



Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Communication Server 1000 R7.6, Avaya Aura® Session Manager R6.3 and Avaya Session Border Controller for Enterprise R6.3 to support Vodafone Libertel B.V. SIP Trunk Service - Issue 1.0

Abstract

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between Vodafone Libertel B.V. SIP Trunk Service and an Avaya SIP enabled enterprise solution.

The Avaya solution consists of Avaya Session Border Controller for Enterprise R6.3, Avaya Aura® Session Manager R6.3 and Avaya Communication Server 1000 R7.6. Vodafone Libertel B.V. is a member of the DevConnect Service Provider program.

Readers should pay attention to **Section 2**, in particular the scope of testing as outlined in **Section 2.1** as well as the observations noted in **Section 2.2**, to ensure that their own use cases are adequately covered by this scope and results.

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

Table of Contents

1.	Introduction.....	4
2.	General Test Approach and Test Results.....	4
2.1.	Interoperability Compliance Testing.....	5
2.2.	Test Results	5
2.3.	Support	6
3.	Reference Configuration	7
4.	Equipment and Software Validated	8
5.	Configure Avaya Communication Server 1000.....	9
5.1.	Logging into the Avaya Communication Server 1000.....	9
5.2.	Confirm System Features	10
5.3.	Configure Codecs for Voice and FAX operation.....	12
5.4.	Virtual Trunk Gateway Configuration	14
5.5.	Configure Bandwidth Zones	17
5.6.	Configure Incoming Digit Conversion Table	17
5.7.	Configure SIP Trunks.....	18
5.8.	Configure Analog, Digital and IP Telephones	22
5.9.	Configure the SIP Line Gateway Service	27
5.10.	Configure SIP Line Telephones	28
5.11.	Save Configuration	30
6.	Configuring Avaya Aura® Session Manager	31
6.1.	Log in to Avaya Aura® System Manager.....	31
6.2.	Administer SIP Domain	32
6.3.	Administer Locations	33
6.4.	Administer Adaptations.....	34
6.5.	Administer SIP Entities.....	35
6.5.1.	Avaya Aura® Session Manager SIP Entity	36
6.5.2.	Avaya Communication Server 1000 SIP Entity	37
6.5.3.	Avaya Session Border Controller for Enterprise SIP Entity.....	38
6.6.	Administer Entity Links	39
6.7.	Administer Routing Policies	40
6.8.	Administer Dial Patterns	42
7.	Configure Avaya Session Border Controller for Enterprise	44
7.1.	Access Avaya Session Border Controller for Enterprise	44
7.2.	Global Profiles.....	46
7.2.1.	Server Interworking - Avaya	46
7.2.2.	Server Interworking – Vodafone Libertel B.V.	48
7.2.3.	Server Configuration – Avaya	50
7.2.4.	Server Configuration – Vodafone Libertel B.V.....	51
7.2.5.	Routing.....	53
7.2.6.	Topology Hiding.....	57
7.3.	Define Network Information.....	59
7.4.	Define Interfaces	60

7.4.1.	Signalling Interfaces	60
7.4.2.	Media Interfaces.....	61
7.5.	Server Flows.....	62
8.	Configure Vodafone Libertel B.V. SIP Trunk Equipment	67
9.	Verification Steps.....	67
9.1.	Avaya Communication Server 1000 Verification.....	67
9.1.1.	IP Network Maintenance and Reports Commands.....	67
9.2.	Verify Avaya Communication Server 1000 Operational Status	69
9.3.	Verify Avaya Aura® Session Manager Operational Status	70
9.3.1.	Verify Avaya Aura® Session Manager is Operational.....	70
9.3.2.	Verify SIP Entity Link Status	71
9.4.	Avaya Session Boarder Controller for Enterprise Verification	72
9.4.1.	Incidents.....	72
9.4.2.	Trace Settings.....	73
10.	Conclusion	74
11.	Additional References.....	74
12.	Appendix A – Communication Server 1000 Software	75
13.	Appendix B – Inbound & Outbound CallFlow Examples	79

1. Introduction

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between Vodafone Libertel B.V. (Vodafone Libertel) SIP Trunk Service and an Avaya SIP-enabled enterprise solution. The Avaya solution consists of Avaya Session Border Controller for Enterprise (Avaya SBCE) R6.3, Avaya Aura® Session Manager R6.3 and Avaya Communication Server 1000 (CS1000) R7.6. Customers using this Avaya SIP-enabled enterprise solution with the Vodafone Libertel SIP Trunk Service are able to place and receive PSTN calls via a dedicated Internet connection and the SIP protocol. The Vodafone solution incorporates routing for calls placed to and from their Mobile and Fixed networks separately and offer short dialling from dedicated mobile telephones. This converged network solution is an alternative to traditional PSTN trunks. This approach generally results in lower cost for the enterprise.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using an Avaya SIP telephony solution consisting of CS1000, Session Manager and Avaya SBCE. The enterprise site was configured to use the SIP Trunking Service provided by Vodafone Libertel.

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.

Avaya recommends our customers implement Avaya solutions using appropriate security and encryption capabilities enabled by our products. The testing referenced in this DevConnect Application Note included the enablement of supported encryption capabilities in the Avaya products. Readers should consult the appropriate Avaya product documentation for further information regarding security and encryption capabilities supported by those Avaya products.

Support for these security and encryption capabilities in any non-Avaya solution component is the responsibility of each individual vendor. Readers should consult the appropriate vendor-supplied product documentation for more information regarding those products.

For the testing associated with this Application Note, the interface between Avaya systems and the Vodafone Libertel SIP Trunk Service did not include use of any specific encryption features.

2.1. Interoperability Compliance Testing

The interoperability test included the following:

- Incoming calls to the enterprise site from PSTN phones using the Vodafone Libertel SIP Fixed Trunking Service, calls made to SIP and UNISTim telephones at the enterprise.
- Outgoing calls from the enterprise site completed via the Vodafone Libertel SIP Fixed Trunking Service to PSTN destinations, calls made from SIP and UNISTim telephones.
- Incoming calls to the enterprise site from mobile and short-dial numbers using the Vodafone Libertel SIP Mobile Trunking Service, calls made to SIP and UNISTim telephones at the enterprise.
- Outgoing calls from the enterprise site completed via the Vodafone Libertel SIP Mobile Trunking Service to Mobile and short-dial destinations, calls made from SIP and UNISTim telephones.
- Inbound and outbound PSTN calls to/from Avaya 2050IP Softphone.
- Calls using the G.711A and G.729 codec's.
- Fax calls to/from a group 3 fax machine to a PSTN-connected fax machine using T.38 and G.711 pass-through fax transmissions.
- Caller ID Presentation and Caller ID Restriction.
- DTMF transmission using RFC 2833.
- Voice Mail/Vector navigation for inbound and outbound calls.
- User features such as hold and resume, transfer and conference.
- Call coverage and call forwarding for endpoints at the enterprise site.
- Off-net call forwarding and Mobile-X mobile twinning.
- Transmission and response of SIP OPTIONS messages sent by Vodafone Libertel's SIP Trunk requiring Avaya response and sent by Avaya requiring Vodafone Libertel response.

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for Vodafone Libertel's SIP Trunk Service with the following observations:

- During testing it was observed that when CS1000 initiates a call-hold, the CS1000 sends a re-INVITE with the attributes "a=inactive" and "c=0.0.0.0" in the SDP as design intent. This results in no RTCP packets being transmitted during the call-hold duration. Vodafone Libertel expects to receive RTCP packets during the call-hold duration and have 30 second RTCP timers configured on their SIP MGW. As Vodafone Libertel do not receive any RTCP packets from the CS1000 after 30 seconds, Vodafone Libertel issue a BYE and the call is torn down. **Note:** In order to resolve this RTCP timer issue, Music on Hold (MOH) must be enabled on the CS1000 when call-hold is initiated. With MOH enabled, the CS1000 sends a re-INVITE with the attribute "SendRecv" in the SDP. With "SendRecv" attribute in the SDP, the CS1000 will send both RTP and RTCP packets when on-hold to the Vodafone Libertel SIP trunk thus resolving the call-hold problem.

- The CS1000 default configuration will not allow a blind transfer to be executed (incoming SIP Service Provider trunk to outgoing SIP Service Provider trunk) if the SIP Service Provider in question does not support the SIP UPDATE method. With the installation of plugin 501 on the CS1000, the blind transfer will be allowed, and the call will be completed. The limitation of this plugin is that no ringback is provided to the originator of the call for the duration that the destination set is ringing. In addition to plugin 501, it is required that **VTRK SU version “cs1000-vtrk-7.65.16.22.-4.i386.000.ntl”** or higher be used on all SSG signalling servers to ensure proper operation of the blind transfer feature. The use of plugin 501 does not restrict the use of the SIP UPDATE method of blind transfer to other parties that do happen to support the UPDATE method, but rather extends support to those parties that do not. Note that plugin 501 is independent of and does not require the Global Plugin Package 409.
- Mobile-X features such as on-net and off-net calling were not tested as the From Header CLID containing the Mobile-X mobility number on inbound calls to Vodafone Libertel SIP Trunk service was automatically changed by Vodafone Libertel to a CLID number recognizable to the Vodafone Libertel network.
- All unwanted MIME was stripped on outbound calls using the Adaptation Module in Session Manager.
- No inbound toll-free numbers were tested, however routing of inbound DDI numbers and the relevant number translation was successfully tested.
- Access to Emergency Services was not tested as no test call had been booked with the Emergency Services Operator.

2.3. Support

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

For technical support on Vodafone Libertel B.V. SIP Trunking Services, contact Vodafone Libertel support at <http://www.vodafone.nl/midden-groot-bedrijf/oplossingen/>.

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an Enterprise site connected to Vodafone Libertel's SIP Trunk Service. Located at the Enterprise site is an Avaya SBCE, Session Manager and CS1000. Endpoints are Avaya 1140 series IP telephones (with Unistim and SIP firmware), Avaya 1200 series IP telephones (with Unistim and SIP firmware), Avaya IP 2050PC Softphone, Avaya Digital telephone, Analog telephone and fax machine. For security purposes, any public IP addresses or PSTN routable phone numbers used in the compliance test are not shown in these Application Notes.

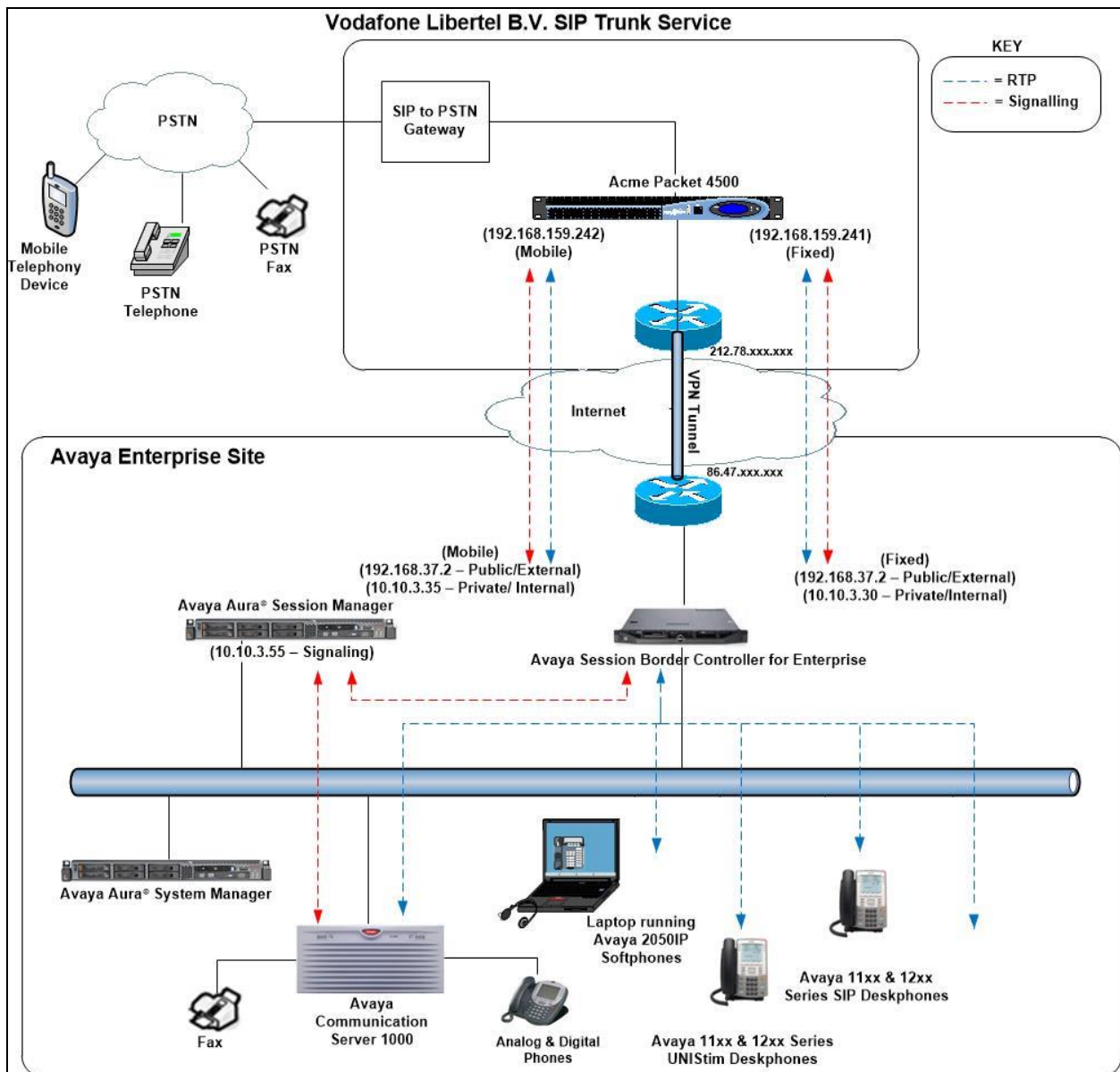


Figure 1: Test Setup Vodafone Libertel B.V. SIP Trunk to Avaya Enterprise

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya Aura® System Manager	R6.3.22 Build No – 6.3.0.8.5682-6.3.8.6302 Software Update Revision No: 6.3.22.19.8226
Avaya Aura® Session Manager	R6.3.22.0.632205
Avaya Communication Server 1000	Avaya Communication Server 1000 R7.6 Version 7.65.P Depllist: CPL_X21_07_65P All CS1000 patches listed in Appendix A
Avaya Communication Server 1000 Media Gateway	CSP Version: MGCC DC01 MSP Version: MGCM AB02 APP Version: MGCA BA18 FPGA Version: MGCF AA22 BOOT Version: MGCB BA18 DSP1 Version: DSP2 AB07
Avaya Session Border Controller for Enterprise	6.3.7-01-12611
Avaya 1140e and 1230 Unistim Telephones	FW: 0625C96
Avaya 1140e and 1230 SIP Telephones	FW: 04.04.30.00.bin
Avaya 2050PC	Release 4.04.217 (R 4.4 SP9
Avaya Analog Telephone	N/A
Avaya M3904 Digital Telephone	N/A
Vodafone Libertel B.V.	
Acme Packet Net-Net 4500 VoF	SCZ740p4
Acme Packet Net-Net 4500 CNoIP	SCX620m11p4
OneAccess One700	ONEOS11-VOIP_SIP_11N-V4.3R7C14_HC4
SIP GW CPE Cisco 2901	VF-CUBE (15.4(3)M3)

