]$
[admin@car2-sps ~]$ cslogin

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

TTY 09 SCH MTC TRF BUG OSN 14:05
OVL111 BKGD 44
```

5.2. Administer a Node IP Telephony

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

5.2.1. Obtain Node IP address

These Application Notes assume the basic configuration has already been administered and that a Node has already been created. This section describes configuration steps for Node ID 2005.

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

AVAYA CS1000 Element Manager Help | Logout

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

IP Telephony Nodes
Click the Node ID to view or edit its properties.

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

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

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

b) The **Node Details** page is shown in the screenshot below with the IP address of the Node ID 2005. The SIP Signaling Gateway uses the **Node IP Address** to connect to Session Manager for the SIP Trunk to Level 3.

AVAYA CS1000 Element Manager Help | Logout

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

Node Details (ID: 2005 - 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
- SNTP
- Numbering Zones
- MCDN Alternative Routing Treatment (MALT) Causes

Applications (click to edit configuration)

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

* Required Value. Save Cancel

5.2.2. Administer Quality of Service (QoS)

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

AVAYA CS1000 Element Manager

Help | Logout

Managing: 110.10.97.90 Username: admin

System » IP Network » IP Telephony Nodes » Node Details » Quality of Service (QoS)

Node ID: 2005 - Quality of Service (QoS)

Diffserv Codepoint (DSCP)

Enable Avaya automatic QoS: ☒

Control packets: 40 (0-63)

Voice packets: 46 (0-63)

VLAN tagging: ☐ 802.1Q support

802.1Q bits value (802.1P): 6 (0-7)

5.2.3. Synchronize the new configuration

- d) Continued from **Section 5.2.3**, return to the **Node Details** page (not shown) and click the **Save** button.
- e) The **Node Saved** screen is displayed. Click **Transfer Now** button (not shown).
- f) The **Synchronize Configuration Files** screen is displayed (not shown). Check the Signaling Server checkbox and click the **Start Sync** button (not shown).
- g) When the synchronization completes, check the Signaling Server check box and click the **Restart Applications** button (not shown).

5.3. Administer Voice Codec

5.3.1. Enable Voice Codec, Node IP Telephony

- a) To configure a Voice Codec, select **IP Network** → **Nodes: Servers, Media Cards** from the left pane, and in the **IP Telephony Nodes** screen, select the **Node ID** of the CS1000 system. The **Node Details** screen is displayed as described in **Section 5.2.1**.
- b) On the **Node Details** page (not shown), click on **Voice Gateway (VGW) and Codec**.
- c) Level 3 supports voice codecs G.729 and G.711, payload size 20 ms, with VAD disabled. The following screenshots show appropriated voice codec profiles configured on the CS1000.

AVAYA CS1000 Element Manager Help | Logout

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

Node ID: 2005 - Voice Gateway (VGW) and Codecs

General | Voice Codecs | Fax

Voice Codecs

Codec G711: ☒ Enabled (required)

Voice payload size: 20 (milliseconds per frame)

Voice playout (jitter buffer) delay: 40 80 (milliseconds)
Nominal Maximum
Maximum delay may be automatically adjusted based on nominal settings.

☒ Voice Activity Detection (VAD)

Codec G722: ☐ Enabled

AVAYA CS1000 Element Manager Help | Logout

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

Node ID: 2005 - Voice Gateway (VGW) and Codecs

General | Voice Codecs | Fax

Voice Codecs

Codec G729: ☒ Enabled

Voice payload size: 20 (milliseconds per frame)

Voice playout (jitter buffer) delay: 40 80 (milliseconds)
Nominal Maximum
Maximum delay may be automatically adjusted based on nominal settings.

☒ Voice Activity Detection (VAD)

Codec G723.1: ☐ Enabled

d) For Fax over IP, Level 3 supports T.38. This parameter is enabled by default on the CS1000 as shown in the following screenshot.

AVAYA CS1000 Element Manager Help | Logout

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

Node ID: 2005 - Voice Gateway (VGW) and Codecs

General | Voice Codecs | Fax

Voice Codecs

Codec G723.1: ☐ Enabled

Voice payload size: 30 (milliseconds per frame)

Voice playout (jitter buffer) delay: 60 120 (milliseconds)
Nominal Maximum
Maximum delay may be automatically adjusted based on nominal settings.

Coding rate: 5.3 (kbps)

Fax

Codec name: T.38 FAX

Maximum rate: 14400 (bps)

Fax TCF method: 2

Fax playout nominal delay: 100 (0 - 300 milliseconds)

FAX no activity timeout: 20 (10 - 32000 milliseconds)

Packet size: 30 (bps)

e) Click **Save**.

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

Note: Fax over IP using G.711MU codec is not supported, please refer to **Section 2.2**, observation #01 for detail information.

5.3.2. Administer Voice Codec on Media Gateways

The CS1000 uses media gateways to support traditional analog and digital phones calls over a SIP Trunk. Media gateways are also needed to support analog terminals and to send fax over IP.

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

b) Level 3 supports voice codecs G.729 and G.711, payload size 20 ms, with VAD disabled. The screenshot below shows appropriated codec profile configured for media gateways.

AVAYA CS1000 Element Manager

Media Gateways Configuration

Codec G.711

Codec name: G.711

Voice payload size: 20 (ms/frame)

Voice playout (jitter buffer) nominal delay: 40

Voice playout (jitter buffer) maximum delay: 80

VAD: ☐

Codec G.729A

Codec name: G.729A

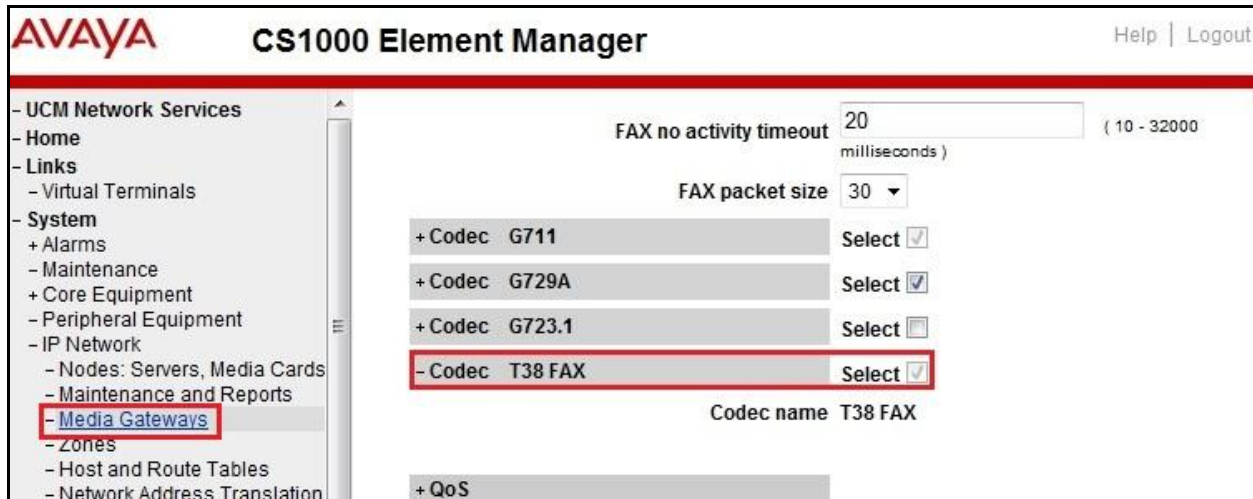
Voice payload size: 20 (ms/frame)

Voice playout (jitter buffer) nominal delay: 40

Voice playout (jitter buffer) maximum delay: 80

VAD: ☐

c) For Fax over IP, Level 3 supports T.38 codec. This parameter is enabled by default on CS1000 as shown in the following screenshot.



Note: Fax over IP using G.711MU codec is not supported, please refer to **Section 2.2**, observation #01 for detail information.

5.4. Administer Zones and Bandwidth

This section describes the steps to create 2 zones: zone 10 for Voice Gateway (VGW) and IP phones and zone 255 for a SIP Trunk. The CS1000 uses zone configuration for bandwidth management purposes.

5.4.1. Create a zone for IP phones

a) To create zone 10 for VGW and IP phone, select **IP Network** → **Zones** configuration from the left pane, click **Bandwidth Zones** link (not shown).
 b) In **Bandwidth Zones** screen (not shown), click **Add** button (not shown).
 c) In the **Add Bandwidth Zone** screen (not shown), click on **Zone Basic Property and Bandwidth Management**, select the values as shown (in red box) in the screenshot below and click on the **Submit** button.

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

Level 3 supports G.729 as the first choice, G.711. In the sample configuration as shown in the screenshot below, the **MO** Zone 10 is configured with **Strategy Best Quality (BQ)** to allow the CS1000 to select G.711MU as a first choice and G.729 as the second choice for a voice call.

AVAYA

CS1000 Element Manager

Help | Logout

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

QoS Thresholds

Personal Directories

Unicode Name Directory

Interfaces

Engineered Values

Emergency Services

Geographic Redundancy

Software

Customers

Managing: 110.10.97.90 Username: admin

System » IP Network » Zones » Bandwidth Zones » Bandwidth Zones 10 » Edit Bandwidth Zone » Zone Basic Property and Bandwidth Management

Zone Basic Property and Bandwidth Management

Input Description	Input Value
Zone Number (ZONE):	10 (1 - 8000)
Intrazone Bandwidth (INTRA_BW):	100000 (0 - 10000000)
Intrazone Strategy (INTRA_STGY):	Best Quality (BQ)
Interzone Bandwidth (INTER_BW):	100000 (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

5.4.2. Create a zone for virtual SIP trunk

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

AVAYA

CS1000 Element Manager

Help | Logout

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

QoS Thresholds

Personal Directories

Unicode Name Directory

Interfaces

Engineered Values

Emergency Services

Geographic Redundancy

Software

Customers

Managing: 110.10.97.90 Username: admin

System » IP Network » Zones » Bandwidth Zones » Bandwidth Zones 255 » Edit Bandwidth Zone » Zone Basic Property and Bandwidth Management

Zone Basic Property and Bandwidth Management

Input Description	Input Value
Zone Number (ZONE):	255 (1 - 8000)
Intrazone Bandwidth (INTRA_BW):	100000 (0 - 10000000)
Intrazone Strategy (INTRA_STGY):	Best Quality (BQ)
Interzone Bandwidth (INTER_BW):	100000 (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

5.5. Administer SIP Trunk Gateway

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

5.5.1. Integrated Services Digital Network (ISDN)

a) To configure ISDN, select **Customers** in the left pane. The **Customers** screen is displayed (not shown). Click on the link associated with the appropriate customer, in this case is 05. The system can support more than one customer with different network settings and options. The **Customer 05 Edit** page will appear (not shown). Select the **Feature Packages** option from this page (not shown).

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

The screenshot displays the AVAYA CS1000 Element Manager web interface. On the left is a navigation tree with the following items: UCM Network Services, Home, Links, Virtual Terminals, System, Alarms, Maintenance, Core Equipment, Peripheral Equipment, IP Network, Interfaces, Engineered Values, Emergency Services, Geographic Redundancy, Software, Customers (highlighted with a red box), Routes and Trunks, and Routes and Trunks. The main content area shows the configuration for the 'Integrated Services Digital Network' feature package (Package: 145). A red box highlights the following fields: 'Integrated Services Digital Network' (checked), 'Virtual private network identifier' (5), 'Private network identifier' (5), and 'Node DN' (2005). Other visible fields include 'Multi-location business group' (0), 'Business sub group consult-only' (65535), 'Prefix 1', and 'Prefix 2'. The top of the interface shows the 'Enhanced Night Service' package (133).

5.5.2. Administer SIP Trunk Gateway to Session Manager

a) To configure SIP Trunk Gateway, select **IP Network → Nodes: Servers, Media Cards** configuration from the left pane, and in the **IP Telephony Nodes** screen, select the **Node ID** 2005. The **Node Details** screen is displayed as shown in **Section 5.2.1**.

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

c) Under **General** tab of the **Virtual Trunk Gateway Configuration Details** screen, enter the following values which are highlighted in red boxes as shown in screenshot below. These configurations are obtained when a user creates a SIP Entity on the Session Manager, these are shown in **Section 6.4**. Retain the default values for the remaining fields.

- **Vtrk gateway application:** SIP Gateway (SIPGw)
- **SIP domain name:** level3.com
- **Local SIP port:** 5060
- **Gateway endpoint name:** 1-23Q-3413 (This parameter is provided by Level 3)

- **Gateway password:** ***** (This parameter is provided by Level 3)
- **Application node ID:** 2005

Note: The gateway endpoint name and gateway password values are provided by Level 3, they are used by the CS1000 to construct a proper response to the Digest Authentication challenges implemented on the SIP Trunk by Level 3.

AVAYA CS1000 Element Manager

Managing: 110.10.97.90 Username: admin

System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration

Node ID: 2005 - 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: level3.com *

Local SIP port: 5060 * (1 - 65535)

Gateway endpoint name: 1-23Q-3413 *

Gateway password: ***** *

Application node ID: 2005 * (0-9999)

Enable failsafe NRS: ☐

SIP ANAT: ☒ IPv4 ☐ IPv6

Virtual Trunk Network Health Monitor

☐ Monitor IP addresses (listed below)

Information will be captured for the IP addresses listed below.

Monitor IP: Add

Monitor addresses: Remove

* Required Value.

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

Save Cancel

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

AVAYA CS1000 Element Manager

Help | Logout

Managing: 110.10.97.90 Username: admin

System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration

Node ID: 2005 - Virtual Trunk Gateway Configuration Details

General | SIP Gateway Settings | SIP Gateway Services

Proxy Or Redirect Server:

Proxy Server Route 1:

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

Port: 5060 (1 - 65535)

Transport protocol: TCP

Options: ☐ Support registration
☐ Primary CDS proxy

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

Port: 5060 (1 - 65535)

Transport protocol: TCP

* Required Value.

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

Save Cancel

e) On the same page, scroll down to the **SIP URI Map** section as shown in the screenshot below. Under the **Public E.164 Domain Names**:

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

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

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

f) Then click **Save** button.

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

AVAYA CS1000 Element Manager

Managing: 110.10.97.90 Username: admin

System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration

Node ID: 2005 - Virtual Trunk Gateway Configuration Details

General | SIP Gateway Settings | SIP Gateway Services

SIP URI Map:

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

SIP Gateway Services

5.5.3. Administer Virtual D-Channel

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

b) The **D-Channels Property Configuration** of DCH 105 is shown in the screenshot below. Enter the following values for the specified fields, and retain the default values for the remaining fields.

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

AVAYA

CS1000 Element Manager

Help | Logout

UCM Network Services

Home

Links

System

Customers

Routes and Trunks

D-Channels

Dialing and Numbering Plans

Phones

Tools

Security

Managing: 110.10.97.90 Username: admin

Routes and Trunks » D-Channels » D-Channels 105 Property Configuration

D-Channels 105 Property Configuration

Basic Configuration

Input Description	Input Value