5. Configure Avaya Communication Server 1000

This section describes the steps required to configure CS1000 for SIP Trunking and also the basic configuration for telephones (analog, SIP and IP phones). SIP trunks are established between CS1000 and Session Manager. SIP trunks are also established between Session Manager and the Avaya SBCE private interface. The Avaya SBCE public interface connects to the Vodafone Libertel SIP trunks. Incoming PSTN calls from the Vodafone Libertel SIP Trunk service traverse the Avaya SBCE and are directed to the Session Manager, which directs the calls to CS1000 (see **Figure 1**).

When a SIP message arrives at CS1000, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed. All outgoing calls to the PSTN are processed within CS1000 and may be first subject to outbound features such as route selection, digit manipulation and class of service restrictions. When CS1000 selects a SIP trunk for outgoing PSTN calls, SIP signaling is directed to Session Manager. Session Manager directs the outbound SIP messages to the Avaya SBCE private interface. The Avaya SBCE public interface manages outgoing SIP sessions onwards to the Vodafone Libertel SIP trunks.

Specific CS1000 configuration was performed using Element Manager and the system terminal interface. The general installation of the CS1000, System Manager, Session Manager and Avaya SBCE is presumed to have been previously completed and is not discussed here. Configuration details will be provided as required to draw attention to changes in default system configurations.

5.1. Logging into the Avaya Communication Server 1000

Configuration on the CS1000 will be performed by using both SSH Putty session and Avaya Unified Communications Management GUI.

Log in using SSH to the ELAN IP address of the Call Server with a username containing the correct privileges. Once logged in type **csconsole**, this will take the user into the vxworks shell of the call server. Next type **login**; the user will then be asked to login with correct credentials. Once logged-in the user can then progress to load any overlay.

Log in using the web-based Avaya Unified Communications Management GUI. Avaya Unified Communications Management GUI may be launched directly via <http://<ipaddress>> where the relevant <ipaddress> is the TLAN IP address of the CS1000. Avaya Unified Communications Management can also be implemented on System Manager.

The following screen shows the login screen. Login with the appropriate credentials.

AVAYA

Use this page to access the server by IP address. You will need to log in again when switching to another server, even if it is in the same security domain.

Important: Only accounts which have been previously created in the primary security server are allowed. Expired or reset passwords that normally must be changed during login will fail authentication in this mode (use the link to manual password change instead). Local OS-authenticated User IDs cannot be used.

[Go to central login for Single Sign-On](#)

User ID:

Password:

Log In

[Change Password](#)

The Avaya Unified Communications Management **Elements** page will be used for configuration. Click on the Element Name corresponding to CS1000 in the Element Type column. In the abridged screen below, the user would click on the Element Name **EM on cs1kv19**.

Host Name: 10.10.9.57 User Name: admin

Elements

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

Search Reset

Add... Edit... Delete

	Element Name	Element Type ^	Release	Address	Description
1	smorv9.avaya.com (primary)	Base OS	7.6	10.10.9.57	Base OS element.
2	<input checked="" type="checkbox"/> EM on cs1kv19	CS1000	7.6	192.168.27.2	New element.
3	<input type="checkbox"/> cs1kv19.avaya.com (member)	Linux Base	7.6	10.10.9.20	Base OS element.
4	<input type="checkbox"/> 192.168.27.3	Media Gateway Controller	7.6	192.168.27.3	New element.
5	<input type="checkbox"/> NRSIM on cs1kv19	Network Routing Service	7.6	192.168.27.2	New element.

5.2. Confirm System Features

The keycode installed on the Call Server controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative to add additional capacity. Use the CS1000 system terminal and manually load overlay 22 to print the System Limits (the required command is **slt**) and verify that the number of SIP Access Ports reported by the system is sufficient for the combination of trunks to the Vodafone Libertel network, and any other SIP trunks needed. See the following screenshot for a typical System Limits printout. The value of **SIP ACCESS PORTS** defines the maximum number of SIP trunks for the CS1000.

CMN; Reviewed:
SPOC 12/5/2018

Solution & Interoperability Test Lab Application Notes
©2018 Avaya Inc. All Rights Reserved.

10 of 93
VLBVCS1KSMSBC63

System type is - Communication Server 1000/CP PM
CP PM - Pentium M 1.4 GHz

IPMGs Registered:	4				
IPMGs Unregistered:	0				
IPMGs Configured/unregistered:	2				
TRADITIONAL TELEPHONES	120	LEFT	110	USED	10
DECT USERS	16	LEFT	16	USED	0
IP USERS	10000	LEFT	9954	USED	46
BASIC IP USERS	16	LEFT	13	USED	3
TEMPORARY IP USERS	8	LEFT	8	USED	0
DECT VISITOR USER	16	LEFT	16	USED	0
ACD AGENTS	192	LEFT	185	USED	7
MOBILE EXTENSIONS	8	LEFT	7	USED	1
TELEPHONY SERVICES	16	LEFT	13	USED	3
CONVERGED MOBILE USERS	8	LEFT	8	USED	0
AVAYA SIP LINES	16	LEFT	12	USED	4
THIRD PARTY SIP LINES	16	LEFT	16	USED	0
PCA	20	LEFT	18	USED	2
ITG ISDN TRUNKS	0	LEFT	0	USED	0
H.323 ACCESS PORTS	524	LEFT	524	USED	0
AST	6652	LEFT	6640	USED	12
SIP CONVERGED DESKTOPS	16	LEFT	16	USED	0
SIP CTI TR87	16	LEFT	8	USED	8
SIP ACCESS PORTS	524	LEFT	518	USED	6
RAN CON	90	LEFT	90	USED	0
MUS CON	120	LEFT	120	USED	0

Load Overlay 21 and confirm the customer is setup to use **ISDN** trunks by typing the **PRT** and **NET_DATA** commands as shown below.

```
REQ: prt
TYPE: net
TYPE NET_DATA
CUST 0

TYPE NET_DATA
CUST 00
OPT RTD
AC1 INTL NPA SPN NXX LOC
AC2
FNP YES
ISDN YES
```

5.3. Configure Codecs for Voice and FAX operation

Vodafone Libertel's SIP Trunk supports G.711A and G.729 voice codecs. Using the CS1000 Element Manager sidebar, select **Nodes, Servers, Media Cards**. Navigate to the **IP Network → IP Telephony Nodes → Node Details → VGW and Codecs** property page and configure the CS1000 **General** codec settings as in the following screenshots. The values highlighted are required for correct operation. The following screenshot shows the necessary **General** settings.

Move down to the Voice Codecs section and configure the G.711 codec settings. The following screenshot shows the G.711 codec settings.

Managing: 192.168.27.2 Username: admin
System » IP Network » IP Telephony Nodes » Node Details » VGW and Codecs

Node ID: 200 - Voice Gateway (VGW) and Codecs

General | Voice Codecs | Fax

Codec G711: ☒ Enabled (required)

Voice payload size: 20 (milliseconds per frame)

Voice playout (jitter buffer) delay: 40 (Nominal) 80 (Maximum) (milliseconds)

Maximum delay may be automatically adjusted based on nominal settings.

☐ Voice Activity Detection (VAD)

Next, scroll down to the G.729 codec section and configure the settings.

Managing: 192.168.27.2 Username: admin
System » IP Network » IP Telephony Nodes » Node Details » VGW and Codecs

Node ID: 200 - Voice Gateway (VGW) and Codecs

General | Voice Codecs | Fax

Codec G729: ☒ Enabled

Voice payload size: 20 (milliseconds per frame)

Voice playout (jitter buffer) delay: 40 80 (milliseconds)

Nominal Maximum

Maximum delay may be automatically adjusted based on nominal settings.

☐ Voice Activity Detection (VAD)

Finally, configure the Fax settings as in the highlighted section of the next screenshot. Click on the **Save** button when finished.

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)

5.4. Virtual Trunk Gateway Configuration

Use CS1000 Element Manager to configure the system node properties. Navigate to the **System** → **IP Networks** → **IP Telephony Nodes** → **Node Details** and verify the highlighted section is completed with the correct IP addresses and subnet masks of the Node. The call server and signaling server have previously been configured with IP addresses. The Node IPv4 address is the IP address that the IP phones use to register. This is also where the SIP trunk connection is made to Session Manager. When an entity link is added in Session Manager for the CS1000, it is the Node IPv4 address that is used (see **Section 6.5** – Define SIP Entities for more details).

Managing: 192.168.27.2 Username: admin

System » IP Network » IP Telephony Nodes » Node Details

Node Details (ID: 200 - SIP Line, LTPS, PD, Gateway (SIPGw))

Node ID: * (0-9999)

Call server IP address: *

Embedded LAN (ELAN)
Gateway IP address: *
Subnet mask: *

IP Telephony Node Properties

- [Voice Gateway \(VGW\) and Codecs](#)
- [Quality of Service \(QoS\)](#)
- [LAN](#)
- [SNTP](#)
- [Numbering Zones](#)
- [MCDN Alternative Routing Treatment \(MALT\) Causes](#)

TLAN address type: ☒ IPv4 only
☐ IPv4 and IPv6

Telephony LAN (TLAN)
Node IPv4 address: *
Subnet mask: *
Node IPv6 address:

Applications (click to edit configuration)

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

* Required Value.

SaveCancel

CMN; Reviewed:
SPOC 12/5/2018

Solution & Interoperability Test Lab Application Notes
©2018 Avaya Inc. All Rights Reserved.

14 of 93
VLBVCS1KSMSBC63

The next two screenshots show the SIP Virtual Trunk Gateway configuration, navigate to **System → IP Networks → IP Telephony Nodes → Node Details → Gateway (SIPGW) Virtual Trunk Configuration Details** and fill in the highlighted areas with the relevant settings.

- **Vtrk gateway application:** Provides option to select Gateway applications. The three supported modes are **SIP Gateway (SIPGw)**, **H.323Gw**, and **SIPGw and H.323Gw**
- **SIP domain name:** The SIP domain name is the SIP Service Domain. The SIP domain name configured in the Signaling Server properties must match the Service Domain name configured in Session Manager; in this case **avaya.com**.
- **Local SIP port:** The Local SIP Port is the port to which the gateway listens. The default value is **5060**.
- **Gateway endpoint name:** This field cannot be left blank, so a value is needed here. This field is used when a Network Routing Server is used for registration of the endpoint. In this network a Session Manager is used so any value can be put in here and will not be used.
- **Application node ID:** This is a unique value that can be alphanumeric and is for the new Node that is being created, in this case **200**.
- **Proxy or Redirect Server:** Primary TLAN IP address is the Security Module IP address of Session Manager. The **Transport protocol** used for **SIP**, in this case is **TCP**.
- **SIP URI Map:** **Public E.164 - National** and **Private - Unknown** are left blank. All other fields in the SIP URI Map are left with default values.

Managing: 192.168.27.2 Username: admin
System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration

Node ID: 200 - Virtual Trunk Gateway Configuration Details

General | SIP Gateway Settings | SIP Gateway Services

Vtrk gateway application: ☒ Enable gateway service on this node

General

Vtrk gateway application: SIP Gateway (SIPGw) ▼

SIP domain name: avaya.com *

Local SIP port: 5060 *(1 - 65535)

Gateway endpoint name: cs1kv19 *

Gateway password: *

Application node ID: 200 *(0-9999)

Enable failsafe NRS: ☐

Note: FailSafe NRS cannot be enabled, if all servers in the node have NRS application deployed.

SIP ANAT: ☒ IPv4

Virtual Trunk Network Health Monitor

☐ Monitor IP addresses (listed below)

Information will be captured for the IP addresses listed below.

Monitor IP:

Monitor addresses:

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

Proxy Or Redirect Server: Proxy Server Route 1:	
Primary TLAN IP address:	<input type="text" value="10.10.3.55"/> <small>The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"</small>
Port:	<input type="text" value="5060"/> (1 - 65535)
Transport protocol:	<input type="text" value="TCP"/> ▼
Options:	<input type="checkbox"/> Support registration <input type="checkbox"/> Primary CDS proxy
Secondary TLAN IP address:	<input type="text" value="0.0.0.0"/> <small>The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"</small>
Port:	<input type="text" value="5060"/> (1 - 65535)
Transport protocol:	<input type="text" value="TCP"/> ▼
SIP URI Map:	
Public E.164 domain names	Private domain names
National: <input type="text"/>	UDP: <input type="text" value="udp"/>
Subscriber: <input type="text" value="subscriber"/>	CDP: <input type="text" value="cdp.udp"/>
Special number: <input type="text" value="PublicSpecial"/>	Special number: <input type="text" value="PrivateSpecial"/>
Unknown: <input type="text" value="PublicUnknown"/>	Vacant number: <input type="text" value="PrivateUnknown"/>
	Unknown: <input type="text"/>

5.5. Configure Bandwidth Zones

Bandwidth Zones are used for alternate call routing between IP stations and for bandwidth management. SIP trunks require a unique zone, not shared with other resources and best practice dictates that IP telephones and Media Gateways are all placed in separate zones. In the sample configuration SIP trunks use zone 01 and IP and SIP Telephones use zone 02; system defaults were used for each zone other than the parameter configured for **Zone Intent**. For SIP Trunks (zone 01), **VTRK** is configured for **Zone Intent**. For IP, SIP Telephones (zone 02), **MO** is configured for **Main Office**.

Use Element Manager to define bandwidth zones as in the following highlighted example. Use Element Manager and navigate to **System → IP Network → Zones → Bandwidth Zones** and add new zones as required.

Managing: 192.168.27.2 Username: admin
System » IP Network » Zones » Bandwidth Zones

Bandwidth Zones

Add... Edit... Import... Export Maintenance... Delete

	Zone ▲	Intrazone Bandwidth	Intrazone Strategy	Interzone Bandwidth	Interzone Strategy	Resource Type	Zone Intent	Description
1	1	1000000	BQ	1000000	BQ	SHARED	VTRK	
2	2	1000000	BQ	1000000	BQ	SHARED	MO	

5.6. Configure Incoming Digit Conversion Table

A limited number of Direct Dial Inwards (DDI) numbers were available. The Incoming Digit Conversion (IDC) table was configured to translate incoming PSTN numbers to four-digit local telephone extension numbers. The digits of the actual PSTN DDI number are obscured for security reasons. The following screenshot shows the incoming PSTN numbers converted to local extension numbers. These were altered during testing to map to various SIP, Analog, Digital or UNISim telephones depending on the particular test case being executed.

Managing: 192.168.27.2 Username: admin
Dialing and Numbering Plans » Incoming Digit Translation » Customer 00 » 0 Configuration

0 Configuration

Regular IDC tree
Send calling party DID disabled

Add... Delete IDC Delete IDC tree

	Incoming Digits ▲	Converted Digits	CPND Name
1	2091	6003	
2	03 2091	6000	
3	03 2092	6002	
4	03 2093	6003	
5	03 2094	6001	
6	03 2095	6005	

5.7. Configure SIP Trunks

CS1000 virtual trunks will be used for all inbound and outbound PSTN calls to the Vodafone Libertel SIP Trunk service. Six separate steps are required to configure CS1000 virtual trunks:

- Configure a D-Channel Handler (**DCH**); configure using the CS1000 system terminal and overlay 17.
- Configure a SIP trunk Route Data Block (**RDB**); configure using the CS1000 system terminal and overlay 16.
- Configure SIP trunk members; configure using the CS1000 system terminal and overlay 14.
- Configure a Digit Manipulation Data Block (**DGT**), configure using the CS1000 system terminal and overlay 86.
- Configure a Route List Block (**RLB**); configure using the CS1000 system terminal and overlay 86.
- Configure Co-ordinated Dialling Plan(s) (**CDP**); configure using the CS1000 system terminal and overlay 87.

The following is an example DCH configuration for SIP trunks. Load **Overlay 17** at the CS1000 system terminal and enter the following values. The highlighted entries are required for correct SIP trunk operation. Exit overlay 17 when completed.

```
Overlay 17
ADAN      DCH 1
CTYP DCIP
DES  VIR_TRK
USR  ISLD
ISLM 4000
SSRC 3700
OTBF 32
NASA YES
IFC  SL1
CNEG 1
RLS  ID  4
RCAP ND2
MBGA NO
H323
OVLN NO
OVLS NO
```

Next, configure the SIP trunk Route Data Block (RDB) using the CS1000 system terminal and overlay 16. Load **Overlay 16**, enter **RDB** at the prompt, press return and commence configuration. The value for **DCH** is the same as previously entered in overlay 17. The value for **NODE** should match the node value in **Section 5.4**. The value for **ZONE** should match that used in **Section 5.5** for **VTRK**. The remaining highlighted values are important for correct SIP trunk operation.

Overlay 16 TYPE: RDB CUST 00 ROUT 1 TYPE RDB CUST 00 ROUT 1 DES VIR_TRK TKTP TIE NPID_TBL_NUM 0 ESN NO RPA NO CNVT NO SAT NO RCLS EXT VTRK YES ZONE 00001 PCID SIP CRID NO NODE 200 DTRK NO ISDN YES MODE ISLD DCH 1 IFC SL1 PNI 00000 NCNA YES NCRD YES TRO NO FALT NO CTYP UKWN INAC NO ISAR NO DAPC NO MBXR NO MBXOT NPA MBXT 0 PTYP ATT CNDP UKWN AUTO NO DNIS NO DCDR NO ICOG IAO SRCH LIN TRMB YES STEP	ACOD 1111 TCPP NO PII NO AUXP NO TARG CLEN 1 BILN NO OABS INST IDC YES DCNO 0 NDNO 0 * DEXT NO DNAM NO SIGO STD STYP SDAT MFC NO ICIS YES OGIS YES TIMR ICF 1920 OGF 1920 EOD 13952 LCT 256 DSI 34944 NRD 10112 DDL 70 ODT 4096 RGV 640 GTO 896 GTI 896 SFB 3 PRPS 800 NBS 2048 NBL 4096 IENB 5 TFD 0 VSS 0 VGD 6 EESD 1024 SST 5 0 DTD NO SCDT NO 2 DT NO NEDC ORG FEDC ORG	CPDC NO DLTN NO HOLD 02 02 40 SEIZ 02 02 SVFL 02 02 DRNG NO CDR NO NATL YES SSL CFWR NO IDOP NO VRAT NO MUS YES MRT 21 PANS YES RACD NO MANO NO FRL 0 0 FRL 1 0 FRL 2 0 FRL 3 0 FRL 4 0 FRL 5 0 FRL 6 0 FRL 7 0 OHQ NO OHQT 00 CBQ NO AUTH NO TTBL 0 ATAN NO OHTD NO PLEV 2 OPR NO ALRM NO ART 0 PECL NO DCTI 0 TIDY 1600 100 ATRR NO TRRL NO SGRP 0 ARDN NO CTBL 0 AACR NO
---	--	---

Next, configure virtual trunk members using the CS1000 system terminal and **Overlay 14**. Configure sufficient trunk members to carry both incoming and outgoing PSTN calls. The following example shows a single SIP trunk member configuration. Load **Overlay 14** at the system terminal and type **new X**, where X is the required number of trunks. Continue entering data until the overlay exits. The **RTMB** value is a combination of the **ROUT** value entered in the previous step and the first trunk member (usually 1). The remaining highlighted values are important for correct SIP trunk operation.

```
Overlay 14
TN 100 0 0 0
DATE
PAGE
DES VIR_TRK
TN 100 0 00 00 VIRTUAL
TYPE IPTI
CDEN 8D
CUST 0
XTRK VTRK
ZONE 00001
TIMP 600
BIMP 600
AUTO_BIMP NO
NMUS NO
TRK ANLG
NCOS 0
RTMB 1 1
CHID 1
TGAR 1
STRI/STRO IMM IMM
SUPN YES
AST NO
IAPG 0
CLS UNR DIP CND ECD WTA LPR APN THFD XREP SPCD MSBT
P10 NTC
TKID
AACR NO
```

Next, configure a Digit Manipulation data block (DGT) in overlay 86. Load **Overlay 86** at the system terminal and type **new**. The following example shows the values used. The value for Digit Manipulation Index (**DMI**) is the same as when inputting the **DMI** value during configuration of the Route List Block.

Overlay 86

```
CUST 0
FEAT dgt
DMI 10
DEL 0
ISPN 0
CTYP NPA
```

Configure a Route List Block (RLB) in overlay 86. Load **Overlay 86** at the system terminal and type **new**. The following example shows the values used. The value for **ROUT** is the same as previously entered in overlay 16. The **RLI** value is unique to each RLB.

Overlay 86

```
CUST 0
FEAT rlb
RLI 10
ELC NO
ENTR 0
LTER NO
ROUT 1
TOD 0 ON 1 ON 2 ON 3 ON
    4 ON 5 ON 6 ON 7 ON
VNS NO
SCNV NO
CNV NO
EXP NO
FRL 0
DMI 10
CTBL 0
ISDM 0
```

```
FCI 0
FSNI 0
BNE NO
DORG NO
SBOC NRR
PROU 1
IDBB DBD
IOHQ NO
OHQ NO
CBQ NO

ISET 0
NALT 5
MFRL 0
OVLL 0
```

Next, configure Co-ordinated Dialling Plan(s) (CDP) which users will dial to reach PSTN numbers. Use the CS1000 system terminal and **Overlay 87**. The following are some example CDP entries used. The highlighted **RLI** value previously configured in overlay 86 is used as the Route List Index (**RLI**), this is the default PSTN route to the SIP Trunk service.

```
TSC 00353
FLEN 0
RRPA NO
RLI 10
CCBA NO
```

```
TSC 18
FLEN 0
RRPA NO
RLI 10
CCBA NO
```

```
TSC 800
FLEN 0
RRPA NO
RLI 10
CCBA NO
```

```
TSC 08
FLEN 0
RRPA NO
RLI 10
CCBA NO
```

5.8. Configure Analog, Digital and IP Telephones

A variety of telephone types were used during the testing, the following is the configuration for the Avaya 1140e UNISim IP telephone. Load **Overlay 20** at the system terminal and enter the following values. A unique four-digit number is entered for the **KEY 00**. The value for **CFG_ZONE** is the value used in **Section 5.5** for IP and SIP Telephones.

Load Overlay 20 IP Telephone configuration

```
DES 1140
TN 100 0 03 0 VIRTUAL
TYPE 1140
CDEN 8D
CTYP XDLC
CUST 0
NUID
NHTN
CFG_ZONE 00002
CUR_ZONE 00002
ERL 0
ECL 0
FDN 0
TGAR 0
LDN NO
NCOS 0
SGRP 0
RNPG 1
SCI 0
SSU
LNRS 16
XLST
SCPW
SFLT NO
CAC_MFC 0
CLS UNR FBA WTA LPR PUA MTD FNA HTA TDD HFA CRPD
MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
POD SLKD CCSO SWD LNA CNDA
CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBF
ICDA CDMD LLCN MCTD CLBD AUTR
GPUD DPUD DNDA CFXA ARHD FITD CLTD ASCD
CPFA CPTA ABDD CFHD FICD NAID BUZZ AGRD MOAD
UDI RCC HBTA AHD IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
DRDD EXR0
USMD USRD ULAD CCBF RTDD RBDD RBHD PGND OCBF FLXD FTTC DNDY DNO3 MCBN
FDSD NOVD VOLA VOUD CDMR PRED RECA MCDD T87D SBMD KEM3 MSNV FRA PKCH MUTA MWTD
---continued on next page---
```

---continued from previous page---

```
DVLD CROD CROD
CPND_LANG ENG
RCO 0
HUNT 0
LHK 0
PLEV 02
PUID
DANI NO
AST 00
IAPG 1
AACS NO
ITNA NO
DGRP
MLWU_LANG 0
MLNG ENG
DNDR 0
KEY 00 MCR 6000 0      MARP
      CPND
        CPND_LANG ROMAN
        NAME IP1140
        XPLN 10
        DISPLAY_FMT FIRST, LAST
01 MCR 6000 0
      CPND
        CPND_LANG ROMAN
        NAME IP1140
        XPLN 10
        DISPLAY_FMT FIRST, LAST
02
03 BSY
04 DSP
05
06
07
08
09
10
11
12
13
14
15
16
17 TRN
18 AO6
19 CFW 16
20 RGA
21 PRK
22 RNP
23
24 PRS
25 CHG
26 CPN
```

Digital telephones are configured using the overlay 20; the following is a sample 3904 digital set configuration. Again, a unique number is entered for the **KEY 00** and **KEY 01** value.