Action Device And Number (ADAN):	DCH
D channel Card Type:	DCIP
Designator:	Level3
Recovery to Primary:	<input type="checkbox"/>
PRI loop number for Backup D-channel:	
User:	Integrated Services Signaling Link Dedicated (ISLD)
Interface type for D-channel:	Meridian Meridian1 (SL1)
Country:	ETS 300 =102 basic protocol (ETSI)
D-Channel PRI loop number:	
Primary Rate Interface:	<input type="button" value="more PRI"/>
Secondary PRI2 loops:	
Meridian 1 node type:	Slave to the controller (USR)
Release ID of the switch at the far end:	25
Central Office switch type:	100% compatible with Bellcore standard (STD)
Integrated Services Signaling Link Maximum:	4000 Range: 1 - 4000
Signalling server resource capacity:	3700 Range: 0 - 3700

+ Basic options (BSCOPT)

+ Advanced options (ADVOPT)

+ Feature Packages

Submit

Refresh

Delete

Cancel

- c) Continued from **D-Channels Property Configuration** described above, click on the **Basic Options** then click on the **Edit** button next to the **Remote Capabilities (RCAP)** attribute (not shown). The **Remote Capabilities Configuration** page will appear. Then check on the **ND2** and the **MWI** checkboxes as shown in the screenshot below.
- d) Click **Return – Remote Capabilities** button (not shown).
- e) Click **Submit** 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
- Interfaces
- Engineered Values
- Emergency Services
- Geographic Redundancy
- Software
- Customers
- Routes and Trunks
- Routes and Trunks
- **D-Channels**
- Digital Trunk Interface
- Dialing and Numbering Plans
- Electronic Switched Network
- Flexible Code Restriction
- Incoming Digit Translation
- Phones
- Templates
- Reports
- Views
- Lists
- Properties
- Migration
- Tools
- Backup and Restore
- Date and Time
- Logs and reports
- Security
- Passwords
- Policies
- Login Options

Managing: **110.10.97.90** Username: admin
Routes and Trunks > D-Channels > D-Channels 105 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 (MWM)	<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"/>

5.5.4. Administer Virtual Super-Loop

To add a virtual loop, select **System** → **Core Equipments** → **Superloops** from the left pane to display the **Superloops** screen. If the Superloop does not exist, then click “**Add**” button, provide an available virtual loop identification number then click the Save button (not shown) to create a new one as shown in the screenshot below. In this example, Superloop 104 is added.

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

Interfaces

Engineered Values

Emergency Services

Geographic Redundancy

Managing: 110.10.97.90 Username: admin

System » Core Equipment » Superloops

Superloops

Add...

Delete

Refresh

	Superloop Number ▲	Superloop Type
1	4	IPMG
2	24	Virtual
3	96	Virtual
4	100	Virtual
5	104	Virtual
6	108	Virtual
7	112	Phantom

5.5.5. Enable Music for Customer Data Block

- To enable music for a customer, select **Customers** in the left pane. The **Customers** screen is displayed (not shown). Click on the link associated with the appropriate customer, in this case is 05. The **Customer 05 Edit** page will appear (not shown). Select the **Feature Packages** option from this page (not shown).
- The screen is populated with a list of **Feature Packages**. Select **Enhanced Music** to edit its parameters. Check to enable music for Customer 05, define music route 55 as shown in the red box of screenshot below. The CS1000 has been pre-configured with music route 55.

AVAYA CS1000 Element Manager Help | Logout

Managing: **110.10.97.90** Username: admin
[Customers](#) » [Customer 05](#) » [Customer Details](#) » [Feature Packages](#)

Feature Packages

+ Do Not Disturb Individual	Package: 9
+ End-to-End Signaling	Package: 10
+ Message Waiting Center	Package: 46
+ New Flexible Code Restriction	Package: 49
+ Set Relocation	Package: 53
+ Network Alternate Route Selection	Package: 58
+ Distinctive Ringing	Package: 74
+ Departmental Listed Directory Number	Package: 76
+ Command Status Link	Package: 77
+ Pretranslation	Package: 92
+ Dialed Number Identification System	Package: 98
+ Malicious Call Trace	Package: 107
+ Incoming Digit Conversion	Package: 113
+ Directed Call Pickup	Package: 115
- Enhanced Music	Package: 119
Music for sets: <input checked="" type="checkbox"/>	
- Music Route for sets: 55	
+ Station Camp-On	Package: 121
+ Integrated Digital Access	Package: 122

5.5.6. Administer Virtual SIP Routes

a) To create a SIP Route, select **Routes and Trunks** → **Routes and Trunks** from the left pane to display the **Routes and Trunks** screen. In this example, **Customer 05** is added. Click **Add route** button as shown in the screenshot below.

AVAYA CS1000 Element Manager Help | Logout

Managing: **110.10.97.90** Username: admin
[Routes and Trunks](#) » [Routes and Trunks](#)

Routes and Trunks

+ Customer: 0	Total routes: 2	Total trunks: 32	<input type="button" value="Add route"/>
+ Customer: 1	Total routes: 2	Total trunks: 34	<input type="button" value="Add route"/>
+ Customer: 3	Total routes: 3	Total trunks: 66	<input type="button" value="Add route"/>
+ Customer: 4	Total routes: 3	Total trunks: 66	<input type="button" value="Add route"/>
+ Customer: 5	Total routes: 2	Total trunks: 34	<input type="button" value="Add route"/>

b) The **Customer 5, New Route Configuration** screen is displayed (not shown). Scroll down until the **Basic Configuration** section is displayed and enter the following values for the

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

- **Route Number (ROUT):** Select an available route number
- **Designator field for trunk (DES):** A descriptive text
- **Trunk Type (TKTP):** TIE trunk data block (TIE)
- **Incoming and Outgoing trunk (ICOG):** Incoming and Outgoing (IAO)
- **Access Code for the trunk route (ACOD):** An available access code
- Check the field **The route is for a virtual trunk route (VTRK)**, to enable additional fields to appear
- For the **Zone for codec selection and bandwidth management (ZONE)** field, enter 255 (created in **Section 5.4.2**)
- For the **Node ID of signalling server of this route (NODE)** field, enter the node number 2005 (created in **Section 5.2.1**)
- Select **SIP (SIP)** from the drop-down list for **the Protocol ID for the route (PCID)** field
- Check the **Integrated Services Digital Network option (ISDN)** checkbox to enable additional fields to appear. Enter the following values for the specified fields, and retain the default values for the remaining fields
 - **Mode of operation (MODE):** Route uses ISDN Signalling Link (ISLD)
 - **D channel number (DCH):** D-Channel number 105 (created in **Section 5.5.3**)
 - **Network calling name allowed (NCNA):** Checked
 - **Network call redirection (NCRD):** Checked
 - **Insert ESN access code (INAC):** Checked

CS1000 Element Manager

[Help](#) | [Logout](#)

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

Managing: **110.10.97.90** Username: admin
 Routes and Trunks » [Routes and Trunks](#) » Customer 5, Route 105 Property Configuration

Customer 5, Route 105 Property Configuration

- Basic Configuration

Route data block (RDB) (TYPE) :

Customer number (CUST) :

Route number (ROUT) :

Designator field for trunk (DES) :

Trunk type (TKTP) :

Incoming and outgoing trunk (ICOG) :

Access code for the trunk route (ACOD) :

Trunk type M911P (M911P) :

☐

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

☒

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

(0 - 8000)

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

(0 - 9999)

- Protocol ID for the route (PCID) :

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

☐

Integrated services digital network option (ISDN) :

☒

- Mode of operation (MODE) :

- D channel number (DCH) :

(0 - 254)

- Interface type for route (IFC) :

- Private network identifier (PNI) :

(0 - 32700)

- Network calling name allowed (NCNA) :

☒

- Network call redirection (NCRD) :

☒

- Trunk route optimization (TRO) :

☐

- Recognition of DT12 ABCD FALT signal for ISL (FALT) :

☐

- Channel type (CHTY) :

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

- Insert ESN access code (INAC) :

☒

- Integrated service access route (ISAR) :

☐

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

AVAYA
CS1000 Element Manager

Help | Logout

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

Managing: **110.10.97.90** Username: admin
Routes and Trunks » Routes and Trunks » Customer 5, Route 105 Property Configuration

Customer 5, Route 105 Property Configuration

+ Basic Configuration
- Basic Route Options

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

+ Network Options
+ General Options
+ Advanced Configurations

- Continued from **Route Configuration** described above, click on **Advance Configurations**; check **Music-on-holds** to enable music on hold on the route. Input music route 55 to the boxes as shown in the screenshot below. The CS1000 has been pre-configured with route 55 as a music route.
- c) Click **Submit** 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
- 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

Identify originating party (IDOP) :
Insert (INST) :
Manual outgoing trunk route (MANO) :
Manual route (MNL) :
Music on-hold (MUS) :
- Music route number (MRT) : 55 (0 - 511)
Outgoing identifier send (OGIS) :
Off-hook timer delay (OHTD) :
Outpulsing route (OPR) :
Pseudo answer (PANS) :
Periodic clearing signal (PECL) :
Privacy indicator ignored (PII) :
Auxiliary application (AUXP) :
Priority level (PLEV) : 2
Protocol selection (PSEL) : DM-DM Protocol Selection (DMDM)
Preference trunk usage threshold (PTUT) : 0 (0 - 510)

5.5.7. Administer Virtual Trunks

a) Continued from **Section 5.5.6**, the **Routes and Trunks** screen is displayed and updated with the newly added route (not shown). In the compliance test, route 105 is added. Click **Add trunk** button next to the newly added route 105 as shown in the screenshot below.

AVAYA CS1000 Element Manager Help | Logout

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

Routes and Trunks

Customer	Total routes	Total trunks	Action
+ Customer: 0	2	32	Add route
+ Customer: 1	2	34	Add route
+ Customer: 3	3	66	Add route
+ Customer: 4	3	66	Add route
- Customer: 5	2	34	Add route

Route	Type	Description	Action
+ Route: 55	MUS	MUS	Edit Add trunk
+ Route: 105	TIE	LEVEL3	Edit Add trunk

b) The **Customer 5, Route 105, Trunk 1 Property Configuration** is shown in the screenshot below. Enter **The Multiple trunk input number (MTINPUT)** field to add multiple trunks in a single operation, or repeat the operation for each trunk. In the certification test, 32 trunks are created (not shown). The following values are entered for specified fields and retain the default values for the remaining fields.

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

AVAYA **CS1000 Element Manager** Help | Logout

Managing: **110.10.97.90** Username: admin
 Routes and Trunks » Routes and Trunks » Customer 5, Route 105, Trunk 1 Property Configuration

Customer 5, Route 105, Trunk 1 Property Configuration

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

- Basic Configuration

Auto increment member number: ☒
 Trunk data block:
 Terminal number:
 Designator field for trunk:
 Extended trunk:
 Member number:

 Level 3 Signaling:
 Card density:

Start arrangement Incoming:
 Start arrangement Outgoing:
 Trunk group access restriction:
 Channel ID for this trunk:

 Class of Service: Edit

+ Advanced Trunk Configurations

c) The Media Security (sRTP) has to be disabled at the trunk level by editing the **Class of Service (CLS)** at the bottom basic trunk configuration page. Click **Edit** button. For **Media Security**, select **Media Security Never (MSNV)**. Select **Restriction level** as **Unrestricted (UNR)**. The remaining values are kept as default as shown in the screenshot below. Scroll down to the bottom of the screen and click **Return Class of Service** and then click **Save** button (not shown).

AVAYA **CS1000 Element Manager** Help | Logout

- Maintenance
- + Core Equipment
- Peripheral Equipment
- + IP Network
- + Interfaces
- Engineered Values
- + Emergency Services
- + Geographic Redundancy
- + Software
- Customers
- Routes and Trunks
 - Routes and Trunks**
 - D-Channels
 - Digital Trunk Interface
- Dialing and Numbering Plans
 - Electronic Switched Network
 - Flexible Code Restriction
 - Incoming Digit Translation
- Phones
 - Templates
 - Reports
 - Views
 - Lists
 - Properties
 - Migration

- 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

5.5.8. Administer Calling Line Identification Entries

a) To create a Calling Line Identification Entry, select **Customers > 05 > ISDN and ESN Networking**. Click on **Calling Line Identification Entries** link at the bottom of the page (not shown)

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

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

- **National Code:** leave as blank
- **Local Code:** input prefix digits assigned by Service Provider, in this case it is 6 digits – 716261. This **Local Code** is used for call display purpose of outbound international call configuration in **Section 5.6.6** where the Special Number 0 is associated with Call Type = Unknown
- **Home Location Code:** input prefix digits assigned by Service Provider, in this case it is 6 digits - 716261. This **Home Location Code** is used for call display purpose for Call Type = National (NPA)
- **Local Steering Code:** input prefix digits assigned by Service Provider, in this case it is 6 digits - 716261. This **Local Steering Code** is be used for call display purpose for Call Type = Local Subscriber (NXX)
- **Calling Party Name Display:** Uncheck Roman characters

d) Click **Save** button.

AVAYA
CS1000 Element Manager
[Help](#) | [Logout](#)

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

Managing: **110.10.97.90** Username: admin
[Customers](#) » [Customer 05](#) » [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: YES

Emergency Services Access

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

Emergency Options:

☐ Home national number for emergency services access calls

☒ Append the originating directory number for emergency services access calls

Calling Party Name Display

Roman characters: ☐

CPND Name:
first name, last name

Expected Length:

Display Format: First name, Last name

Save Cancel

5.5.9. Enable External Trunk to Trunk Transferring

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

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