Overlay 20 - Digital Set configuration

```

TYPE: 3904
DES 3904
TN 000 0 09 08 VIRTUAL
TYPE 3904
CDEN 8D
CTYP XDLC
CUST 0
MRT
ERL 0
FDN 0
TGAR 0
LDN NO
NCOS 0
SGRP 0
RNPG 1
SCI 0
SSU
LNRS 16
XLST
SCPW
SFLT NO
CAC_MFC 0
CLS UNR FBD WTA LPR PUA MTD FND HTD TDD HFA GRLD CRPA STSD
    MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
    POD SLKD CCSD SWD LNA CNDA
    CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBF
    ICDA CDMA LLCN MCTD CLBD AUTU
    GPUD DPUD DNDA CFXA ARHD FITD CNTD CLTD ASCD
    CPFA CPTA ABDA CFHD FICD NAID BUZZ AGRD MOAD
    UDI RCC HBTD AHA IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
    DRDD EXR0
    USMD USRD ULAD CCBF RTDD RBDD RBHD PGND OCBD FLXD FTTC DNDY DNO3 MCBN
    FDSF NOVD CDMR PRED RECA MCDD T87D SBMD PKCH CROD CROD
CPND LANG ENG
RCO 0
HUNT
PLEV 02
PUID
DANI NO
SPID NONE
AST
IAPG 1
AACS
ACQ
ASID
SFNB
SFRB
USFB
CALB
FCTB
ITNA NO
DGRP
PRI 01
MLWU_LANG 0

```

---continued on next page---

---continued from previous page----

MLNG ENG

DNDR 0

KEY 00 MCR 6066 0 MARP

CPND

CPND_LANG ROMAN

NAME Digital Set

XPLN 10

DISPLAY_FMT FIRST, LAST

01 MCR 6066 0

CPND

CPND_LANG ROMAN

NAME Digital Set

XPLN 10

DISPLAY_FMT FIRST, LAST

02 DSP

03 MSB

04

05

06

07

08

09

10

11

12

13

14

15

16

17 TRN

18 AO6

19 CFW 16

20 RGA

21 PRK

22 RNP

23

24 PRS

25 CHG

26 CPN

27 CLT

28 RLT

29

30

31

Analog telephones are also configured using overlay 20; the following example shows an analog port configured to allow fax transmission. A unique value is entered for **DN**, this is the extension number. **DTN** is required if the telephone uses DTMF dialing. Values **FAXA** and **MPTD** configure the port for T.38 Fax transmissions. Values **FAXD** and **MPTA** configure the port for G711 pass-through Fax transmissions if required.

```

Overlay 20 - Analog Telephone Configuration
DES 500
TN 100 0 00 03
TYPE 500
CDEN 4D
CUST 0
MRT

ERL 00000
WRLS NO
DN 6004
AST NO
IAPG 0
HUNT
TGAR 0
LDN NO
NCOS 0
SGRP 0
RNPG 0
XLST
SCI 0
SCPW
SFLT NO
CAC_MFC 0
CLS UNR DTN FBD XFD WTA THFD FND HTD ONS
    LPR XRD AGRD CWD SWD MWD RMMD SMWD LPD XHD SLKD CCSD LND TVD
    CFTD SFD MRD C6D CNID CLBD AUTU
    ICDD CDMD LLCN EHTD MCTD
    GPUD DPUD CFXD ARHD OVDD AGTD CLTD LDTD ASCD SDND
    MBXD CPFA CPTA UDI RCC HBTD IRGD DDGA NAMA MIND
    NRWD NRCD NROD SPKD CRD PRSD MCRD
    EXR0 SHL SMSD ABDD CFHD DNDY DNO3
    CWND USMD USRD CCBD BNRD OCBT RTDD RBDD RBHD FAXA CNUD CNAD PGND FTTC
    FDSD NOVD CDMR PRED MCDD T87D SBMD PKCH MPTD
PLEV 02
PUID
AACS NO
MLWU_LANG 0
FTR DCFW 4

```

5.9. Configure the SIP Line Gateway Service

SIP terminal operation requires the CS1000 node to be configured as a SIP Line Gateway (SLG) before SIP telephones can be configured. Prior to configuring the SIP Line node properties, the SIP Line service must be enabled in the customer data block. Use the CS1000 system terminal and overlay 15 to activate SIP Line services (SLS_DATA), as in the following example where **SIPL_ON** is set to **YES**.

```
SLS_DATA
SIPL_ON YES
UAPR 11
NMME NO
```

If a numerical value is entered against the **UAPR** setting, this number will be pre-appended to all SIP Line configurations and is used internally in the SIP Line server to track SIP terminals. Use Element Manager and navigate to the **IP Network → IP Telephony Nodes → Node Details → SIP Line Gateway Configuration** page. See the following screenshot for highlighted critical parameters.

- **SIP Line Gateway Application:** Enable the SIP line service on the node, check the box to enable
- **SIP domain Name:** The value must match that configured in **Section 6.2**.
- **SLG endpoint name:** The endpoint name is the same endpoint name as the SIP Line Gateway and will be used for SIP gateway registration.
- **SLG Local Sip port:** Default value is **5070**.
- **SLG Local Tls port:** Default value is **5071**.

Managing: 192.168.27.2 Username: admin
System » IP Network » IP Telephony Nodes » Node Details » SIP Line Configuration

Node ID: 200 - SIP Line Configuration Details

General | SIP Line Gateway Settings | SIP Line Gateway Service

SIP Line Gateway Application: ☒ Enable gateway service on this node

General

SIP domain name: *

SLG endpoint name:

SLG Group ID:

SLG Local Sip port: (1 - 65535)

SLG Local Tls port: (1 - 65535)

Virtual Trunk Network Health Monitor

☐ Monitor IP addresses (listed below)

Information will be captured for the IP addresses listed below.

Monitor IP:

Monitor addresses:

5.10. Configure SIP Line Telephones

When SIP Line service configuration is completed, use the CS1000 system terminal and **Overlay 20** to add a Universal Extension (UEXT). See the following example of a SIP Line extension. The value for **UXTY** must be **SIPL**. This example is for an Avaya SIP telephone, so the value for **SIPN** is 1. The **SIPU** value is the username, **SCPW** is the logon password and these values are required to register the SIP telephone to the SLG. The value for **CFG_ZONE** is the value used in **Section 5.5** for IP and SIP Telephones. A unique telephone number is entered for value **KEY 00**. The value for **KEY 01** is comprised of the **UAPR** (set in **Section 5.9**) value and the telephone number used in **KEY 00**.

```
Load Overlay 20 - SIP Telephone Configuration
DES  SIPD
TN    100 0 03 3  VIRTUAL
TYPE  UEXT
CDEN  8D
CTYP  XDLC
CUST  0
UXTY  SIPL
MCCL  YES
SIPN  1
SIP3  0
FMCL  0
TLSV  0
SIPU  6002
NDID  200
SUPR  NO
SUBR  DFLT MWI RGA CWI MSB
UXID
NUID
NHTN
CFG_ZONE 00002
CUR_ZONE 00002
ERL   0
ECL   0
VSIT  NO
FDN
TGAR  0
LDN   NO
NCOS  0
SGRP  0
RNPG  0
SCI   0
SSU
XLST
SCPW  1234
SFLT  NO
CAC_MFC 0
CLS   UNR FBD WTA LPR MTD FNA HTA TDD HFD CRPD
      MWD LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
      POD SLKD CCSD SWD LND CNDA
      CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBF
      ICDD CDMD LLCN MCTD CLBD AUTU
      GPUD DPUD DNDA CFXA ARHD FITD CLTD ASCD
      CPFA CPTA ABDD CFHD FICD NAID BUZZ AGRD MOAD

---continued on next page---
```

---continued from previous page---

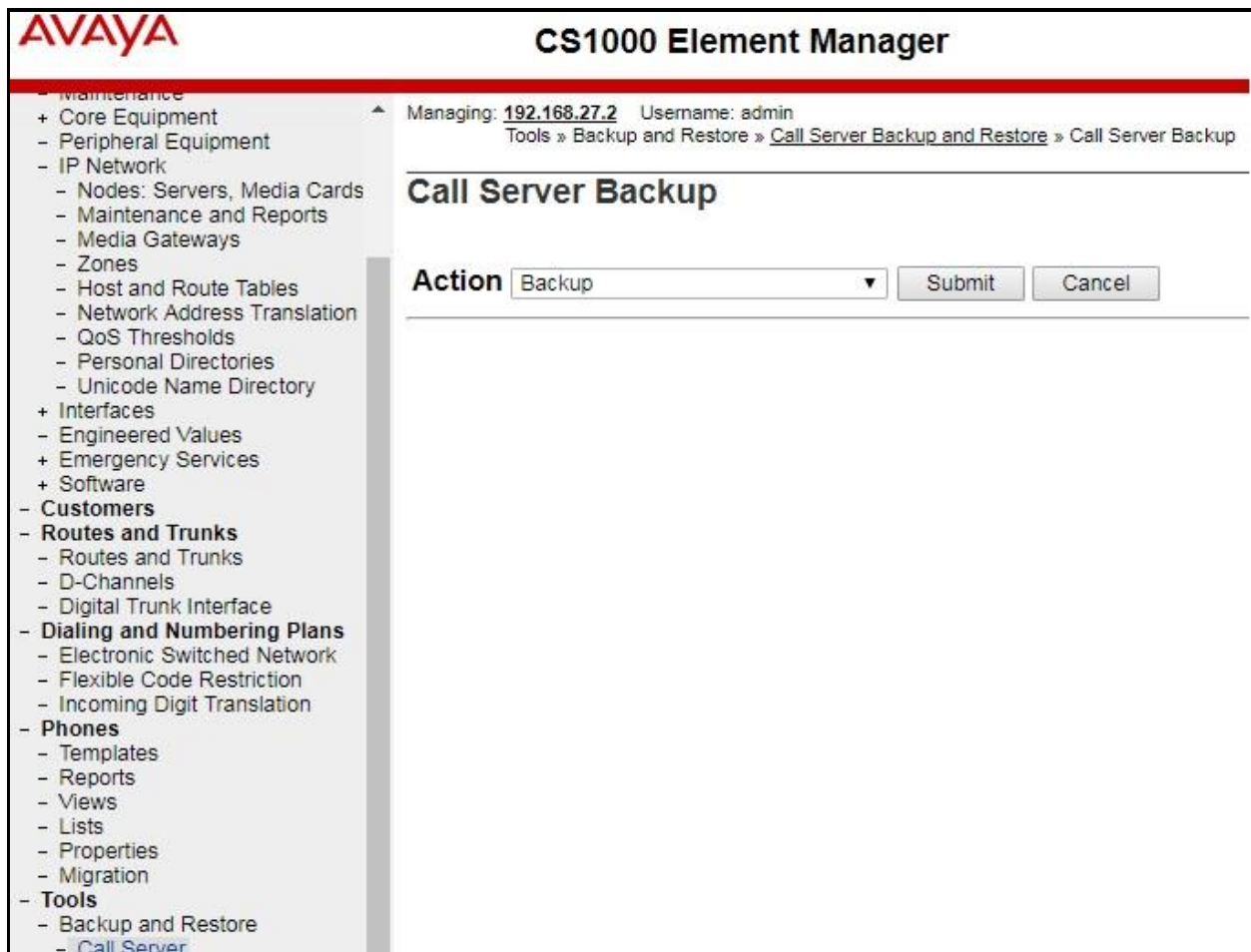
```

      UDI RCC HBTB AHA IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
      DRDD EXRO
      USMD USRD ULAD CCBD RTDD RBDD RBHD PGND OCBF FLXD FTTC DNDY DNO3 MCBN
      FDSD NOVD VOLA VOUD CDMR PRED RECD MCDD T87D SBMD ELMD MSNV FRA  PKCH MWTD DVLD
CROD CROD
CPND_LANG ENG
RCO 0
HUNT
LHK 0
PLEV 02
PUID
DANI NO
AST
IAPG 0 *

AACS NO
ITNA NO
DGRP
MLWU_LANG 0
MLNG ENG
DNDR 0
KEY 00 MCR 6002 0      MARP
      CPND
      CPND_LANG ROMAN
      NAME Sigma 1140
      XPLN 11
      DISPLAY_FMT FIRST, LAST*
01 HOT U 116002 MARP 0
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16
17 TRN
18 AO6
19 CFW 16
20 RGA
21 PRK
22 RNP
23 *
24 PRS
25 CHG
26 CPN
27
28
29
30
31
```

5.11. Save Configuration

Expand **Tools** → **Backup and Restore** on the left navigation panel and select **Call Server**. Select **Backup** (not shown) and click **Submit** to save configuration changes as shown below.



The screenshot shows the AVAYA CS1000 Element Manager web interface. On the left is a navigation tree with categories like Maintenance, Core Equipment, Peripheral Equipment, IP Network, Interfaces, Customers, Routes and Trunks, Dialing and Numbering Plans, Phones, and Tools. The 'Tools' category is expanded, showing 'Backup and Restore' and 'Call Server'. The main content area is titled 'Call Server Backup'. At the top of this area, it says 'Managing: 192.168.27.2 Username: admin' and 'Tools » Backup and Restore » Call Server Backup and Restore » Call Server Backup'. Below this is a section labeled 'Call Server Backup' with an 'Action' dropdown menu set to 'Backup' and 'Submit' and 'Cancel' buttons.

The backup process will take several minutes to complete. Scroll to the bottom of the page to verify the backup process completed successfully as shown below.

```
RMD device found available
.
Backing up reten.bkp to "/var/opt/nortel/cs/fs/cf2/backup/single"
Database backup Complete!
TEMU207
Backup process to local Removable Media Device ended successfully.
```

6. Configuring Avaya Aura® Session Manager

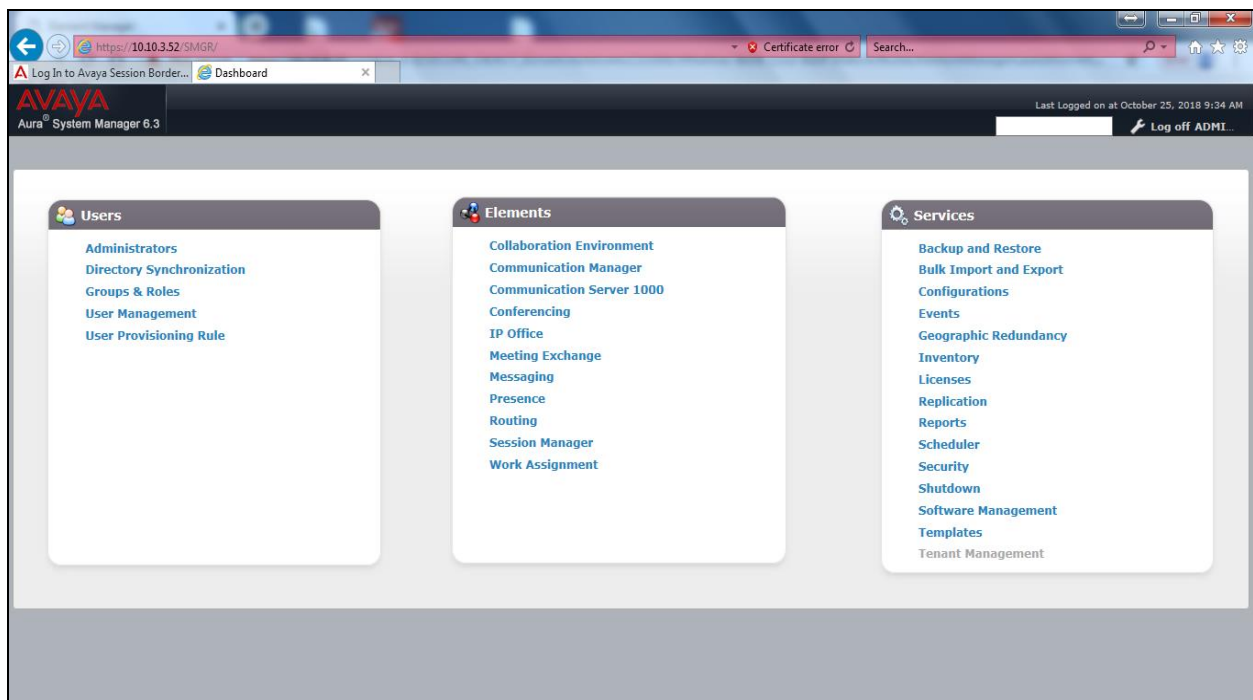
This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

- Log in to Avaya Aura® System Manager.
- Administer SIP Domain.
- Administer SIP Location.
- Administer Adaptations.
- Administer SIP Entities.
- Administer Entity Links.
- Administer Routing Policies.
- Administer Dial Patterns.

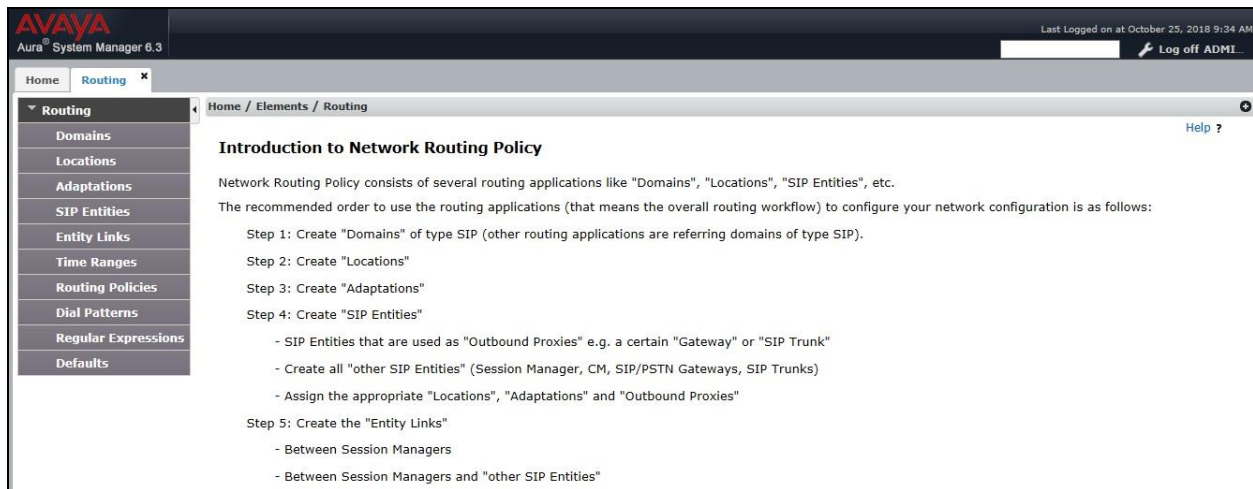
It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session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

6.1. Log in to Avaya Aura® System Manager

Access the System Manager using a Web Browser by entering **http://<FQDN >/SMGR**, where **<FQDN>** is the fully qualified domain name of System Manager. Log in using appropriate credentials (not shown) and the **Home** tab will be presented with menu options shown below.



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

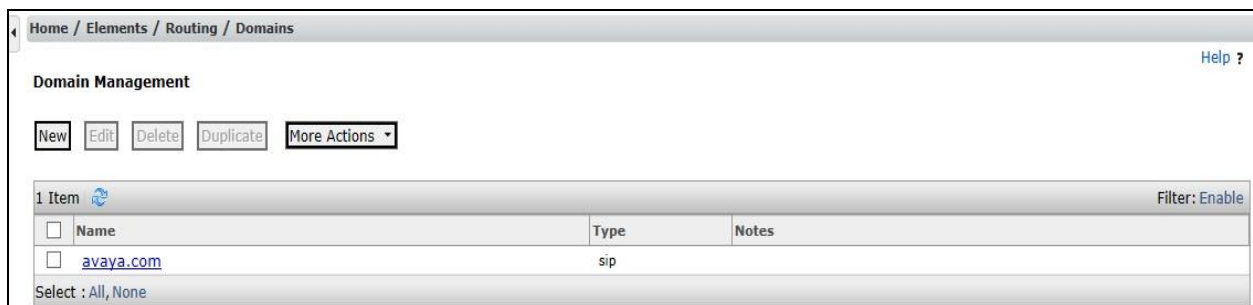


6.2. Administer SIP Domain

Create a SIP domain for each domain for which Session Manager will need to be aware in order to route calls. Expand **Elements** → **Routing** and select **Domains** from the left navigation menu, click **New** (not shown). Enter the following values and use default values for remaining fields.

- **Name** Enter a Domain Name. In the sample configuration, **avaya.com** was used.
- **Type** Verify **SIP** is selected.
- **Notes** Add a brief description [Optional].

Click **Commit** to save. The screen below shows the SIP Domain defined for the sample configuration.



6.3. Administer Locations

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. Use default values for all remaining fields:

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

The Location Pattern is used to identify call routing based on IP address. Session Manager matches the IP address against the patterns defined in this section. If a call is from a SIP Entity that does not match the IP address pattern, then Session Manager uses the location administered for the SIP Entity.

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

- **IP Address Pattern** Enter the logical pattern used to identify the location.
- **Notes** Add a brief description [Optional].

Click **Commit** to save. The screenshot below shows the Location **SMGRVL3** defined for the compliance testing.

The screenshot displays the Avaya Session Manager Administration console interface. The breadcrumb navigation at the top reads 'Home / Elements / Routing / Locations'. The main content area is titled 'Location Details' and includes 'Commit' and 'Cancel' buttons in the top right. The 'General' section contains a required field for 'Name' with the value 'SMGRVL3' and an optional 'Notes' field. Below this is the 'Dial Plan Transparency in Survivable Mode' section, which includes an 'Enabled' checkbox (unchecked), a 'Listed Directory Number' field, and a dropdown for 'Associated CM SIP Entity'. The 'Overall Managed Bandwidth' section features a 'Managed Bandwidth Units' dropdown set to 'Kbit/sec', and fields for 'Total Bandwidth' and 'Multimedia Bandwidth'. A checkbox for 'Audio Calls Can Take Multimedia Bandwidth' is checked. The 'Location Pattern' section at the bottom has 'Add' and 'Remove' buttons, a table with 3 items, and a 'Filter: Enable' button. The table has columns for 'IP Address Pattern' and 'Notes'. The listed patterns are '*10.10.3.*', '*10.10.5.*', and '*10.10.8.*'. At the bottom of the console, there are 'Commit' and 'Cancel' buttons.

IP Address Pattern	Notes
10.10.3.	
10.10.5.	
10.10.8.	

6.4. Administer Adaptations

Adaptations can be used to modify the called and calling party numbers to meet the requirements of the service. The called party number present in the SIP INVITE Request URI is modified by the **Digit Conversion** in the Adaptation. The example below was applied to the Avaya SBCE SIP Entity and was used in test to convert numbers being passed between the Avaya SBCE and Session Manager.

To add an adaptation, under the **Routing** tab select **Adaptations** on the left-hand menu and then click on the **New** button (not shown). Under **Adaptation Details** → **General**:

- **Adaption Name:** Enter an appropriate name such as **VLBV**.
- **Module Name:** Select **DigitConversionAdapter**.
- **Modular Parameter Type:** Select **Name-Value Parameter**.

Click **Add** to add the name and value parameters.

- **Name:** Enter **fromto**. Modifies From and To header of a message.
- **Value:** Enter **true**.
- **Name:** Enter **MIME**. Removes MIME message bodies on egress from Session Manager.
- **Value:** Enter **no**.

Home / Elements / Routing / Adaptations

Adaptation Details

Commit Cancel

Help ?

General

* Adaptation Name: VLBV

Module Name: DigitConversionAdapter

Module Parameter Type: Name-Value Parameter

Add Remove

<input type="checkbox"/> Name	Value
<input type="checkbox"/> fromto	True
<input type="checkbox"/> MIME	no

Select : All, None

Egress URI Parameters:

Notes:

6.5. Administer SIP Entities

A SIP Entity must be added for each SIP-based telephony system supported by a SIP connection to Session Manager. To add a SIP Entity, select **SIP Entities** on the left panel menu and then click on the **New** button (not shown). The following will need to be entered for each SIP Entity.

Under **General**:

- In the **Name** field enter an informative name.
- In the **FQDN or IP Address** field enter the IP address of Session Manager or the signalling interface on the connecting system.
- In the **Type** field use **Session Manager** for a Session Manager SIP Entity, **Other** for a Communication Server 1000 SIP Entity and **SIP Trunk** for the Avaya SBCE SIP Entities.
- In the **Location** field select the appropriate location from the drop-down menu.
- In the **Time Zone** field enter the time zone for the SIP Entity.

In this configuration there are four SIP Entities.

- Session Manager SIP Entity.
- Communication Server 1000 SIP Entity.
- Avaya SBCE Fixed SIP Entity.
- Avaya SBCE Mobile SIP Entity.

6.5.1. Avaya Aura® Session Manager SIP Entity

The following screens show the SIP entity for Session Manager. The **FQDN or IP Address** field is set to the IP address of the Session Manager SIP signalling interface and **Type** is **Session Manager**. Set the **Location** to that defined in **Section 6.3** and the **Time Zone** to the appropriate time.

The screenshot shows the 'SIP Entity Details' form for 'Session Manager'. The form is divided into two sections: 'General' and 'SIP Link Monitoring'. In the 'General' section, the 'Name' is 'Session Manager', 'FQDN or IP Address' is '10.10.3.55', 'Type' is 'Session Manager', 'Notes' is empty, 'Location' is 'SMGRVL3', 'Outbound Proxy' is empty, 'Time Zone' is 'Europe/Dublin', and 'Credential name' is empty. In the 'SIP Link Monitoring' section, 'SIP Link Monitoring' is set to 'Use Session Manager Configuration'. There are 'Commit' and 'Cancel' buttons at the top right.

SIP Entity Details	
General	
* Name:	Session Manager
* FQDN or IP Address:	10.10.3.55
Type:	Session Manager
Notes:	
Location:	SMGRVL3
Outbound Proxy:	
Time Zone:	Europe/Dublin
Credential name:	
SIP Link Monitoring	
SIP Link Monitoring:	Use Session Manager Configuration

Session Manager must be configured with the port numbers on the protocols that will be used by the other SIP entities. To configure these scroll to the bottom of the page and under **Port**, click **Add**, then edit the fields in the resulting new row.

- In the **Port** field enter the port number on which the system listens for SIP requests.
- In the **Protocol** field enter the transport protocol to be used for SIP requests.
- In the **Default Domain** field, from the drop-down menu select the domain added in **Section 6.2** as the default domain.

The screenshot shows the 'Port' configuration section. It includes fields for 'TCP Failover port' and 'TLS Failover port', and 'Add' and 'Remove' buttons. Below is a table with 3 items, showing columns for 'Port', 'Protocol', 'Default Domain', and 'Notes'. The table contains three rows: TCP on 5060, TLS on 5061, and UDP on 5061, all with 'avaya.com' as the default domain. There is a 'Filter: Enable' button and a 'Select: All, None' option at the bottom.

Port	Protocol	Default Domain	Notes
5060	TCP	avaya.com	
5061	TLS	avaya.com	
5061	UDP	avaya.com	

6.5.2. Avaya Communication Server 1000 SIP Entity

The following screen shows the SIP entity for CS1000. The **FQDN or IP Address** field is set to the IP address of the interface on CS1000 that will be providing SIP signalling and **Type** is **Other**. Set the **Location** to that defined in **Section 6.3** and the **Time Zone** to the appropriate time.

The screenshot shows the 'SIP Entity Details' configuration page. At the top, there is a breadcrumb trail: 'Home / Elements / Routing / SIP Entities'. Below this, the page title 'SIP Entity Details' is followed by 'Commit' and 'Cancel' buttons. The 'General' tab is selected. The form contains the following fields and values:

- Name:** CS1K_7.6
- * FQDN or IP Address:** 10.10.9.21
- Type:** Other (dropdown menu)
- Notes:** (empty text area)
- Adaptation:** (empty dropdown menu)
- Location:** SM_7 (dropdown menu)
- Time Zone:** Europe/Dublin (dropdown menu)
- * SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text area)
- Securable:** (checkbox, unchecked)
- Call Detail Recording:** none (dropdown menu)
- CommProfile Type Preference:** (empty dropdown menu)
- Loop Detection:** (section header)
- Loop Detection Mode:** Off (dropdown menu)

Other parameters can be set for the SIP Entity as shown in the following screenshot, but for test, these were left at default values.

The screenshot shows the 'Loop Detection' and 'SIP Link Monitoring' configuration page. The 'Loop Detection' section has a 'Loop Detection Mode' dropdown menu set to 'Off'. The 'SIP Link Monitoring' section has a 'SIP Link Monitoring' dropdown menu set to 'Use Session Manager Configuration'.

6.5.3. Avaya Session Border Controller for Enterprise SIP Entity

The following screen shows the SIP entities for the Avaya SBCE used for routing Fixed and Mobile calls. The **FQDN or IP Address** field is set to the IP address of the private administered in **Section 7** of this document. Set **Type** to **SIP Trunk**. Set the **Location** to that defined in **Section 6.3**, set **Adaptation** to one created in **Section 6.4** and the **Time Zone** to the appropriate time zone.