```

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

TYPE NET_DATA
CUST 5
OPT
...
TRNX YES
EXTT YES
  
```

5.5.10. Enable plug-in 501

This section shows how to enable plug-in 501 in pdt mode to support blind transfer without UPDATE method. For more information, please refer to **Section 2.2**, observation #02.

- a) Login Call Server CLI (please refer to **Section 5.1.2** for more detail).
- b) Press Ctrl + pdt.
- c) Login using user name as admin and provide proper password.
- d) Issue command “ple 501” to enable plug-in 501.

```
PDT login on /pty/ptty01.S
Username: admin
Password:

The software and data stored on this system are the property of,
or licensed to, Avaya Inc. and are lawfully available only to
authorized users for approved purposes. Unauthorized access to
any software or data on this system is strictly prohibited and
punishable under appropriate laws. If you are not an authorized
user then logout immediately. This system may be monitored for
operational purposes at any time.
pdt> ple 501

PLUG-IN 501  IS ENABLED

pdt>
```

5.6. Administer Dialing Plans

5.6.1. Define ESN Access Codes and Parameters (ESN)

- a) Select **Dialing and Numbering Plans → Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen. When Administering Dial Plans, the highlighted sections below will be configured in this section in the order they appear on the screen. To configure ESN parameter, select **ESN Access Code and Parameters (ESN)**.

AVAYA

CS1000 Element Manager

[Help](#) | [Logout](#)

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

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

Electronic Switched Network (ESN)

- + Customer 00
- + Customer 01
- + Customer 03
- + Customer 04
- **Customer 05**
 - Network Control & Services
 - Network Control Parameters (NCTL)
 - ESN Access Codes and Parameters (ESN)
 - Digit Manipulation Block (DGT)
 - Home Area Code (HNPA)
 - Flexible CLID Manipulation Block (CMDB)
 - Free Calling Area Screening (FCAS)
 - Free Special Number Screening (FSNS)
 - Route List Block (RLB)
 - Incoming Trunk Group Exclusion (ITGE)
 - Network Attendant Services (NAS)
 - Coordinated Dialing Plan (CDP)
 - Local Steering Code (LSC)
 - Distant Steering Code (DSC)
 - Trunk Steering Code (TSC)
 - Numbering Plan (NET)
 - Access Code 1
 - Home Location Code (HLOC)
 - Location Code (LOC)
 - **Numbering Plan Area Code (NPA)**
 - **Exchange (Central Office) Code (NXX)**
 - **Special Number (SPN)**
 - Network Speed Call Access Code (NSCL)
 - Access Code 2
 - Home Location Code (HLOC)
 - Location Code (LOC)
 - Numbering Plan Area Code (NPA)
 - Exchange (Central Office) Code (NXX)
 - Special Number (SPN)
 - Network Speed Call Access Code (NSCL)

- b) In the **ESN Access Codes and Basic Parameters** page, define **NARS/ BARS Access Code 1** and disable **Check for Trunk Group Access Restrictions** as shown in the screenshot below.
- c) Click **Submit** button (not shown).

AVAYA **CS1000 Element Manager** Help | Logout

- + IP Network
- + Interfaces
- Engineered Values
- + Emergency Services
- + Geographic Redundancy
- + Software
- Customers
- Routes and Trunks
 - Routes and Trunks
 - D-Channels
 - Digital Trunk Interface
- **Dialing and Numbering Plans**
 - **Electronic Switched Network**
 - Flexible Code Restriction
 - Incoming Digit Translation
- Phones
 - Templates
 - Reports
 - Views
 - Lists
 - Properties
 - Migration
- Tools
 - + Backup and Restore
 - + Date and Time
 - + Logs and reports
- Security
 - + Passwords

Managing: **110.10.97.90** Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 05 » Network Control & Services » ESN Access Codes and Basic Parameters

ESN Access Codes and Basic Parameters

General Properties

NARS/BARS Access Code 1: 6

NARS Access Code 2: 9
NARS/BARS Dial Tone after dialing AC1 or AC2 access codes: ☒
Expensive Route Warning Tone: ☒
- Expensive Route Delay Time: 6 (0 - 10)
Coordinated Dialing Plan feature for this customer: ☒
- Maximum number of Steering Codes: 64000 (1 - 64000)
- Number of digits in CDP DN (DSC + DN or LSC + DN): 4 (3 - 10)
Routing Controls: ☐

Check for Trunk Group Access Restrictions: ☐

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

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

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

TYPE NET_DATA
CUST 5
OPT
AC2 xNPA xSPN
FNP
CLID
...
```

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

```
>ld 21
PT1000

REQ: prt
TYPE: net
TYPE NET_DATA
CUST 4

TYPE NET_DATA
CUST 01
```

```
OPT RTA
AC1 INTL NPA SPN NXX LOC
AC2
FNP YES
...
```

5.6.3. Digit Manipulation Block (DMI)

a) To create a DMI, select **Dialing and Numbering Plans → Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen (not shown).

b) Select **Digit Manipulation Block (DGT)** as shown in **Section 5.6.1.b)** In the **Choose a DMI Number** field, select an available DMI from the drop-down list and click **to Add** (not shown).

c) The screenshot below shows DMI 1 is created with following values.

- **Number of leading digits to be Deleted (Del): 0**
- **Call Type to be used by the manipulated digits (CTYP): NPA**

d) Click **Submit** button.

AVAYA CS1000 Element Manager Help | Logout

Managing: 110.10.97.90 Username: admin
Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 05 » Network Control & Services » Digit Manipulation Block List » Digit Manipulation Block

Digit Manipulation Block

Digit Manipulation Index numbers: 1

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

Insert:

IP Special Number: ☐

Call Type to be used by the manipulated digits: NPA (NPA)

Submit Cancel

5.6.4. Route List Block (RLB)

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

a) To create RLB 105, select **Dialing and Numbering Plans → Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen. Select **Route List Block (RLB)** as shown in **Section 5.6.1**.

b) Select an available value .e.g. 105 in the textbox for the **route list index** and click on the “**to Add**” button (not shown).

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

- **Route number (ROUT): 105** (created in **Section 5.5.6**)
- **Digit Manipulation Index (DMI): 1** (created in **Section 5.6.3**)

d) On the same page, scroll down to the bottom of the screen, and click **Submit** 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
 + Interfaces
 - Engineered Values
 + Emergency Services
 + Geographic Redundancy
 + Software
 - Customers
 - Routes and Trunks
 - Routes and Trunks
 - D-Channels
 - Digital Trunk Interface
 - **Dialing and Numbering Plans**
 - **Electronic Switched Network**
 - Flexible Code Restriction
 - Incoming Digit Translation
 - Phones
 - Templates
 - Reports
 - Views
 - Lists
 - Properties
 - Migration
 - Tools
 + Backup and Restore
 - Date and Time
 + Logs and reports
 - Security
 + Passwords
 + Policies
 + Login Options

Managing: **110.10.97.90** Username: admin
 Dialing and Numbering Plans » **Electronic Switched Network (ESN)** » Customer 05 » Network Control & Services » **Route List Blocks** » Route List Block

Route List Block

General Properties

Number of Alternate Routing Attempts: (1 - 10)
 Initial Set: (0 - 64)
 Set Minimum Facility Restriction Level :
 Overlap Length: (0 - 24)
 Extended Local Calls: ☐
Route List Index: 105
 Entry Number for the Route List: (0 - 63)

Indexes

Time of Day Schedule:
 Facility Restriction Level: (0 - 7)
Digit Manipulation Index: 1
 ISL D-Channel Down Digit Manipulation Index: (0 - 1999)
 Free Calling Area Screening Index:
 Free Special Number Screening Index:
 Business Network Extension Route: ☐
 Incoming CLID Table: (0 - 256)

Options

Local Termination entry: ☐
Route Number: 105
 Skip Conventional Signaling: ☐
 Display Originator's Information: ☐

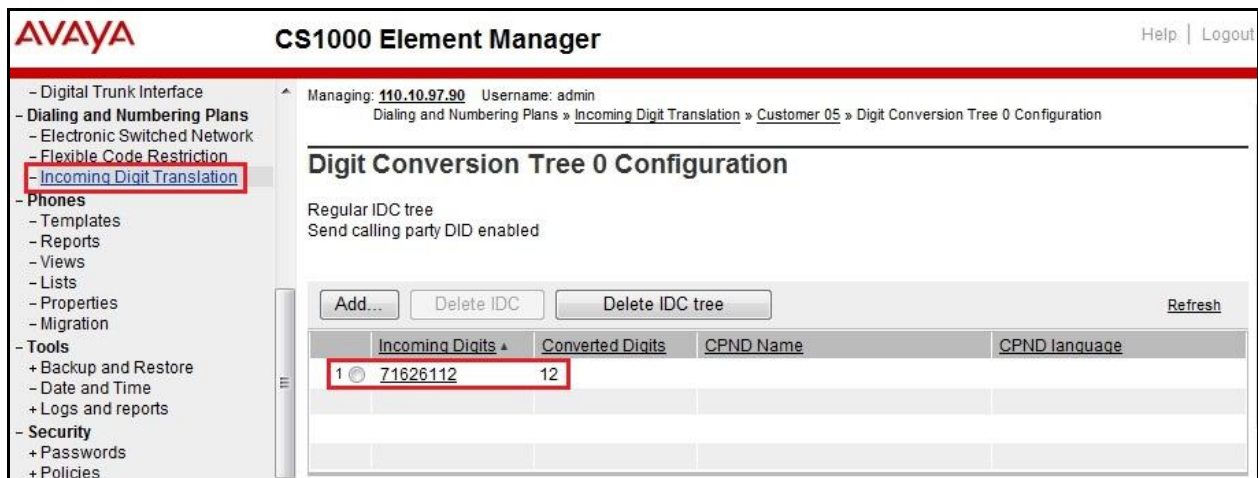
5.6.5. Incoming Digit Translation (IDC)

This section describes the steps for receiving calls from the PSTN via Level 3.

a) To create an IDC, select **Dialing and Numbering Plans** → **Incoming Digit Translation** from the left pane to display the **Incoming Digit Translation** screen. Click on the **Edit IDC** button (not shown).

b) Click on **New DCNO** to create a digit translation entry. In this example, Digit Conversion Tree Number (**DCN0**) **0** is created. Detail configuration of the **DCNO** is shown in screenshot below. The **Incoming Digits** can be added to map to the **Converted Digits** which would be the CS1000 DN. This **DCN0** has been assigned to route 105 as shown in **Section 5.5.6**.