The screenshot shows the 'SIP Entity Details' configuration page for a Fixed SIP entity. The breadcrumb navigation at the top is 'Home / Elements / Routing / SIP Entities'. The page title is 'SIP Entity Details' with 'Commit' and 'Cancel' buttons. The 'General' tab is selected. The configuration fields are as follows:

- Name:** Avaya_SBCE_Fixed
- FQDN or IP Address:** 10.10.3.30
- Type:** SIP Trunk (dropdown)
- Notes:** (empty text field)
- Adaptation:** VLBV (dropdown)
- Location:** SMGRVL3 (dropdown)
- Time Zone:** Europe/Dublin (dropdown)
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text field)
- Call Detail Recording:** egress (dropdown)
- Loop Detection Mode:** Off (dropdown)

The screenshot shows the 'SIP Entity Details' configuration page for a Mobile SIP entity. The breadcrumb navigation at the top is 'Home / Elements / Routing / SIP Entities'. The page title is 'SIP Entity Details' with 'Commit' and 'Cancel' buttons. The 'General' tab is selected. The configuration fields are as follows:

- Name:** Avaya_SBCE_Mobile
- FQDN or IP Address:** 10.10.3.35
- Type:** SIP Trunk (dropdown)
- Notes:** (empty text field)
- Adaptation:** VLBV (dropdown)
- Location:** SMGRVL3 (dropdown)
- Time Zone:** Europe/Dublin (dropdown)
- SIP Timer B/F (in seconds):** 4
- Credential name:** (empty text field)
- Call Detail Recording:** egress (dropdown)
- Loop Detection Mode:** Off (dropdown)

6.6. Administer Entity Links

A SIP trunk between a Session Manager and another system is described by an Entity Link. To add an Entity Link, select **Entity Links** on the left panel menu and click on the **New** button (not shown). Fill in the following fields in the new row that is displayed.

- In the **Name** field enter an informative name.
- In the **SIP Entity 1** field select **Session Manager**.
- In the **Protocol** field enter the transport protocol to be used to send SIP requests.
- In the **Port** field enter the port number to which the other system sends its SIP requests.
- In the **SIP Entity 2** field enter the other SIP Entity for this link, created in **Section 6.5**.
- In the **Port** field enter the port number to which the other system expects to receive SIP requests.
- Select **Trusted** from the drop-down menu to make the other system trusted.

Click **Commit** to save changes. The following screenshot shows the Entity Links used in this configuration.

Home / Elements / Routing / Entity Links [Help ?](#)

Entity Links

[New](#) [Edit](#) [Delete](#) [Duplicate](#) [More Actions](#)

4 Items [Filter: Enable](#)

<input type="checkbox"/>	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
<input type="checkbox"/>	Avaya_SBCE_Fixed	Session Manager	TCP	5060	Avaya_SBCE_Fixed	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	Avaya_SBCE_Mobile	Session Manager	TCP	5060	Avaya_SBCE_Mobile	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	CS1000	Session Manager	TCP	5060	CS1000	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	
<input type="checkbox"/>	Messaging	Session Manager	TCP	5060	Messaging	<input type="checkbox"/>	5060	trusted	<input type="checkbox"/>	

Select : All, None

6.7. Administer Routing Policies

Routing policies must be created to direct how calls will be routed to a system. To add a routing policy, select **Routing Policies** on the left panel menu and then click on the **New** button (not shown).

Under **General**:

- Enter an informative name in the **Name** field.
- Under **SIP Entity as Destination**, click **Select**, and then select the appropriate SIP entity to which this routing policy applies.
- Under **Time of Day**, click **Add**, and then select the time range.

The following screen shows the routing policy for CS1000.

The screenshot shows the 'Routing Policy Details' form for a policy named 'to_CS1000'. The form is divided into three main sections: General, SIP Entity as Destination, and Time of Day.

General Section:

- Name:** to_CS1000
- Disabled:** ☐
- Retries:** 0
- Notes:** (empty field)

SIP Entity as Destination Section:

- Select:** (button)
- | Name | FQDN or IP Address | Type | Notes |
|--------|--------------------|-----------|-------|
| CS1000 | 10.10.9.21 | SIP Trunk | |

Time of Day Section:

- Add** (button), **Remove** (button), **View Gaps/Overlaps** (button)
- 1 Item** (with refresh icon)
- Filter:** Enable

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
0	24/7	Mon Column Not sorted							00:00	23:59	Time Range 24/7

- Select:** All, None

The following screen shows the routing policy for Avaya SBCE for the Fixed trunk:

Home / Elements / Routing / Routing Policies Help ?

Routing Policy Details Commit Cancel

General

* Name: x

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Avaya_SBCE_Fixed	10.10.3.30	SIP Trunk	

Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

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

Select : All, None

The following screen shows the routing policy for Avaya SBCE for the Mobile trunk

Home / Elements / Routing / Routing Policies Help ?

Routing Policy Details Commit Cancel

General

* Name:

Disabled: ☐

* Retries:

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
Avaya_SBCE_Mobile	10.10.3.35	SIP Trunk	

Time of Day

Add Remove View Gaps/Overlaps

1 Item Filter: Enable

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

Select : All, None

6.8. Administer Dial Patterns

A dial pattern must be defined to direct calls to the appropriate telephony system. To configure a dial pattern, select **Dial Patterns** on the left panel menu and then click on the **New** button (not shown).

Under **General**:

- In the **Pattern** field enter a dialled number or prefix to be matched.
- In the **Min** field enter the minimum length of the dialled number.
- In the **Max** field enter the maximum length of the dialled number.
- In the **SIP Domain** field select **ALL** or alternatively one of those configured in **Section 6.2**.

Under **Originating Locations and Routing Policies**:

- Click **Add**, in the resulting screen (not shown).
- Under **Originating Location**, select the location defined in **Section 6.3** or **ALL**.
- Under **Routing Policies** select one of the routing policies defined in **Section 6.7**.
- Click **Select** button to save.

The following screen shows an example dial pattern configured for Vodafone Libertel Fixed SIP Trunk.

Home / Elements / Routing / Dial Patterns

Dial Pattern Details

Commit Cancel

General

* Pattern: 00

* Min: 2

* Max: 16

Emergency Call: ☐

Emergency Priority: 1

Emergency Type:

SIP Domain: avaya.com

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	SMGRVL3	to_AvayaSBCE_Fixed		0	<input type="checkbox"/>	Avaya_SBCE_Fixed	

Select : All, None

The following screen shows an example dial pattern configured for Vodafone Libertel Mobile SIP Trunk.

Home / Elements / Routing / Dial Patterns Help ?

Dial Pattern Details Commit Cancel

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	SMGRVL3		to_Avaya_SBCE_Mobile	0	<input type="checkbox"/>	Avaya_SBCE_Mobile	

Select : All, None

The following screen shows the test dial pattern configured for CS1000.

Home / Elements / Routing / Dial Patterns Help ?

Dial Pattern Details Commit Cancel

General

* Pattern:

* Min:

* Max:

Emergency Call: ☐

Emergency Priority:

Emergency Type:

SIP Domain:

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Filter: Enable

<input type="checkbox"/>	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	SMGRVL3		to_CS1000	0	<input type="checkbox"/>	CS1000	

Select : All, None

7. Configure Avaya Session Border Controller for Enterprise

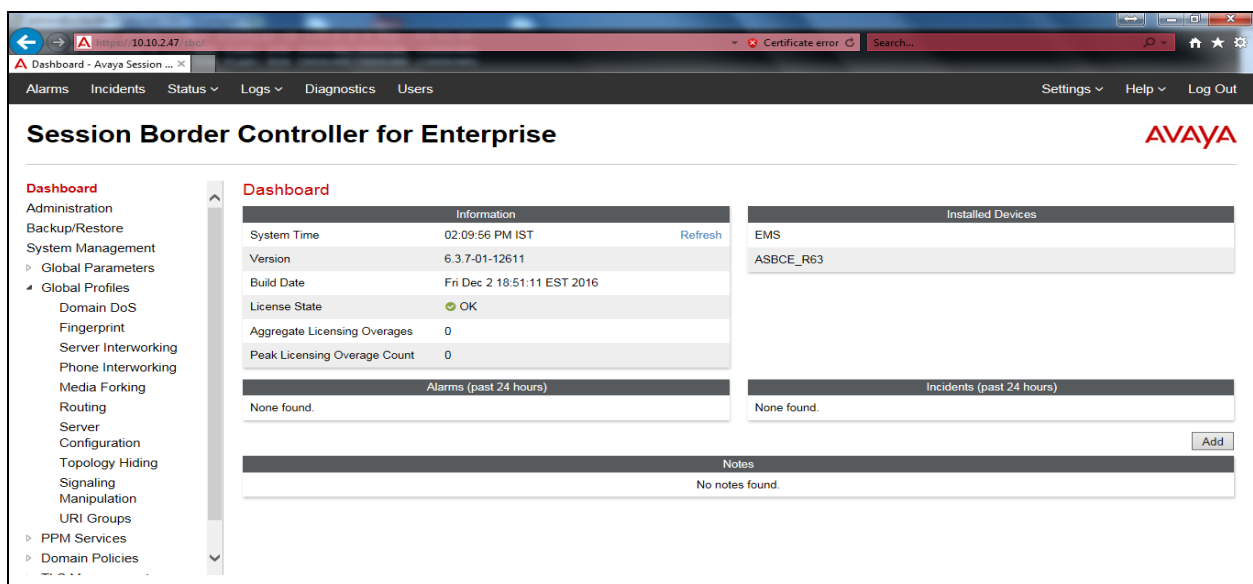
This section describes the configuration of the Session Border Controller for Enterprise (Avaya SBCE). The Avaya SBCE provides security and manipulation of signalling to provide an interface to the Service Provider's SIP Trunk that is standard where possible and adapted to the Service Provider's SIP implementation where necessary.

7.1. Access Avaya Session Border Controller for Enterprise

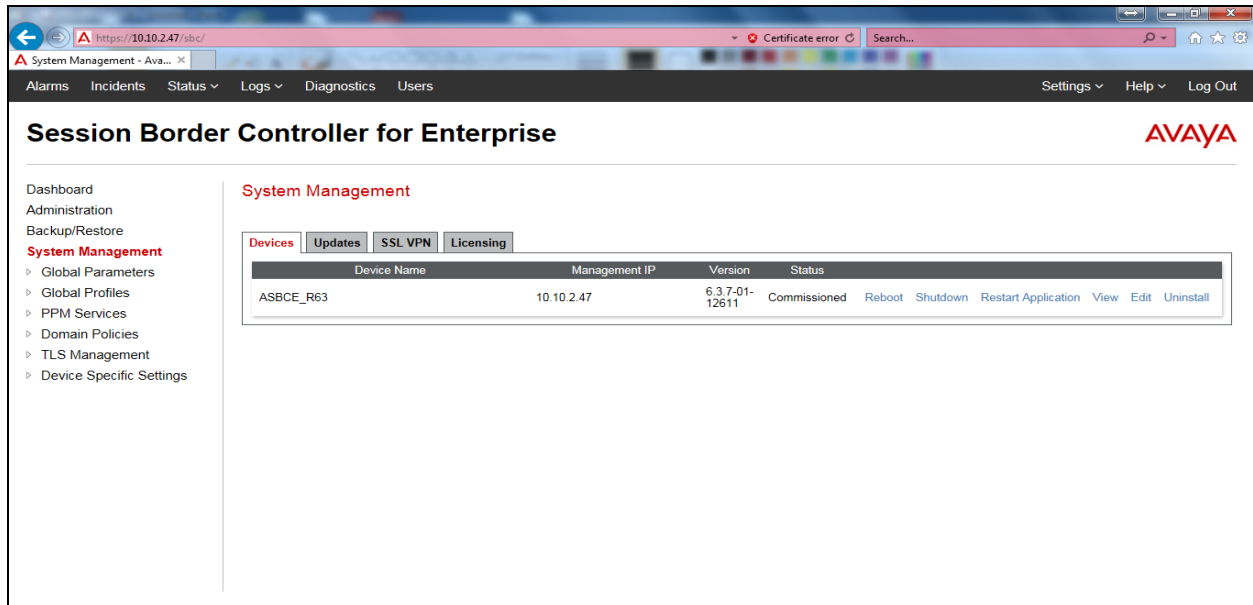
Access the Avaya SBCE using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation and enter the **Username** and **Password**.