In the following configuration, incoming calls from PSTN with prefix 71626112XX will be translated to CS1K DN 12XX, including the DID 7162611214 is translated to 1214 for voice mail access purpose.



5.6.6. Outbound Call - Special Number Configuration

Special numbers are configured for this testing. For example, 0 to reach an operator, 0+10 digits to reach operator assistant, 011 prefix for international calls, 1 for a national long distance call, 411 for directory assistant and so on.

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

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

Special Number: 0

- **Flexible length:** 0 (flexible, unlimited and accept the character # to ending dial number).
- **Call Type:** NONE.
- **Route list index:** 105, created in **Section 5.6.4**.

Special Number: 1

- **Flexible length:** 0 (flexible, unlimited and accept the character # to ending dial number).
- **Call Type:** NATL.
- **Route list index:** 105, created in **Section 5.6.4**.

Special Number: 411

- **Flexible length:** 3.
- **CallType:** SSER.
- **Route list index:** 105, created in **Section 5.6.4**.

AVAYA CS1000 Element Manager Help | Logout

Managing: 110.10.97.90 Username: admin
 Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 05 » Numbering Plan (NET) » Access Code 1 » Special Number List

Special Number List

Please enter a Special Number

Special Number -- 0	Flexible length: 0 International dialing plan: NO Type of call that is defined by the special number: NONE Route list index: 105	<input type="button" value="Edit"/>
Special Number -- 1	Flexible length: 0 Type of call that is defined by the special number: NATL Route list index: 105	<input type="button" value="Edit"/>
Special Number -- 411	Flexible length: 0 International dialing plan: NO Type of call that is defined by the special number: SSER Route list index: 105	<input type="button" value="Edit"/>

Left Navigation Menu:

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

5.6.7. Outbound Call - Numbering Plan Area (NPA)

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

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

b) Enter area code desired in the textbox and click “to Add” button (not shown). The screenshot below shows NPA numbers 716 is configured for this testing. These NPA numbers are associated to the SIP Trunk for 10-digit outbound local call.

AVAYA CS1000 Element Manager Help | Logout

Managing: 110.10.97.90 Username: admin
 Dialing and Numbering Plans » Electronic Switched Network (ESN) » Customer 05 » Numbering Plan (NET) » Access Code 1 » Numbering Plan Area Code List

Numbering Plan Area Code List

Please enter an area code

Numbering Plan Area Code -- 716	Route List Index: 105 Incoming Trunk group Exclusion Index: NONE	<input type="button" value="Edit"/>
---------------------------------	---	-------------------------------------

Left Navigation Menu:

- 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

6. Configure Avaya Aura® Session Manager

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

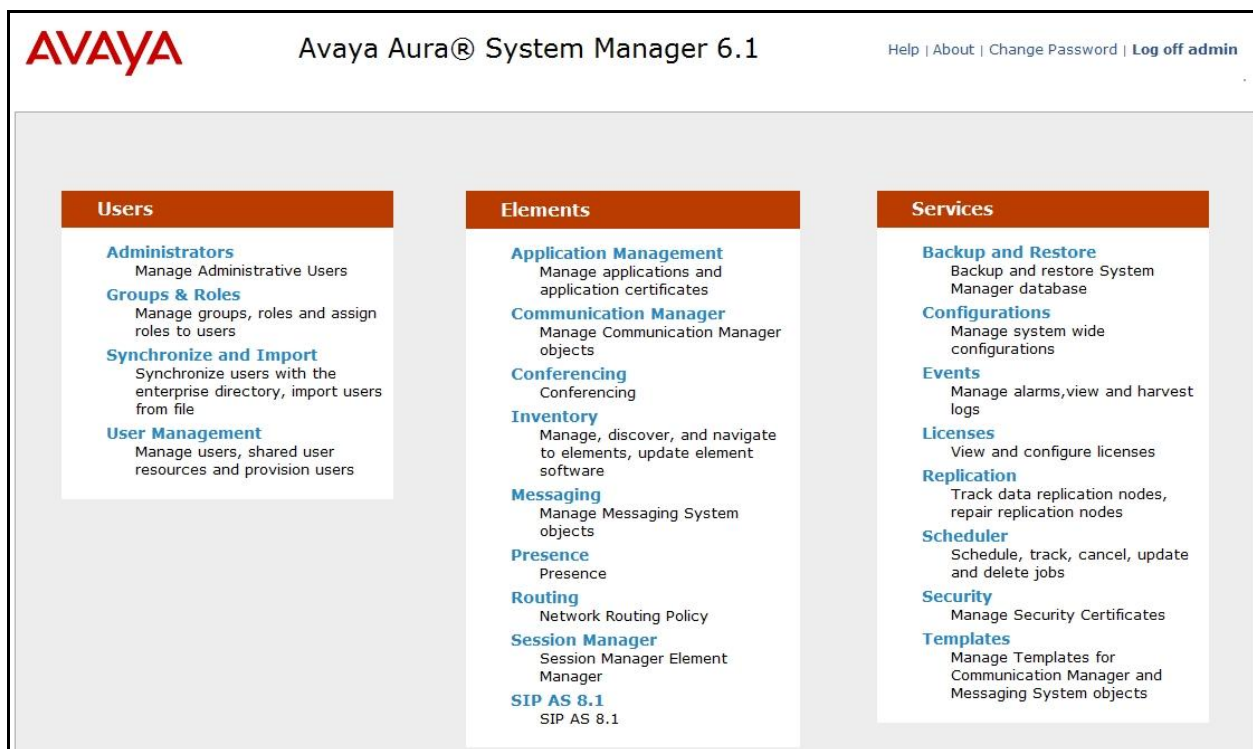
- SIP domain

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

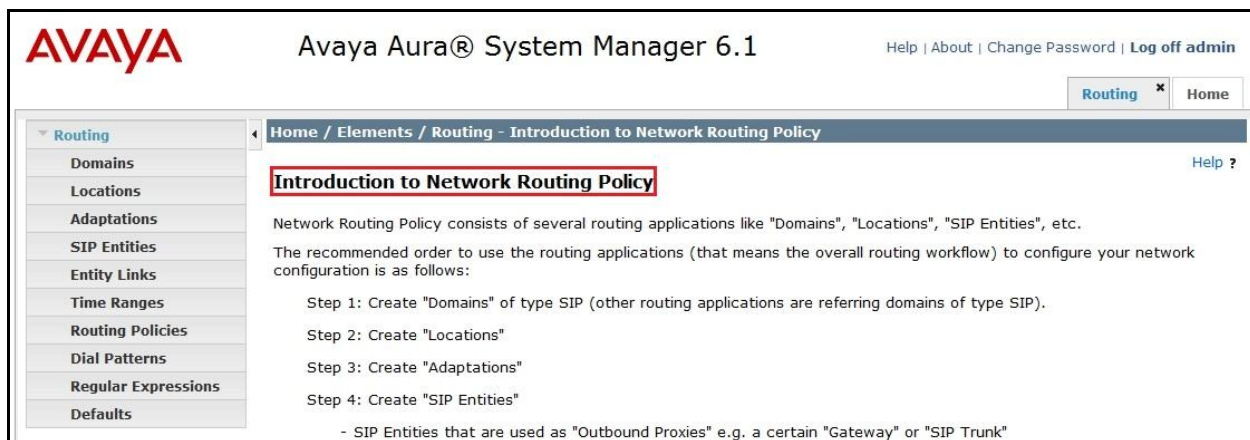
It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session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

6.1. System Manager Login and Navigation

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



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

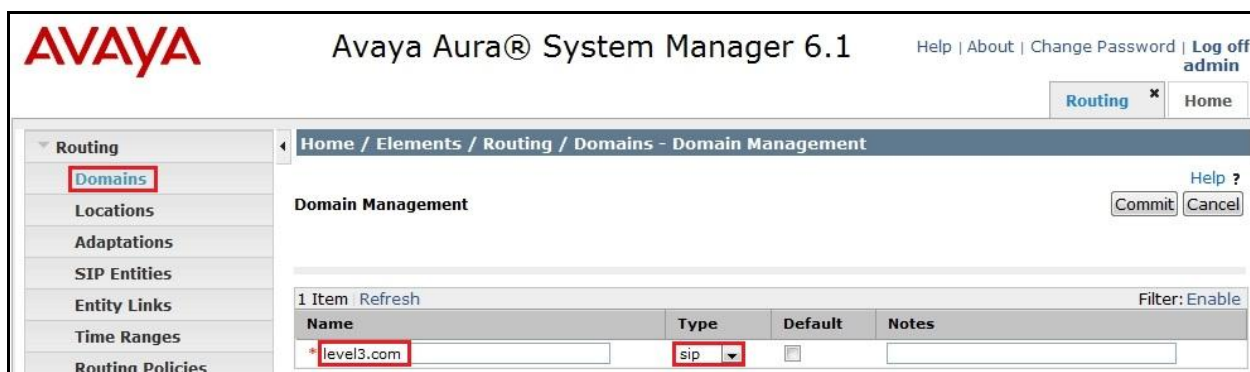


The navigation tree displayed in the left pane will be referenced in subsequent sections to navigate to items requiring configuration.

6.2. Specify SIP Domain

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

The following screenshot shows domain **level3.com** is already created. It is used for communication among a number of Avaya systems and applications with SIP integration to Session Manager. The domain **level3.com** is not known to Level 3. Later, it will be adapted by the Acme SBC to an IP address based URI-Host to meet the requirements of Level 3.



6.3. Add Location

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

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

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

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

In the **Location Pattern** section, click **Add** and enter the following values:

- **IP Address Pattern:** Enter two subnets 110.10.97.x and 110.10.98.x which are IP address patterns used to identify the location including the CS1000, Session Manager and the Acme SBC
- **Notes:** Add a brief description (optional)
- Click **Commit** button.

AVAYA Avaya Aura® System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

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

Home / Elements / Routing / Locations - Location Details

Location Details [Help ?](#) [Commit](#) [Cancel](#)

Call Admission Control has been set to ignore SDP. All calls will be counted using the Default Audio Bandwidth. See Session Manager -> Session Manager Administration -> Global Setting

General

* **Name:**

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units:

Total Bandwidth:

Per-Call Bandwidth Parameters

* **Default Audio Bandwidth:**

Location Pattern

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

6 Items [Refresh](#) [Filter: Enable](#)

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* <input type="text" value="110.10.97.*"/>	<input type="text"/>
<input type="checkbox"/>	* <input type="text" value="110.10.98.*"/>	<input type="text"/>

6.4. Add SIP Entities

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

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

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

- **Name:** Enter a descriptive name

- **FQDN or IP Address:** Enter the FQDN or IP address of the SIP Entity that is used for SIP signaling
- **Type:** Select **Session Manager** for Session Manager and select **Other** for CS1000 and Acme SBC
- **Location:** Select one of the locations defined previously in **Section 6.3**
- **Time Zone:** Select the time zone for the location above
- Click **Commit** button.

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

The screenshot displays the Avaya Aura System Manager 6.1 web interface. The left sidebar shows the navigation menu with 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and includes a 'General' section with the following fields: Name (DevASM), FQDN or IP Address (110.10.97.198), Type (Session Manager), Notes (For Session Manager), Location (Belleville), Outbound Proxy, Time Zone (America/Toronto), and Credential name. Below this is the 'SIP Link Monitoring' section with a dropdown set to 'Use Session Manager Configuration'. The 'Commit' button is highlighted with a red box.

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

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

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

Port				
<input type="button" value="Add"/> <input type="button" value="Remove"/>				
9 Items <input type="button" value="Refresh"/> Filter: Enable				
<input type="checkbox"/>	Port	Protocol	Default Domain	Notes
<input type="checkbox"/>	15060	TLS	bvwdev.com	
<input type="checkbox"/>	5060	UDP	bvwdev.com	
<input type="checkbox"/>	5060	TCP	level3.com	
<input type="checkbox"/>	5061	TLS	bvwdev.com	

The following screen shows the addition of the CS1000 in the **SIP Entities** section. In order for Session Manager to send SIP traffic on an entity link to the CS1000, it is necessary to create a SIP Entity. The **FQDN or IP Address** field is set to the Node IP address of the CS1000 (see **Section 5.2.1**). Select **Type** as **Other**.

AVAYA

Avaya Aura® System Manager 6.1

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

Routing
Home

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

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

SIP Entity Details

General

* Name: car2-ssg-level3

* FQDN or IP Address: 110.10.97.188

Type: Other

Notes: car2-ssg-level3

Adaptation:

Location: Belleville

Time Zone: America/New_York

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

The following screen shows the addition of the SIP Entity for the Acme SBC. The **FQDN or IP Address** field is set to the IP address of its private network interface (see **Figure 1**). Select **Type** as **Other**. SIP Link Monitoring is disabled to prevent OPTIONS from being sent by Session Manager to the Acme SBC, Session Manager will use ICMP ping to monitor status of the SIP Trunk instead.

AVAYA Avaya Aura® System Manager 6.1 [Help](#) | [About](#) | [Change Password](#) | [Log off admin](#)

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

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

SIP Entity Details [Help ?](#)

General

* Name: ACME

* FQDN or IP Address: 110.10.97.184

Type: Other

Notes: ACME PACKET 3800

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

SIP Link Monitoring

SIP Link Monitoring: Link Monitoring Disabled

Commit **Cancel**

6.5. Add Entity Links

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

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

- **Name:** Enter a descriptive name
- **SIP Entity 1:** Select the Session Manager
- **Protocol:** Select the transport protocol used for this link
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. For CS1000, this must match the port of **Proxy Server Route 1** which defined in **Section 5.5.2** step d)
- **SIP Entity 2:** Select the name of the other system. For CS1000 select the CS1000 SIP Entity; for the Acme SBC, select the Acme SBC SIP Entity. The SIP Entities are defined in **Section 6.4**
- **Port:** Port number on which the other system receives SIP requests from the Session Manager. For CS1000, this must match the **Local SIP Port** defined in **Section 5.5.2** step c)
- **Connection Policy:** Select **Trusted**. **Note:** If this is not selected, calls from the associated SIP Entity specified in **Section 6.4** will be denied
- Click **Commit** button to save

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

Entity Link to CS1000:

Entity Links

Add Remove

1 Item Refresh Filter: Enable

SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
DevASM	TCP	*5060	car2-ssg-level3	*5060	Trusted

Select : All, None

Entity Link to Acme SBC:

Entity Links

Add Remove

1 Item Refresh Filter: Enable

SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy
DevASM	UDP	*5060	ACME	*5060	Trusted

Select : All, None

6.6. Add Routing Policies

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

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

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

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

The following screens show the Routing Policies **Level3_To_CS1K** for the CS1000.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Routing Policies - Routing Policy Details

Routing Policy Details

Commit Cancel Help ?

General

* Name: Level3_To_CS1K

Disabled: ☐

Notes: Level3_To_CS1K

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
car2-ssg-level3	110.10.97.188	Other	car2-ssg-level3

The following screens show the Routing Policies **CS1K_To_Level3** for the Acme SBC.

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing * Home

Home / Elements / Routing / Routing Policies - Routing Policy Details

Routing Policy Details

Commit Cancel Help ?

General

* Name: CS1K_To_Level3

Disabled: ☐

Notes: CS1K_To_Level3

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
ACME	110.10.97.184	Other	ACME PACKET 3800

6.7. Add Dial Patterns

Dial Patterns are needed to route specific calls through Session Manager. For the compliance test, dial patterns are needed to route calls from CS1000 to Level 3 and vice versa. Dial Patterns define which route policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing → Dial Patterns** in the left navigation pane and click on the **New** button in the right pane (not shown). Fill in the following, as shown in the screens below:

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

- **Pattern:** Enter a dial string that will be matched against the Request-URI of the call

- **Min:** Enter a minimum length used in the match criteria
- **Max:** Enter a maximum length used in the match criteria
- **SIP Domain:** Enter the destination domain used in the match criteria
- **Notes:** Add a brief description (optional)

In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria. Lastly, select the routing policy from the list that will be used to route all calls that match the specified criteria. Click **Select**.

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

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

The first example in the screen below shows dial pattern for outbound 11-digit numbers. The dialed number starts with prefix 1 and has a destination domain of *level3.com* and uses route policy **CS1K_To_Level3** as defined in **Section 6.6**. The dial patterns for outbound calls that start with prefix 0 or 411 are configured similarly to this dial pattern.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The left sidebar contains a navigation menu with options: Routing, Domains, Locations, Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns (highlighted), Regular Expressions, and Defaults. The main content area is titled 'Dial Pattern Details' and includes a 'General' section with the following fields: Pattern (1), Min (11), Max (11), Emergency Call (unchecked), SIP Domain (level3.com), and Notes. At the bottom, there is a table titled 'Originating Locations and Routing Policies' with columns: Add, Remove, 1 Item, Refresh, Filter: Enable, Originating Location Name, Originating Location Notes, Routing Policy Name, Rank, Routing Policy Disabled, Routing Policy Destination, and Routing Policy Notes. The table contains one entry: Belleville, Belleville DevConnect lab, CS1K_To_Level3, 0, unchecked, ACME, CS1K_To_Level3.

Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
Belleville	Belleville DevConnect lab	CS1K_To_Level3	0	<input type="checkbox"/>	ACME	CS1K_To_Level3

The second example in the screen below shows dial pattern for inbound 10-digit numbers. The dialed number starts with prefix **716261** to domain **level3.com** and uses route policy **Level3_To_CS1000** as defined in **Section 6.6**. These are the DID numbers assigned to the enterprise by Level 3.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The left navigation pane has 'Dial Patterns' highlighted. The main area is titled 'Dial Pattern Details' and contains a 'General' tab. The following fields are visible and highlighted with red boxes: Pattern (716261), Min (10), Max (10), SIP Domain (level3.com), and a table of Originating Locations and Routing Policies. The table has one item: Belleville, with Originating Location Notes (Belleville DevConnect lab), Routing Policy Name (Level3_To_CS1K), Rank (0), Routing Policy Disabled (unchecked), Routing Policy Destination (car2-ssg-level3), and Routing Policy Notes (Level3_To_CS1K).

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing x Home

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

Dial Pattern Details

Help ?

Commit Cancel

General

* Pattern: 716261

* Min: 10

* Max: 10

Emergency Call: ☐

SIP Domain: level3.com

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh

	Originating Location Name 1	Originating Location Notes	Routing Policy Name	Rank 2	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	Belleville	Belleville DevConnect lab	Level3_To_CS1K	0	<input type="checkbox"/>	car2-ssg-level3	Level3_To_CS1K

6.8. Add/View Session Manager

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

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

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

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

AVAYA Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Session Manager x Routing x Home

Session Manager

Home / Elements / Session Manager - Session Manager

Help ?

Edit Session Manager Commit Cancel

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

General

SIP Entity Name

Description

*Management Access Point Host Name/IP

*Direct Routing to Endpoints

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

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

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

Security Module

SIP Entity IP Address

*Network Mask

*Default Gateway

*Call Control PHB

*QOS Priority

*Speed & Duplex

VLAN ID

7. Configure Acme Packet Net-Net 3800 Session Border Controller

This section describes the configuration of the Acme Packet Session Border Controller (SBC) necessary for interoperability with Avaya SIP-enabled enterprise solution and Level 3 SIP Trunking Service. The SBC is configured via the Acme Packet Command Line Interface (ACLI).

This section will not attempt to describe each component in its entirety, but instead will highlight fields in each component which relates to the functionality in these Application Notes. The remaining fields are generally the default/standard value pre-defined by the SBC.

In the compliance test, according to the recommended configuration in **Figure 1**, the enterprise network resides on the inside and the service provider resides on the outside of the SBC.

7.1. Acme Packet Command Line Interface

The SBC is configured using the ACLI. The following are the generic ACLI steps for configuring various elements.

1. Access to the console port of the SBC using a PC and a terminal emulation program such as HyperTerminal (use the RJ-45 to DB9 adapter as packaged with the SBC for cable connection).

Use the following settings for the serial port on the PC.

- Bits per second: 115200
- Data bits: 8
- Parity: None
- Stop bits: 1
- Flow control: None

2. Log into the SBC with the proper user password.
3. Enable the super user mode by entering **enable** command with a proper super user password. The command prompt will change to include a “#” instead of a “>” while in super user mode. This level of system access (i.e. at the “acmesystem#” prompt) will be referred to as the *main* level of the ACLI.
4. In super user mode, enter **configure terminal** command to access the system level where all operating and system elements may be configured. This level of system access will be referred to as the *configuration* level.
5. Enter the name of an element to be configured (e.g., **system**).
6. Enter the name of a sub-element, if any (e.g., **phy-interface**).
7. Enter the name of an element parameter followed by its value (e.g., **name INSIDE**).
8. Enter **done** to save changes to the element. Use of the **done** command causes the system to save and display the settings for the current element.
9. Enter **exit** as many times as necessary to return to the configuration level.
10. Repeat **Steps 5 - 9** to configure all other elements.
11. Enter **exit** to return to the main level.
12. Type **verify** to verify the configuration.
13. Type **save-config** to save the configuration.
14. Type **activate-config** to activate the configuration.

After accessing different levels of the ACLI to configure elements and parameters, it is necessary to return to the main level in order to run certain tasks such as saving the configuration, activating the configuration, and rebooting the system.

Note: Acme Packet Net-Net 3800 SBC provisioning applicable to the reference configuration is shown in **bold** text. Other parameters and setting are shown for informational purposes.

7.2. Physical and Network Interfaces

As part of the compliance test, the Ethernet interface of slot 1/port 0 of the SBC as shown below. It connects to the external public internet which is an un-trusted network.

phy-interface		
name	OUTSIDE	
operation-type	Media	
port	0	
slot	1	
virtual-mac		
admin-state	enabled	
auto-negotiation	enabled	
duplex-mode	FULL	
speed	100	
overload-protection	disabled	

The Ethernet interface slot 0/port 0 is connected to the internal corporate LAN as shown in the screen below:

phy-interface		
name	INSIDE	
operation-type	Media	
port	0	
slot	0	
virtual-mac		
admin-state	enabled	
auto-negotiation	enabled	
duplex-mode	FULL	
speed	100	
overload-protection	disabled	

Define a logical network interface for each physical interface to assign it a routable IP address. As described in **Figure 1**, the network interface below defines the IP addresses on the physical interface INSIDE which connects to the enterprise network.

network-interface		
name	INSIDE	
sub-port-id	0	
description		
hostname		
ip-address	110.10.97.184	
pri-utility-addr		
sec-utility-addr		
netmask	255.255.255.192	
gateway	110.10.97.129	
sec-gateway		
gw-heartbeat		
state	disabled	
heartbeat	0	
retry-count	0	
retry-timeout	1	
health-score	0	

```

dns-ip-primary
dns-ip-backup1
dns-ip-backup2
dns-domain
dns-timeout                11
hip-ip-list                110.10.97.184
ftp-address
icmp-address              110.10.97.184
snmp-address
telnet-address

```

The network interface below defines the IP addresses on physical interface OUTSIDE which connects to Level 3.

```

network-interface
  name                                OUTSIDE
  sub-port-id                          0
  description
  hostname
  ip-address                          110.10.98.98
  pri-utility-addr
  sec-utility-addr
  netmask                             255.255.255.224
  gateway                             110.10.98.97
  sec-gateway
  gw-heartbeat
    state                             disabled
    heartbeat                          0
    retry-count                        0
    retry-timeout                      1
    health-score                       0
  dns-ip-primary
  dns-ip-backup1
  dns-ip-backup2
  dns-domain
  dns-timeout                          11
  hip-ip-list                          110.10.98.98
  ftp-address
  icmp-address                         110.10.98.98
  snmp-address

```

7.3. Realm

A realm represents a group of related SBC components.