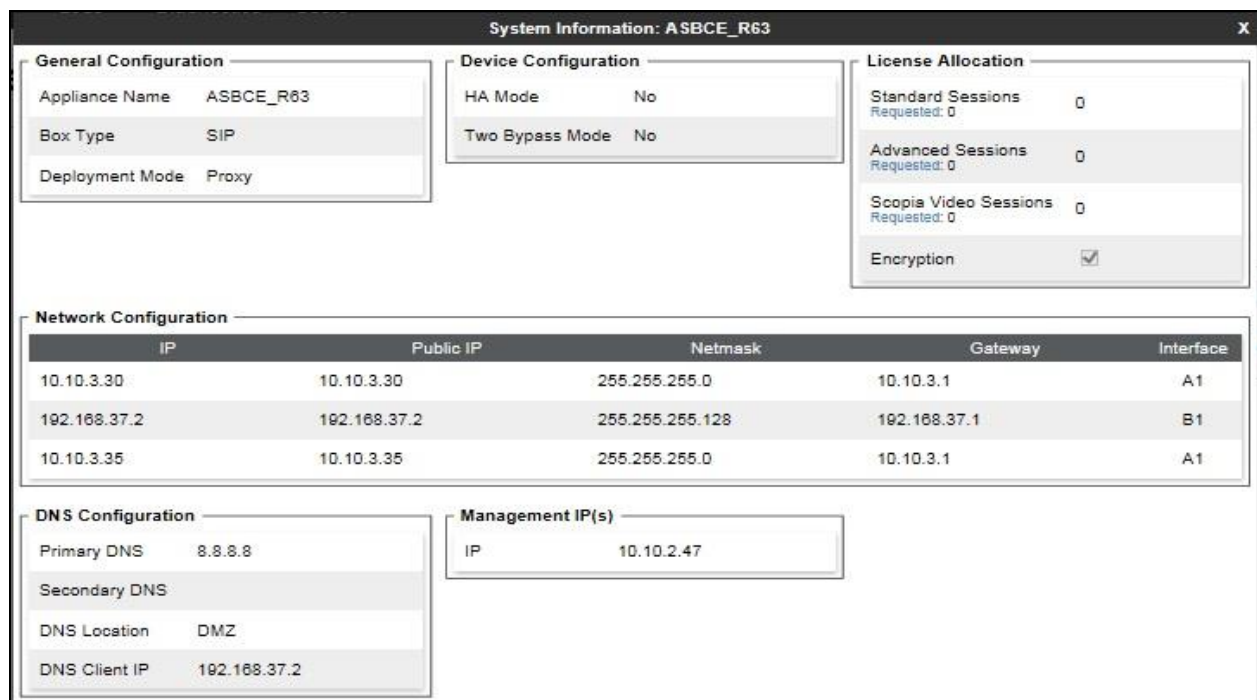
Once logged in, a dashboard is presented with a menu on the left-hand side. The menu is used as a starting point for all configuration of the Avaya SBCE.



To view system information that was configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named **ASBCE_R63** is shown. To view the configuration of this device, click **View** (the third option from the right).



The **System Information** screen shows the **General Configuration**, **Device Configuration**, **License Allocation**, **Network Configuration**, **DNS Configuration** and **Management IP** information.



7.2. Global Profiles

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

7.2.1. Server Interworking - Avaya

Server Interworking allows the configuration and management of various SIP call server-specific capabilities such as call hold and T.38. From the left-hand menu select **Global Profiles** →

Server Interworking and click on **Add**.

- Enter profile name such as **Avaya** and click **Next** (Not Shown).
- Check **Hold Support=None**.
- Check **T.38 Support**.
- All other options on the **General** Tab can be left at default.

Click on **Next** on the following screens and then **Finish**.

The screenshot shows the 'General' configuration tab for a new profile. The settings are as follows:

Setting	Value
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3284 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
URI Group	None
Send Hold	<input type="checkbox"/>
Delayed Offer	<input type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
Re-Invite Handling	<input type="checkbox"/>
Prack Handling	<input type="checkbox"/>
Allow 18X SDP	<input type="checkbox"/>
T.38 Support	<input checked="" type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3281 <input type="radio"/> RFC2543

Default values can be used for the **Advanced Settings** window. Click **Finish**.

Record Routes	<input type="radio"/> None <input type="radio"/> Single Side <input checked="" type="radio"/> Both Sides
Topology Hiding: Change Call-ID	<input type="checkbox"/>
Call-Info NAT	<input type="checkbox"/>
Change Max Forwards	<input checked="" type="checkbox"/>
Include End Point IP for Context Lookup	<input type="checkbox"/>
OCS Extensions	<input type="checkbox"/>
AVAYA Extensions	<input type="checkbox"/>
NORTEL Extensions	<input type="checkbox"/>
Diversion Manipulation	<input type="checkbox"/>
Diversion Header URI	<input type="text"/>
Metaswitch Extensions	<input type="checkbox"/>
Reset on Talk Spurt	<input type="checkbox"/>
Reset SRTP Context on Session Refresh	<input type="checkbox"/>
Has Remote SBC	<input checked="" type="checkbox"/>
Route Response on Via Port	<input type="checkbox"/>
Cisco Extensions	<input type="checkbox"/>
Lync Extensions	<input type="checkbox"/>
SBC FQDN	<input type="text"/>

7.2.2. Server Interworking – Vodafone Libertel B.V.

Server Interworking allows the configuration and management of various SIP call server-specific capabilities such as call hold and T.38. From the left-hand menu select **Global Profiles** → **Server Interworking** and click on **Add**.

- Enter profile name such as **VLBV** and click **Next** (Not Shown).
- Check **Hold Support** = **None**.
- Check **T.38 Support**.
- All other options on the **General** Tab can be left at default.

Click on **Next** on the following screens and then **Finish**.

General	
Hold Support	<input checked="" type="radio"/> None <input type="radio"/> RFC2543 - c=0.0.0.0 <input type="radio"/> RFC3284 - a=sendonly
180 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
181 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
182 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
183 Handling	<input checked="" type="radio"/> None <input type="radio"/> SDP <input type="radio"/> No SDP
Refer Handling	<input type="checkbox"/>
URI Group	None
Send Hold	<input type="checkbox"/>
Delayed Offer	<input type="checkbox"/>
3xx Handling	<input type="checkbox"/>
Diversion Header Support	<input type="checkbox"/>
Delayed SDP Handling	<input type="checkbox"/>
Re-Invite Handling	<input type="checkbox"/>
Prack Handling	<input type="checkbox"/>
Allow 18X SDP	<input type="checkbox"/>
T.38 Support	<input checked="" type="checkbox"/>
URI Scheme	<input checked="" type="radio"/> SIP <input type="radio"/> TEL <input type="radio"/> ANY
Via Header Format	<input checked="" type="radio"/> RFC3281 <input type="radio"/> RFC2543

Default values can be used for the **Advanced Settings** window. Click **Finish**.

Record Routes	<input type="radio"/> None <input type="radio"/> Single Side <input checked="" type="radio"/> Both Sides
Topology Hiding: Change Call-ID	<input type="checkbox"/>
Call-Info NAT	<input type="checkbox"/>
Change Max Forwards	<input checked="" type="checkbox"/>
Include End Point IP for Context Lookup	<input type="checkbox"/>
OCS Extensions	<input type="checkbox"/>
AVAYA Extensions	<input type="checkbox"/>
NORTEL Extensions	<input type="checkbox"/>
Diversion Manipulation	<input type="checkbox"/>
Diversion Header URI	<input type="text"/>
Metaswitch Extensions	<input type="checkbox"/>
Reset on Talk Spurt	<input type="checkbox"/>
Reset SRTP Context on Session Refresh	<input type="checkbox"/>
Has Remote SBC	<input checked="" type="checkbox"/>
Route Response on Via Port	<input type="checkbox"/>
Cisco Extensions	<input type="checkbox"/>
Lync Extensions	<input type="checkbox"/>
SBC FQDN	<input type="text"/>

7.2.3. Server Configuration – Avaya

Servers are defined for each server connected to the Avaya SBCE. In this case, Vodafone Libertel is connected as the Trunk Server and Session Manager is connected as the Call Server. The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow administrator to configure and manage various SIP call server-specific parameters such as TCP and UDP port assignments, IP Server type, heartbeat signalling parameters and some advanced options.

From the left-hand menu select **Global Profiles → Server Configuration** and click on **Add** and enter a descriptive name. On the **Add Server Configuration Profile** tab, set the following:

- Select **Server Type** to be **Call Server**.
- Enter **IP Address / FQDN** to **10.10.3.55** (Session Manager IP Address).
- For **Port**, enter **5060**.
- For **Transport**, select **TCP**.
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs.

IP Address / FQDN	Port	Transport
10.10.3.55	5060	TCP

On the **Advanced** tab:

- Select **Avaya** for **Interworking Profile** defined in **Section 7.2.1**.
- Click **Finish**.

Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input checked="" type="checkbox"/>
Interworking Profile	Avaya
Signaling Manipulation Script	None
Connection Type	SUBID

7.2.4. Server Configuration – Vodafone Libertel B.V.

To define Vodafone Libertel as two separate Trunk Servers for the fixed and mobile networks, navigate to **Global Profiles → Server Configuration** and click on **Add** and enter a descriptive name. On the **Add Server Configuration Profile** tab, set the following:

- Select **Server Type** to be **Trunk Server**.
- Enter **IP Address / FQDN** to **62.140.159.241** (Vodafone Libertel Fixed network).
- For **Port**, enter **5060**.
- For **Transport**, select **UDP**.
- Click **Next** to continue (not shown).

Server Configuration Profile - General

Server Type can not be changed while this Server Configuration profile is associated to a Server Flow.

Server Type: Trunk Server

SIP Domain:

DNS Query Type: NONE/A

TLS Client Profile: None

Add

IP Address / FQDN	Port	Transport
62.140.159.241	5060	UDP

Delete

On the Advanced tab:

- Check **Enable Grooming**.
- Select **VLBV** for Interworking Profile defined in **Section 7.2.2**.
- Click **Finish**.

Server Configuration Profile - Advanced

Enable DoS Protection: ☐

Enable Grooming: ☒

Interworking Profile: VLBV

Signaling Manipulation Script: None

Connection Type: SUBID

Finish

To define the Vodafone Libertel Mobile trunk server, navigate to **Global Profiles → Server Configuration** and click on **Add** and enter a descriptive name. On the **Add Server Configuration Profile** tab, set the following:

- Select **Server Type** to be **Trunk Server**.
- Enter **IP Address / FQDN** to **62.140.159.242** (Vodafone Libertel Mobile network).
- For **Port**, enter **5060**.
- For **Transport**, select **UDP**.
- Click **Next** to continue (not shown).

Server Configuration Profile - General

Server Type can not be changed while this Server Configuration profile is associated to a Server Flow.

Server Type: Trunk Server

SIP Domain:

DNS Query Type: NONE/A

TLS Client Profile: None

Add

IP Address / FQDN	Port	Transport
62.140.159.242	5060	UDP

Delete

On the Advanced tab:

- Check **Enable Grooming**.
- Select **VLBV** for Interworking Profile defined in **Section 7.2.2**.
- Click **Finish**.

Server Configuration Profile - Advanced

Enable DoS Protection: ☐

Enable Grooming: ☒

Interworking Profile: VLBV

Signaling Manipulation Script: None

Connection Type: SUBID

Finish

7.2.5. Routing

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

Routing information is required for routing to Session Manager on the internal side and Vodafone Libertel addresses on the external side. The IP addresses and ports defined here will be used as the destination addresses for signalling. If no port is specified in the **Next Hop IP Address**, default 5060 is used.

7.2.5.1 Routing – Avaya

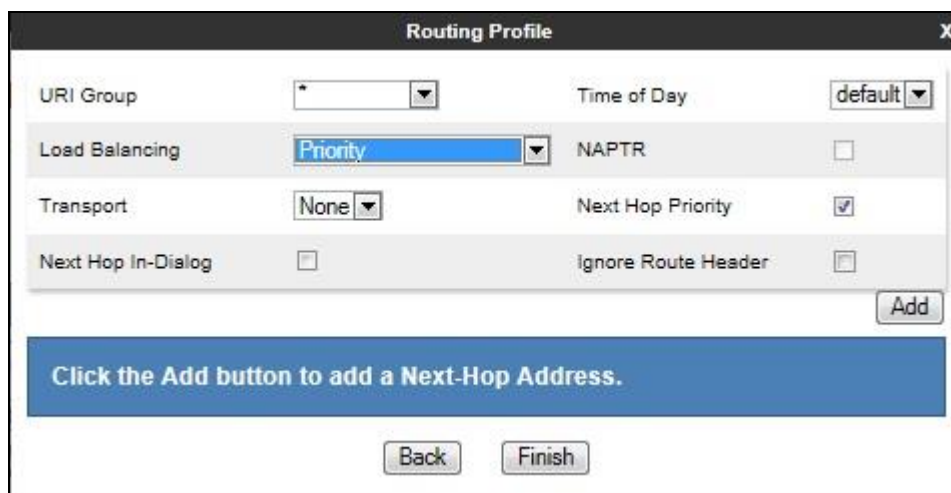
Create a Routing Profile for Session Manager.

- Navigate to **Global Profiles → Routing** and select **Add Profile**.
- Enter a **Profile Name** and click **Next**.



The image shows a 'Routing Profile' window. It has a title bar with 'Routing Profile' and a close button 'X'. Inside, there is a text field labeled 'Profile Name' containing the text 'Avaya'. Below the text field is a button labeled 'Next'.

The Routing Profile window will open. Use the default values displayed and click **Add**.



The image shows a 'Routing Profile' window with various settings. The title bar has 'Routing Profile' and a close button 'X'. The settings are as follows:

URI Group	Time of Day
*	default
Load Balancing	NAPTR
Priority	<input type="checkbox"/>
Transport	Next Hop Priority
None	<input checked="" type="checkbox"/>
Next Hop In-Dialog	Ignore Route Header
<input type="checkbox"/>	<input type="checkbox"/>

Below the settings is an 'Add' button. At the bottom, there is a blue box with the text 'Click the Add button to add a Next-Hop Address.' and two buttons: 'Back' and 'Finish'.

On the **Next Hop Address** window, set the following:

- **Priority/Weight = 1.**
- **Server Configuration = Avaya** (Section 7.2.3) from drop down menu.
- **Next Hop Address = Select 10.10.3.55:5060 TCP** from drop down menu.
- Click **Finish**.