For the compliance test, two realms are created. The realm name INSIDE represents the internal network which contains the elements configured for the enterprise.

```

realm-config
  identifier                        INSIDE
  description
  addr-prefix                        0.0.0.0
  network-interfaces
    INSIDE:0
<Text removed for brevity>

```


The realm name OUTSIDE represents the external network which contains the elements configured for Level 3

```
realm-config
  identifier                OUTSIDE
  description
  addr-prefix                0.0.0.0
  network-interfaces
                                OUTSIDE:0
<Text removed for brevity>
```

7.4. Session Agent

A session agent defines the characteristics of signaling from a peer gateway endpoint such as Session Manager (as known as Call Server) or Level 3 (as known as Trunk Server).

The **session agent** in the screen below represents the configuration for Level 3. As described in **Figure 1**, the IP interface of Level 3 SIP Trunking Service is defined with transport protocol is UDP and port 5070.

- Set **state** to **enabled**
- Set **app-protocol** to **SIP**
- Set **realm-id** to **OUTSIDE**
- Set **in-manipulationid** to **Level3_To_CS1K**. This profile is defined in the SIP Header Manipulation Section as discussed later in **Section 7.7**. It is a set of rules to manipulate the SIP signaling for an inbound call from Level 3 such as to normalize the From, To, Request-URI headers etc. known to the CS1000.
- Set **out-manipulationid** to **CS1K_To_Level3**. This profile is defined in the SIP Header Manipulation Section as discussed later in **Section 7.7**. It is a set of rules to manipulate the SIP signaling for an outbound call to Level 3 such as to normalize the From, To, Request-URI headers etc. known to Level 3.

```
session-agent
  hostname                220.20.35.91
  ip-address              220.20.35.91
  port                    5070
  state                  enabled
  app-protocol            SIP
  app-type
  transport-method        UDP
  realm-id                OUTSIDE
  egress-realm-id
  description             CS1K_To_Level3
    <Text removed for brevity>

  ping-method
  ping-interval
    <Text removed for brevity>

  in-manipulationid       Level3_To_CS1K
  out-manipulationid      CS1K_To_Level3
    <Text removed for brevity>
```

The **session agent** in the screen below represents the configuration for Session Manager. As described in **Figure 1**, the IP interface of Session Manager is defined with transport protocol is TCP and port 5060.

- Set **state** to **enabled**
- Set **app-protocol** to **SIP**
- Set **realm-id** to **INSIDE**

Note: the **in-manipulationid** and **out-manipulationid** are kept default which is blank. It means there is no signaling manipulation performed on the SIP traffic toward the CS1000. The manipulation is already applied to the Trunk Server side.

```
session-agent
  hostname                110.10.97.198
  ip-address              110.10.97.198
  port                    5060
  state                   enabled
  app-protocol            SIP
  app-type
  transport-method        DynamicTCP
  realm-id                INSIDE
  egress-realm-id
  description             Level3_To_CS1K
  <Text removed for brevity>
```

7.5. SIP Configuration

The SIP configuration (*sip-config*) defines the global system-wide SIP parameters.

Configure the sip-config as show in the screen below:

- Set the **state** to **enabled** to allow SIP call to be processed by the SBC
- Set **home-realm-id** to **INSIDE**
- Set **egress-realm-id** to **OUTSIDE**

```
sip-config
  state                   enabled
  operation-mode          dialog
  dialog-transparency     enabled
  home-realm-id           INSIDE
  egress-realm-id         OUTSIDE
  nat-mode                None
  <Text removed for brevity>
```

7.6. SIP Interface

SIP interface (*sip-interface*) enables the SIP application protocol on a particular network interface.

Two SIP interfaces are defined for this compliance test. The SIP interface as shown below is used by the SBC to listen to the enterprise SIP traffic from realm INSIDE. The SBC is configured to listen on network interface 110.10.97.184, transport protocol TCP and port 5060.

```
sip-interface
```

```

state                enabled
realm-id             INSIDE
description
sip-port
    address           110.10.97.184
    port              5060
    transport-protocol TCP
<Text removed for brevity>

```

The SIP interface shown below is used by the SBC to listen to SIP traffic from the realm OUTSIDE defined for Level 3. The SBC is configured to listen on network interface 110.10.98.98, transport protocol UDP and port 5060.

```

sip-interface
state                enabled
realm-id             OUTSIDE
description
sip-port
    address           110.10.98.98
    port              5060
    transport-protocol UDP
<Text removed for brevity>

```

7.7. SIP Manipulation

SIP Header Manipulation Rules (HMR) are used to modify the SIP messages (if necessary) for interoperability between the CS1000 and Level 3.

In the compliance test, Level 3 requires the SIP signaling from the enterprise to meet its specification. For that purpose, HMRs are created for Session Agent which are defined for Level 3 in **Section 7.4**.

The HMR **CS1K_To_Level3** is added as shown in the screen below to apply to SIP messages from the CS1000 toward Level 3. It contains rules to perform the following:

- Header rule **manipRURI** replaces the private enterprise SIP domain in the Request-URI header by \$REMOTE_IP (.e.g. 220.20.35.91) which is the IP address assigned by Level 3.
- Header rule **manipTo** replaces the private enterprise SIP domain in the To header by \$REMOTE_IP (.e.g. 220.20.35.91) which is the IP address assigned by Level 3.
- Header rule **manipFrom** replaces the private enterprise SIP domain in the From header by \$LOCAL_IP (.e.g. 110.10.98.98) which is the public IP address of the Acme SBC.
- Header rule **manipPAI** replaces the private enterprise SIP domain in the P-Asserted-Identity (PAI) header by \$LOCAL_IP (.e.g. 110.10.98.98) which is the public IP address of Acme SBC.
- Level 3 requires Diversion header for call forward scenarios as it does not support History-Info header. Therefore, a header rule **HistoryInfoRegex** was created to check if the History-Info header has a specific “reason code” to match the condition of off-net call forward scenarios. If a positive match happens, **AddDiversion1**, **AddDiversion2** and **AddDiversion3** will construct a Diversion header appropriate to call forward all call, busy and no answers

- Header rule **storePAI** stores calling party number in the PAI header which will be used to construct a Remote-Party-ID header.
- Header rule **chkPrivacy** checks the **Privacy** header for a private call. This condition will be used by header rules **addRPID1**, **addRPID2** and **addRPID3** to construct the Remote-Party-ID from the PAI header value which is stored in the **storePAI** rule. This modification is to meet a requirement of Level 3 with respect to the SIP Trunk because Level 3 uses Remote-Party-ID header as an alternative to a PAI header.
- Header rule **delete_PAI** deletes the PAI header not required by Level 3.
- Header rule **delete_mcdn** deletes the mcdn body parts which are proprietary to the CS1000 and not required by Level 3.
- Header rule **delete_x_nt_e164_clid** deletes the X-nt-e164-clid header which is proprietary to the CS1000 and not required by Level 3.
- Header rule **delete_Alert_Info** deletes the Alert_Info header which is proprietary to the CS1000 and not required by Level 3.
- Header rule **delete_P_Location** deletes the P_Location header that is proprietary to Avaya and not required by Level 3.
- Header rule **delete_History_Info** deletes the History-Info header not required by Level 3.
- Header rule **delete_Route** deletes Route headers not required by Level 3.

```

sip-manipulation
  name          CS1K_To_Level3
  description    CS1K_To_Level3
  split-headers
  join-headers
  header-rule
    name          manipRURI
    header-name    request-uri
    action          manipulate
    comparison-type case-sensitive
    msg-type        request
    methods          INVITE,UPDATE
    match-value
    new-value
    element-rule
      name          modURIHost
      parameter-name
      type          uri-host
      action          replace
      match-val-type any
      comparison-type case-sensitive
      match-value
      new-value      $REMOTE_IP
  header-rule
    name          manipTo
    header-name    To
    action          manipulate
    comparison-type case-sensitive
    msg-type        request
    methods          INVITE
    match-value
    new-value
    element-rule
      name          modTo
      parameter-name

```

	type	uri-host
	action	replace
	match-val-type	any
	comparison-type	case-sensitive
	match-value	
	new-value	\$REMOTE_IP
header-rule		
name		manipFrom
header-name		From
action		manipulate
comparison-type		case-sensitive
msg-type		request
methods		INVITE
match-value		
new-value		
element-rule		
name		modFrom
parameter-name		
type		uri-host
action		replace
match-val-type		any
comparison-type		case-sensitive
match-value		
new-value		\$LOCAL_IP
header-rule		
name		manipPAI
header-name		P-Asserted-Identity
action		manipulate
comparison-type		case-sensitive
msg-type		any
methods		INVITE
match-value		
new-value		
element-rule		
name		modPAI
parameter-name		
type		uri-host
action		replace
match-val-type		any
comparison-type		case-sensitive
match-value		
new-value		\$LOCAL_IP
header-rule		
name		HistoryInfoRegex
header-name		History-Info
action		store
comparison-type		pattern-rule
msg-type		any
methods		
match-value		()
new-value		
element-rule		
name		GetUser
parameter-name		
type		uri-user
action		store
match-val-type		any
comparison-type		pattern-rule
match-value		
new-value		

```

        element-rule
            name
                GetHost
            parameter-name
            type
                uri-host
            action
                store
            match-val-type
                any
            comparison-type
                pattern-rule
            match-value
            new-value

        element-rule
            name
                GetUserReason1
            parameter-name
            type
                header-value
            action
                store
            match-val-type
                any
            comparison-type
                pattern-rule
            match-value
                (.*) (Moved) (.*)
            new-value

        element-rule
            name
                GetUserReason2
            parameter-name
            type
                header-value
            action
                store
            match-val-type
                any
            comparison-type
                pattern-rule
            match-value
                (.*) (Busy) (.*)
            new-value

        element-rule
            name
                GetUserReason3
            parameter-name
            type
                header-value
            action
                store
            match-val-type
                any
            comparison-type
                pattern-rule
            match-value
                (.*) (Unavailable) (.*)
            new-value

    header-rule
        name
            AddDiversion1
        header-name
            Diversion
        action
            add
        comparison-type
            boolean
        msg-type
            any
        methods
        match-value
            $HistoryInfoRegex[0].$GetUserReason1
        new-value
<sip:+$HistoryInfoRegex[0].$GetUser.$0+@$HistoryInfoRegex[0].$GetHost.$0+>;reason=unc
onditional;screen=no
        header-rule
            name
                AddDiverion2
            header-name
                Diversion
            action
                add
            comparison-type
                boolean
            msg-type
                any
            methods
            match-value
                $HistoryInfoRegex[0].$GetUserReason2
            new-value
<sip:+$HistoryInfoRegex[0].$GetUser.$0+@$HistoryInfoRegex[0].$GetHost.$0+>;reason=use
r\~busy;screen=no
            header-rule
                name
                    AddDiversion3
                header-name
                    Diversion
                action
                    add

```


comparison-type	boolean
msg-type	any
methods	
match-value	\$HistoryInfoRegex[0].\$GetUserReason3
new-value	
<sip:+\$HistoryInfoRegex[0].\$GetUser.\$0+@\$HistoryInfoRegex[0].\$GetHost.\$0+>;reason=no\	
-answer;screen=no	
header-rule	
name	chkPrivacy
header-name	Privacy
action	store
comparison-type	pattern-rule
msg-type	any
methods	
match-value	
new-value	
element-rule	
name	privacyNone
parameter-name	
type	header-value
action	store
match-val-type	any
comparison-type	pattern-rule
match-value	^none\$
new-value	
element-rule	
name	privacyID
parameter-name	
type	header-value
action	store
match-val-type	any
comparison-type	pattern-rule
match-value	^id\$
new-value	
element-rule	
name	privacyUser
parameter-name	
type	header-value
action	store
match-val-type	any
comparison-type	pattern-rule
match-value	^user\$
new-value	
element-rule	
name	privacyIDUser
parameter-name	
type	header-value
action	store
match-val-type	any
comparison-type	pattern-rule
match-value	^id;user\$
new-value	
header-rule	
name	storePAI
header-name	P-Asserted-Identity
action	store
comparison-type	case-sensitive
msg-type	any
methods	
match-value	
new-value	

```

        element-rule
            name                                storeHeader
            parameter-name
            type                                header-value
            action                              store
            match-val-type                      any
            comparison-type                     case-sensitive
            match-value
            new-value

    header-rule
        name                                addRPID1
        header-name                        Remote-Party-ID
        action                              add
        comparison-type                     boolean
        msg-type                            any
        methods
        match-value                        $checkPrivacy[0].$privacyNone
        new-value
$storePAI[0].$storeHeader.$0+";screen=no;privacy=off"
    header-rule
        name                                addRPID2
        header-name                        Remote-Party-ID
        action                              add
        comparison-type                     boolean
        msg-type                            any
        methods
        match-value                        $checkPrivacy[0].$privacyID
        new-value
$storePAI[0].$storeHeader.$0+";screen=no;privacy=on"
    header-rule
        name                                addRPID3
        header-name                        Remote-Party-ID
        action                              add
        comparison-type                     boolean
        msg-type                            any
        methods
        match-value                        $checkPrivacy[0].$privacyUser
        new-value
$storePAI[0].$storeHeader.$0+";screen=no;privacy=on"
    header-rule
        name                                addRPID4
        header-name                        Remote-Party-ID
        action                              add
        comparison-type                     case-sensitive
        msg-type                            any
        methods
        match-value                        $checkPrivacy[0].$privacyIDUser
        new-value
$storePAI[0].$storeHeader.$0+";screen=no;privacy=on"
    header-rule
        name                                delete_PAI
        header-name                        P-Asserted-Identity
        action                              delete
        comparison-type                     case-sensitive
        msg-type                            any
        methods
        match-value
        new-value
    header-rule
        name                                delete_mcdn
        header-name                        Content-Type
        action                              manipulate

```

comparison-type	case-sensitive
msg-type	any
methods	
match-value	
new-value	
element-rule	
name	delete_nt_epid
parameter-name	application/x-nt-epid-frag-hex
type	mime
action	delete-element
match-val-type	any
comparison-type	case-sensitive
match-value	
new-value	
element-rule	
name	delete_nt_mcdn
parameter-name	application/x-nt-mcdn-frag-hex
type	mime
action	delete-element
match-val-type	any
comparison-type	case-sensitive
match-value	
new-value	
header-rule	
name	delete_x_nt_el64_clid
header-name	X-nt-el64-clid
action	delete
comparison-type	case-sensitive
msg-type	any
methods	
match-value	
new-value	
header-rule	
name	delete_Alert_Info
header-name	Alert_info
action	delete
comparison-type	case-sensitive
msg-type	any
methods	
match-value	
new-value	
header-rule	
name	delete_P_Location
header-name	P-Location
action	delete
comparison-type	case-sensitive
msg-type	any
methods	
match-value	
new-value	
header-rule	
name	delete_History_Info
header-name	History-Info
action	delete
comparison-type	case-sensitive
msg-type	any
methods	
match-value	
new-value	
header-rule	
name	del_Route
header-name	Route

action	delete
comparison-type	case-sensitive
msg-type	any
methods	
match-value	
new-value	

The HMR **Level3_To_CS1K** in the screen below is created for the Session Agent which is defined for Level 3 in **Section 7.4**. The HMR is applied to SIP messages from Level 3 toward the CS1000. It contains rules to perform the following:

- Header rule **manipRURI** replaces the IP address in the Request-URI header with the domain name **level3.com** expected by the CS1000.
- Header rule **manipTo** replaces the IP address in the To header with the domain name **level3.com** expected by the CS1000.
- Header rule **manipFrom** replaces the IP address in the From header with the domain name **level3.com** expected by the CS1000.
- Header rule **manipAllow** removes UPDATE from the Allow header. This prevents the CS1000 from using UPDATE on the SIP Trunk. This implementation is to support blind transfer off-net scenario when Level 3 does not fully support the UPDATE method. For detail information, please refer to **Section 2.2**, observation #02.

sip-manipulation	
name	Level3_To_CS1K
description	Level3_To_CS1K
split-headers	
join-headers	
header-rule	
name	manipRURI
header-name	request-uri
action	manipulate
comparison-type	case-sensitive
msg-type	any
methods	
match-value	
new-value	
element-rule	
name	modRURI
parameter-name	
type	uri-host
action	replace
match-val-type	any
comparison-type	case-sensitive
match-value	
new-value	level3.com
header-rule	
name	manipTo
header-name	To
action	manipulate
comparison-type	case-sensitive
msg-type	any
methods	
match-value	
new-value	
element-rule	
name	To
parameter-name	

	type	uri-host
	action	replace
	match-val-type	any
	comparison-type	case-sensitive
	match-value	
	new-value	level3.com
header-rule		
	name	manipFrom
	header-name	From
	action	manipulate
	comparison-type	case-sensitive
	msg-type	any
	methods	
	match-value	
	new-value	
	element-rule	
	name	From
	parameter-name	
	type	uri-host
	action	replace
	match-val-type	any
	comparison-type	case-sensitive
	match-value	
	new-value	level3.com
header-rule		
	name	manipAllow
	header-name	Allow
	action	manipulate
	comparison-type	case-sensitive
	msg-type	any
	methods	
	match-value	
	new-value	\$ORIGINAL-", UPDATE"

7.8. Steering Pools

Steering pools define the range of ports to be used for RTP.

For the compliance test, separate steering pools are defined for each realm.

The key steering pool (*steering-pool*) fields are:

- **ip-address:** The network interface will be used to transmit or receive the RTP.
- **start-port:** An number that begins the port range for RTP.
- **end-port:** An number that ends the port range for RTP.
- **realm-id:** The realm to which steering pool is assigne.

The screen below is the steering pool for **OUTSIDE** realm:

steering-pool	
ip-address	110.10.98.98
start-port	20000
end-port	40000
realm-id	OUTSIDE
<Text removed for brevity>	

The screen below is the steering pool for **INSIDE** realm:

```
steering-pool
  ip-address      10.10.97.184
  start-port      20000
  end-port        40000
  realm-id        INSIDE
<Text removed for brevity>
```

7.9. Local Policy

The local policies govern the routing of a call from the enterprise to the service provider and vice versa.

Two local policies are created for the compliance test.

For inbound calls, the local-policy allows all calls from source realm **OUTSIDE** to pass through the Acme SBC.

To activate the local-policy, set the **state** to **enabled**

The policy-attribute is defined as follows:

- Set **from-address** to * (an asterisk character)
- Set **to-address** to * (an asterisk character)
- Set the **next-hop** to the IP address of Session Manager
- Set the **realm** to **INSIDE**
- Set the **app-protocol** to **SIP**
- Set the **state** to **enabled**

```
local-policy
  from-address      *
  to-address        *
  source-realm      OUTSIDE
  description        Level3_To_CS1K
  activate-time      N/A
  deactivate-time    N/A
  state              enabled
  policy-priority    none
<Text removed for brevity>
  policy-attribute
    next-hop        110.10.97.198
    realm            INSIDE
    action           none
    terminate-recursion disabled
    carrier
    start-time       0000
    end-time         2400
    days-of-week     U-S
    cost             0
    app-protocol     SIP
    state            enabled
```



```
methods
<Text removed for brevity>
```

For outbound calls, the local-policy allows all calls from source realm **INSIDE** to any PSTN destination to pass through the Acme SBC.

To activate the local-policy, set the **state** to **enabled**

The policy-attribute is defined as follows:

- Set **from-address** to * (an asterisk character)
- Set **to-address** to * (an asterisk character)
- Set the **next-hop** to the IP address of the Level 3 SIP Trunking Service
- Set the **realm** to **OUTSIDE**
- Set the **app-protocol** to **SIP**
- Set the **state** to **enabled**

```
local-policy
  from-address
                                *
  to-address
                                *
  source-realm
                                INSIDE
  description
  activate-time
                                N/A
  deactivate-time
                                N/A
  state
                                enabled
  policy-priority
                                none
  <Text removed for brevity>
  policy-attribute
    next-hop
                                220.10.35.91
    realm
                                OUTSIDE
    action
                                none
    terminate-recursion
                                disabled
    carrier
    start-time
                                0000
    end-time
                                2400
    days-of-week
                                U-S
    cost
                                0
    app-protocol
                                SIP
    state
                                enabled
    methods
  <Text removed for brevity>
```

8. Level 3 SIP Trunking Service Configuration

Level 3 is responsible for the configuration of its SIP Trunking Service. The customer will need to provide the IP address used to reach the Acme SBC at enterprise side. Level 3 will provide the customer with the necessary information to configure the SIP connection from the enterprise to Level 3. The information provided by Level 3 includes:

- IP address of the Level 3 Session Border Controller

- Level 3 SIP domain. In the compliance test, Level 3 preferred to use an IP address as a URI-Host
- Enterprise SIP domain. In the compliance test, Level 3 preferred to use the IP address of the Acme SBC as a URI-Host
- Supported codecs
- DID numbers
- IP addresses and port numbers used for signaling or media through any security devices
- Digest Authentication information

The sample configuration between Level 3 and the enterprise for the compliance test is a static configuration. There is no registration on the SIP trunk implemented on either Level 3 or enterprise side.

9. Verification and Troubleshooting

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

9.1. Verification Steps

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

9.2. Protocol Traces:

The following SIP headers are inspected using Wireshark traces:

- Request-URI: verify the request number and SIP domain
- From: verify the display name and display number

- To: verify the display name and display number
- Remote-Party-ID: verify the display name and display number
- Privacy: verify privacy masking with “user, id”
- Diversion: verify DID number
- Authorization: verify Digest Authentication

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

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

9.3. Troubleshooting:

9.3.1.1 Acme SBC

Using a network sniffing tool (e.g., Wireshark) to monitor the SIP signaling messages between Level 3 and Acme SBC

The following is an example inbound call from Level 3 to the CS1000.

- Inbound INVITE request from Level 3:

```
INVITE sip:7162611205@110.10.98.98:5060 SIP/2.0
Via: SIP/2.0/UDP 220.20.35.91:5070;branch=z9hG4bKdhms3h30a0o04kkv46c1.1
From: <sip:6139675258@220.20.35.91;user=phone>;tag=SDcsife01-334911229-1317654395748-
To: "AVAYA ."<sip:7162611205@110.10.98.98>
Call-ID: SDcsife01-31188195e95bd3226c681c5c96ba95e5-v3000i1
CSeq: 623459763 INVITE
Contact: <sip:6139675258@220.20.35.91:5070;transport=udp>
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY,UPDATE
Accept: multipart/mixed,application/media_control+xml,application/sdp
Supported:
Max-Forwards: 9
Content-Type: application/sdp
Content-Disposition: session;handling=required
Content-Length: 281

v=0
o=BroadWorks 4903705 1 IN IP4 220.20.35.91
s=-
c=IN IP4 220.20.35.91
t=0 0
m=audio 49264 RTP/AVP 0 8 18 101
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=sendrecv
a=maxptime:20
```

- 200OK/SDP response by the CS1000:

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 220.20.35.91:5070;branch=z9hG4bKdhms3h30a0o04kkv46c1.1
From: <sip:6139675258@220.20.35.91;user=phone>;tag=SDcsife01-334911229-1317654395748-
To: "AVAYA ."<sip:7162611205@110.10.98.98>;tag=633f438-bc610a87-13c4-55013-3f78d-45e32a84-3f78d
Call-ID: SDcsife01-31188195e95bd3226c681c5c96ba95e5-v3000i1
CSeq: 623459763 INVITE
Supported: 100rel,x-nortel-sipvc,replaces
User-Agent: Nortel CS1000 SIP GW release_7.0 version_ssLinux-7.50.17
Privacy: none
Contact: <sip:7162611205@110.10.98.98:5060;user=phone;transport=udp>
Allow:
INVITE,ACK,BYE,REGISTER,REFER,NOTIFY,CANCEL,PRACK,OPTIONS,INFO,SUBSCRIBE,UPDATE
Content-Type: application/sdp
Content-Length: 271
Server: AVAYA-SM-6.1.1.0.611023
Remote-Party-ID: "Level3 i1120"
<sip:7162611205@220.20.35.91;user=phone>;screen=no;privacy=off

v=0
o=- 26 1 IN IP4 110.10.98.98
s=-
c=IN IP4 110.10.98.98
t=0 0
m=audio 20346 RTP/AVP 18 101 111
c=IN IP4 110.10.98.98
a=maxptime:20
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=rtpmap:111 X-nt-inforeq/8000
a=ptime:20
a=sendrecv
```

The following is an example outbound call from the CS1000 to Level 3.

- Outbound INVITE request from CS1000:

```
INVITE sip:16139675279@220.20.35.91;user=phone SIP/2.0
Via: SIP/2.0/UDP 110.10.98.98:5060;branch=z9hG4bKjed9ef30dgh0ng0sv531.1
From: "Level3 i1120" <sip:7162611205@110.10.98.98;user=phone>;tag=633dbb8-bc610a87-13c4-55013-3f58c-111153c4-3f58c
To: <sip:16139675279@220.20.35.91;user=phone>
Call-ID: 7d6d638-bc610a87-13c4-55013-3f58c-38af4fc6-3f58c
CSeq: 1 INVITE
Supported: 100rel,x-nortel-sipvc,replaces
User-Agent: Nortel CS1000 SIP GW release_7.0 version_ssLinux-7.50.17 AVAYA-SM-6.1.1.0.611023
Privacy: none
Contact: <sip:7162611205@110.10.98.98:5060;user=phone;transport=udp>
Allow:
INVITE,ACK,BYE,REGISTER,REFER,NOTIFY,CANCEL,PRACK,OPTIONS,INFO,SUBSCRIBE,UPDATE
Content-Type: application/sdp
Content-Length: 260
```

```
Max-Forwards: 65
Remote-Party-ID: "Level3 i1120"
<sip:7162611205@220.20.35.91;user=phone>;screen=no;privacy=off

v=0
o=- 25 1 IN IP4 110.10.98.98
s=-
c=IN IP4 110.10.98.98
t=0 0
m=audio 20344 RTP/AVP 0 8 18 101 111
c=IN IP4 110.10.98.98
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=rtpmap:111 X-nt-inforeq/8000
a=ptime:20
a=sendrecv
```

- 401 challenge from Level 3 to request Digest Authentication:

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP 110.10.98.98:5060;branch=z9hG4bKjed9ef30dgh0ng0sv531.1
From: "Level3 i1120" <sip:7162611205@110.10.98.98;user=phone>;tag=633dbb8-
bc610a87-13c4-55013-3f58c-111153c4-3f58c
To: <sip:16139675279@220.20.35.91;user=phone>;tag=SDp9aae99-1806987150-
1317653882939
Call-ID: 7d6d638-bc610a87-13c4-55013-3f58c-38af4fc6-3f58c
CSeq: 1 INVITE
WWW-Authenticate: DIGEST
qop="auth", nonce="BroadWorksXgtbl3n0bT4egtd9BW", algorithm=MD5, realm="BroadWorks"
Content-Length:
```

- Re-INVITE from the CS1000 with Authorization header responds to Digest Authentication:

```
INVITE sip:16139675279@220.20.35.91;user=phone SIP/2.0
Via: SIP/2.0/UDP 110.10.98.98:5060;branch=z9hG4bKk6ka0o30eg4hng8th160.1
From: "Level3 i1120" <sip:7162611205@110.10.98.98;user=phone>;tag=633dbb8-
bc610a87-13c4-55013-3f58c-111153c4-3f58c
To: <sip:16139675279@220.20.35.91;user=phone>
Call-ID: 7d6d638-bc610a87-13c4-55013-3f58c-38af4fc6-3f58c
CSeq: 2 INVITE
Supported: 100rel,x-nortel-sipvc,replaces
User-Agent: Nortel CS1000 SIP GW release_7.0 version_ssLinux-7.50.17 AVAYA-SM-
6.1.1.0.611023
Privacy: none
Contact: <sip:7162611205@110.10.98.98:5060;user=phone;transport=udp>
Authorization: Digest username="1-23Q-
3413", realm="BroadWorks", nonce="BroadWorksXgtbl3n0bT4egtd9BW", uri="sip:16139675
279@level3.com;user=phone", response="d78a793bf7ec494cf17bcc6e21e3e366", algorith
m=MD5, cnonce="f772dc7", qop=auth, nc=00000001
Allow:
INVITE,ACK,BYE,REGISTER,REFER,NOTIFY,CANCEL,PRACK,OPTIONS,INFO,SUBSCRIBE,UPDATE
Content-Type: application/sdp
Content-Length: 260
Max-Forwards: 65
```

```
Remote-Party-ID: "Level3 i1120"
<sip:7162611205@220.20.35.91;user=phone>;screen=no;privacy=off

v=0
o=- 25 1 IN IP4 110.10.98.98
s=-
c=IN IP4 110.10.98.98
t=0 0
m=audio 20344 RTP/AVP 0 8 18 101 111
c=IN IP4 110.10.98.98
a=fmtp:18 annexb=no
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=rtpmap:111 X-nt-inforeq/8000
a=ptime:20
a=sendrecv
```

- 200OK/SDP response by Level 3:

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 110.10.98.98:5060;branch=z9hG4bKk6ka0o30eg4hng8th160.1
From: "Level3 i1120" <sip:7162611205@110.10.98.98;user=phone>;tag=633dbb8-
bc610a87-13c4-55013-3f58c-111153c4-3f58c
To: <sip:16139675279@220.20.35.91;user=phone>;tag=SDp9aae99-503571485-
1317653884615
Call-ID: 7d6d638-bc610a87-13c4-55013-3f58c-38af4fc6-3f58c
CSeq: 2 INVITE
Supported:
Contact: <sip:16139675279@220.20.35.91:5070;transport=udp>
Remote-Party-ID:
<sip:16139675279@8.13.220.254;user=phone>;screen=yes;party=called;privacy=off;id-
type=subscriber
Allow: ACK,BYE,CANCEL,INFO,INVITE,OPTIONS,PRACK,REFER,NOTIFY,UPDATE
Accept: multipart/mixed,application/media_control+xml,application/sdp
Content-Type: application/sdp
Content-Disposition: session;handling=required
Content-Length: 210

v=0
o=BroadWorks 4902809 1 IN IP4 220.20.35.91
s=-
c=IN IP4 220.20.35.91
t=0 0
m=audio 49262 RTP/AVP 0 101
a=rtpmap:0 PCMU/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=sendrecv
a=maxptime:20
```

9.3.1.2 CS1000 Verification Steps

a) Verify patch installation on CS1000

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

```

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

```

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

```

[admin@car2-sps ~]$ spstat
There is no SP in loaded status.
The last applied SP: Service_Pack_Linux_7.50_17_20120516.nt1
It is a STANDARD SP.
Has been applied by user nortel on Wed Jun 6 20:02:15 2012.
spins command completed with no errors detected.
[admin@car2-sps ~]$

```

b) Active Call Trace (LD 80)

The following is an example of one of the commands available on the CS1000 to trace the DN when the call is in progress. The call scenario involved the PSTN phone number 6139675258 calling 7162611205 on CS1000.

- Login to the Call Server CLI (please refer to **Section 5.1.2** for more detail)
- Login to the Overlay command prompt, issue the command **LD 80** and then **trace 5 1205**
- After the call is released, issue the command **trac 5 1205** again to see if the DN is released back to idle state

Below is the actual output of the Call Server Command Line mode when the 1205 is in-call state:

```

>ld 80
TRA000
.trac 5 1205

ACTIVE VTN 108 0 00 25

ORIG VTN 104 1 00 00 VTRK IPTI RMBR 105 1 INCOMING VOIP GW CALL
  FAR-END SIP SIGNALLING IP: 110.10.97.184
  FAR-END MEDIA ENDPOINT IP: 110.10.97.184 PORT: 21004
  FAR-END VendorID: AVAYA-SM-6.1.6.0.616008
TERM VTN 108 0 00 20 KEY 0 SCR MARP CUST 5 DN 1205 TYPE 1120
  SIGNALLING ENCRYPTION: INSEC
  MEDIA ENDPOINT IP: 110.10.98.141 PORT: 5200
MEDIA PROFILE: CODEC G.711 MU-LAW PAYLOAD 20 ms VAD OFF
RFC2833: RXPT 101 TXPT 101 DIAL DN 1205
MAIN_PM ESTD
TALKSLOT ORIG 76 TERM 49
EES_DATA:
NONE
QUEU NONE
CALL ID 0 34209

```



```
----- ISDN ISL CALL (ORIG) -----  
CALL REF # = 385  
BEARER CAP = VOICE  
HLC =  
CALL STATE = 10 ACTIVE  
CALLING NO = 6139675258 NUM_PLAN:UNKNOWN TON:UNKNOWN ESN:UNKNOWN  
CALLED NO = 7162611205 NUM_PLAN:UNKNOWN TON:UNKNOWN ESN:UNKNOWN
```

The following is an example after the call on 1205 is completed.

```
.trac 5 1205  
  
IDLE VTN 108 0 00 25 MARP
```

c) SIP Trunk monitoring (LD 32)

Place an inbound call from the PSTN (6139675258) to the CS1000 (7162611205). Then check the SIP Trunk status by using LD 32.

```
>ld 32  
NPR000  
.stat 104 1  
063 UNIT(S) IDLE  
001 UNIT(S) BUSY  
000 UNIT(S) DSBL  
000 UNIT(S) MBSY  
.
```

The following is an example after the call is completed; the BUSY trunk changes its state to IDLE.

```
.stat 104 1  
064 UNIT(S) IDLE  
000 UNIT(S) BUSY  
000 UNIT(S) DSBL  
000 UNIT(S) MBSY  
.
```

10. Conclusion

These Application Notes describe the configuration necessary to connect an Avaya Communication Server 1000 7.5, an Avaya Aura® Session Manager 6.1 and an Acme Packet Session Border Controller 6.2 to Level 3 SIP Trunking Service. Level 3 SIP Trunking Service is a SIP-based Voice over IP solution for customers ranging from small businesses to large enterprises. Level 3 SIP Trunking Service provides a flexible, cost-saving alternative to traditional analog and ISDN-PRI trunks.

All of the test cases have been executed. Despite the number of observations and limitations seen during testing as noted in **Section 2.2**, the test results met the objectives outlined in **Section 2.1**. The Level 3 SIP Trunking Service is considered **compliant** with Avaya Communication Server 1000 7.5, Avaya Aura® Session Manager 6.1 and Acme Packet Session Border Controller 6.2.

11. References

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

- [1] *Network Routing Service Fundamentals*, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-130, Revision 03.02, November 2010.
- [2] *IP Peer Networking Installation and Commissioning*, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-313, Revision: 05.02, November 2010.
- [3] *Communication Server 1000E Overview*, Avaya Communication Server 1000, Release 7.5, Document Number NN43041-110, Revision: 05.02, January 2011.
- [4] *Communication Server 1000 Unified Communications Management Common Services Fundamentals*, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-116, Revision 05.08, January 2011.
- [5] *Communication Server 1000 Dialing Plans Reference*, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-283, Revision 05.02, November 2010.
- [6] *Product Compatibility Reference*, Avaya Communication Server 1000, Release 7.5, Document Number NN43001-256, Revision 05.02, February 2011.
- [7] *Installing and Configuring Avaya Aura® System Platform*, Release 6.03, February 2011.
- [8] *Administering Avaya Aura® System Platform*, Release 6, June 2010.
- [9] *Installing and Upgrading Avaya Aura® System Manager*, Release 6.1, November 2010.
- [10] *Installing and Configuring Avaya Aura® Session Manager*, Release 6.1, April 2011, Number 03-603473.
- [11] *Administering Avaya Aura® Session Manager*, Release 6.1, May 2011, Document Number 03-603324.
- [12] *Acme Packet Net-Net® EMS User Guide*, Release Version 4.1.
- [13] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>
- [14] *RFC 3262, Reliability of Provisional Responses in the Session Initiation Protocol (SIP)* <http://www.ietf.org/>
- [15] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals*, <http://www.ietf.org/>

Product documentation for Level 3 SIP Trunking Service is available from Level 3.

©2012 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ® are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya DevConnect Program at devconnect@avaya.com.