Priority / Weight	Server Configuration	Next Hop Address	Transport
1	Avaya	10.10.3.55:5060 (TCP)	None

7.2.5.2 Routing – Vodafone Libertel B.V.

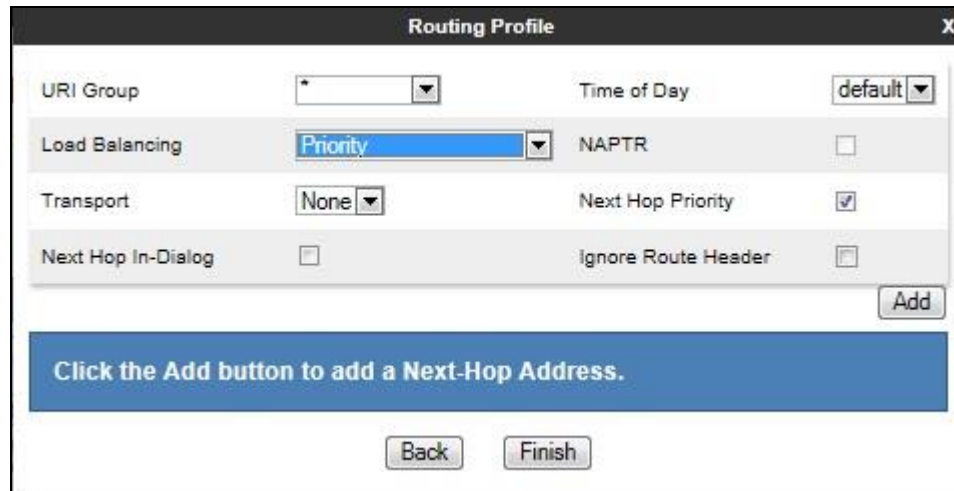
Create a Routing Profile for Vodafone Libertel Fixed network.

- Navigate to **Global Profiles → Routing** and select **Add Profile**.
- Enter a **Profile Name** and click **Next**.

Profile Name: VLBV_Fixed

Next

The Routing Profile window will open. Use the default values displayed and click **Add**.

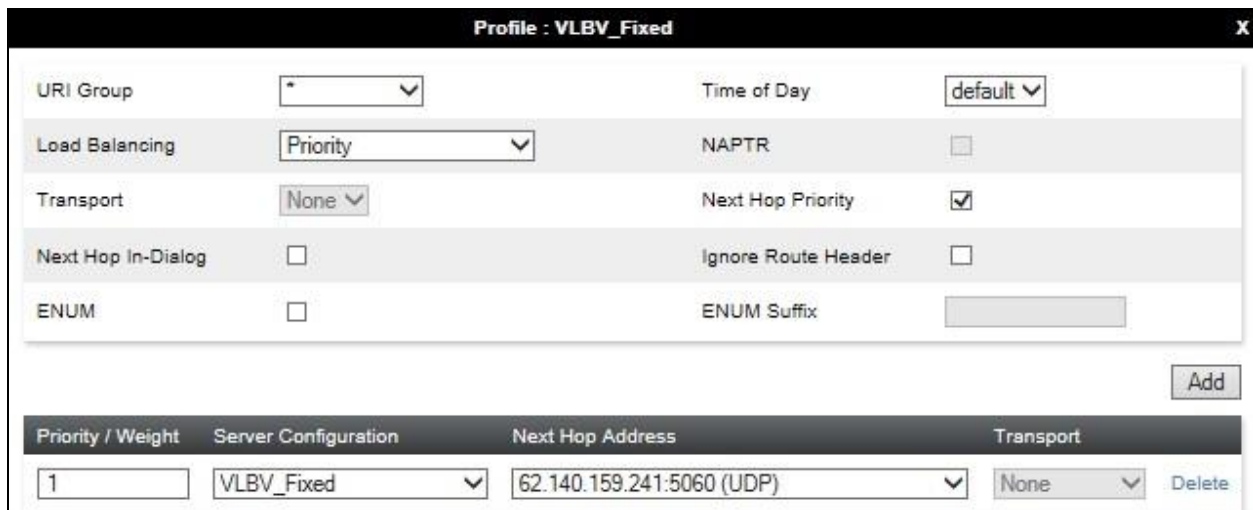


The screenshot shows the 'Routing Profile' window. It contains the following fields and controls:

- URI Group:** A dropdown menu with an asterisk (*) as the selected value.
- Time of Day:** A dropdown menu with 'default' as the selected value.
- Load Balancing:** A dropdown menu with 'Priority' as the selected value.
- NAPTR:** An unchecked checkbox.
- Transport:** A dropdown menu with 'None' as the selected value.
- Next Hop Priority:** A checked checkbox.
- Next Hop In-Dialog:** An unchecked checkbox.
- Ignore Route Header:** An unchecked checkbox.
- Add:** A button located at the bottom right of the configuration area.
- Instruction:** A blue banner with the text 'Click the Add button to add a Next-Hop Address.'
- Back:** A button at the bottom center.
- Finish:** A button at the bottom right, next to the Back button.

On the **Next Hop Address** window, set the following:

- **Priority/Weight = 1.**
- **Server Configuration = VLBV_Fixed** (Section 7.2.4) from drop down menu.
- **Next Hop Address = Select 62.140.159.241:5060 UDP** from drop down menu.
- Click **Finish**.



The screenshot shows the 'Profile : VLBV_Fixed' window. It contains the following fields and controls:

- URI Group:** A dropdown menu with an asterisk (*) as the selected value.
- Time of Day:** A dropdown menu with 'default' as the selected value.
- Load Balancing:** A dropdown menu with 'Priority' as the selected value.
- NAPTR:** An unchecked checkbox.
- Transport:** A dropdown menu with 'None' as the selected value.
- Next Hop Priority:** A checked checkbox.
- Next Hop In-Dialog:** An unchecked checkbox.
- Ignore Route Header:** An unchecked checkbox.
- ENUM:** An unchecked checkbox.
- ENUM Suffix:** An empty text input field.
- Add:** A button located at the bottom right of the configuration area.
- Table:** A table with the following columns: Priority / Weight, Server Configuration, Next Hop Address, Transport, and a Delete button.

Priority / Weight	Server Configuration	Next Hop Address	Transport	
1	VLBV_Fixed	62.140.159.241:5060 (UDP)	None	Delete

Create a Routing Profile for Vodafone Libertel Mobile network.

- Navigate to **Global Profiles → Routing** and select **Add Profile**.
- Enter a **Profile Name** and click **Next**.

The screenshot shows a window titled "Routing Profile" with a close button (X) in the top right corner. Inside the window, there is a text input field labeled "Profile Name" containing the text "VLBV_Mobile". Below this field is a button labeled "Next".

The Routing Profile window will open. Use the default values displayed and click **Add**.

The screenshot shows the "Routing Profile" window with various configuration options. The "URI Group" is set to "*", "Time of Day" is "default", "Load Balancing" is "Priority", "Transport" is "None", "Next Hop In-Dialog" is unchecked, "NAPTR" is unchecked, "Next Hop Priority" is checked, and "Ignore Route Header" is unchecked. There is an "Add" button at the bottom right. Below the configuration fields is a blue banner with the text "Click the Add button to add a Next-Hop Address." At the very bottom are "Back" and "Finish" buttons.

On the **Next Hop Address** window, set the following:

- **Priority/Weight** = 1.
- **Server Configuration** = **VLBV_Mobile** (Section 7.2.4) from drop down menu.
- **Next Hop Address** = Select **62.140.159.242:5060 UDP** from drop down menu.
- Click **Finish**.

The screenshot shows the "Profile : VLBV_Mobile" window. It contains the same configuration options as the previous window. Below these options is a table with the following columns: "Priority / Weight", "Server Configuration", "Next Hop Address", "Transport", and "Delete". The table has one row with the following values: "1", "VLBV_Mobile", "62.140.159.242:5060 (UDP)", "None", and a "Delete" button. There is also an "Add" button at the bottom right of the configuration area.

7.2.6. Topology Hiding

Topology hiding is used to hide local information such as private IP addresses and local domain names. The local information can be overwritten with a domain name or IP addresses. The default **Replace Action** is **Auto**, this replaces local information with IP addresses, generally the next hop. Topology hiding has the advantage of presenting single Via and Record-Route headers externally where multiple headers may be received from the enterprise, particularly from Session Manager. In some cases where Topology Hiding can't be applied, in particular the Contact header, IP addresses are translated to the Avaya SBCE external addresses using NAT.

To define Topology Hiding for Session Manager, navigate to **Global Profiles → Topology Hiding** from menu on the left-hand side. Click on **Add** and enter details in the **Topology Hiding Profile** pop-up menu (not shown).

- Enter a descriptive Profile Name such as **Avaya**.
- If the required Header is not shown, click on **Add Header**.
- Under the **Header** field for **To**, **From** and **Request Line**, select **IP/Domain** under **Criteria** and **Overwrite** under **Replace Action**. For Overwrite value, insert **avaya.com**.
- Click **Finish** (not shown).

Topology Hiding Profiles: Avaya

Add

Topology Hiding Profiles

default

cisco_th_profile

Avaya

VLBV

RenameCloneDelete

Click here to add a description.

Topology Hiding

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

Edit

To define Topology Hiding for Vodafone Libertel, navigate to **Global Profiles → Topology Hiding** from the menu on the left-hand side. Click on **Add** and enter details in the **Topology Hiding Profile** pop-up menu (not shown).

- In the **Profile Name** field enter a descriptive name for Vodafone Libertel and click **Next**.
- If the required Header is not shown, click on **Add Header**.
- Under the **Header** field for **To**, **From** and **Request Line**, select **IP/Domain** under **Criteria** and **Auto** under **Replace Action**.
- Click **Finish** (not shown).

Topology Hiding Profiles: VLBV

Add

Topology Hiding Profiles

default

cisco_th_profile

Avaya

VLBV

Rename
Clone
Delete

Click here to add a description.

Topology Hiding

Header	Criteria	Replace Action	Overwrite Value
Record-Route	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
From	IP/Domain	Auto	---
Via	IP/Domain	Auto	---
To	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---
Request-Line	IP/Domain	Auto	---
SDP	IP/Domain	Auto	---

Edit

7.3. Define Network Information

Network information is required on the Avaya SBCE to allocate IP addresses and masks to the interfaces. Note that only the **A1** and **B1** interfaces are used, typically the **A1** interface is used for the internal side and **B1** is used for external. Each side of the Avaya SBCE can have only one interface assigned.

To define the network information, navigate to **Device Specific Settings → Network Management** from the menu on the left-hand side and click on **Add**. Enter details in the blank box that appears at the end of the list

- Define the two internal IP address with subnet mask and assign to interface **A1**.
- Select **Save** to save the information.
- Click on **Add**.
- Define the external IP address with subnet mask and assign to interface **B1**.
- Select **Save** to save the information.
- Click on **System Management** in the main menu.
- Select **Restart Application** indicated by an icon in the status bar (not shown).

Note: Multiple IP addresses defined on a single interface must be in the same subnet.

Network Management: ASBCE_R63

Devices | **Interfaces** | Networks

ASBCE_R63

Add

Name	Gateway	Subnet Mask	Interface	IP Address	
A1_Internal	10.10.3.1	255.255.255.0	A1	10.10.3.30, 10.10.3.35	Edit Delete
B1_External	192.168.37.1	255.255.255.128	B1	192.168.37.2	Edit Delete

Select the **Interface Configuration** tab and click on **Toggle State** to enable the interfaces.

Network Management: ASBCE_R63

Devices | **Interfaces** | Networks

ASBCE_R63

Add VLAN

Interface Name	VLAN Tag	Status
A1		Enabled
A2		Disabled
B1		Enabled
B2		Disabled

7.4. Define Interfaces

When the IP addresses and masks are assigned to the interfaces, these are then configured as signalling and media interfaces.

7.4.1. Signalling Interfaces

To define the signalling interfaces on the Avaya SBCE, navigate to **Device Specific Settings** → **Signaling Interface** from the menu on the left-hand side. Details of transport protocol and ports for the internal and external SIP signalling are entered here.

To enter details of transport protocol and ports for the SIP signalling on the internal interface:

- Select **Add** and enter details of the internal signalling interface in the pop-up menu (not shown).
- In the **Name** field enter a descriptive name for the internal interface.
- For **IP Address**, select the **A1_Internal** signalling interface IP addresses defined in **Section 7.3**.
- Select **TCP** port number, **5060** is used for Session Manager.

Repeat this process for the internal signalling interface for the Vodafone Libertel Mobile network.

To enter details of transport protocol and ports for the SIP signalling on the external interface:

- Select **Add** and enter details of the external signalling interface in the pop-up menu (not shown).
- In the **Name** field enter a descriptive name for the external signalling interface.
- For **IP Address**, select the **B1_external** signalling interface IP address defined in **Section 7.3**.
- Select **UDP** port number, **5060** is used for Vodafone Libertel.

Signaling Interface: ASBCE_R63

Devices

ASBCE_R63

Signaling Interface

Modifying or deleting an existing signaling interface will require an application restart before taking effect. Application restarts can be issued from System Management.

Add

Name	Signaling IP Network	TCP Port	UDP Port	TLS Port	TLS Profile	
Int_Sig_Fixed	10.10.3.30 A1_Internal (A1, VLAN 0)	5060	---	---	None	Edit Delete
Ext_Sig	192.168.37.2 B1_External (B1, VLAN 0)	---	5060	---	None	Edit Delete
Int_Sig_Mobile	10.10.3.35 A1_Internal (A1, VLAN 0)	5060	---	---	None	Edit Delete

7.4.2. Media Interfaces

To define the media interfaces on the Avaya SBCE, navigate to **Device Specific Settings** → **Media Interface** from the menu on the left-hand side. Details of the RTP and SRTP port ranges for the internal and external media streams are entered here. The IP addresses for media can be the same as those used for signalling.

To enter details of the media IP and RTP port range on the internal interface to be used in the server flow:

- Select **Add Media Interface** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the internal media interface.
- For **IP Address**, select the **A1_Internal** media interface IP address defined in **Section 7.3**.
- Select **RTP port** ranges for the media path with the enterprise end-points.

Repeat this process for the internal media interface for the Vodafone Libertel Mobile network.

To enter details of the media IP and RTP port range on the external interface to be used in the server flow.

- Select **Add Media Interface** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the external media interface.
- For **IP Address**, select the **A1_Internal** media interface IP address defined in **Section 7.3**.
- Select **RTP port** ranges for the external media path.

The following screen shows the Media Interfaces created in the sample configuration for the inside and outside IP interfaces.

Media Interface: ASBCE_R63

Devices

ASBCE_R63

Media Interface

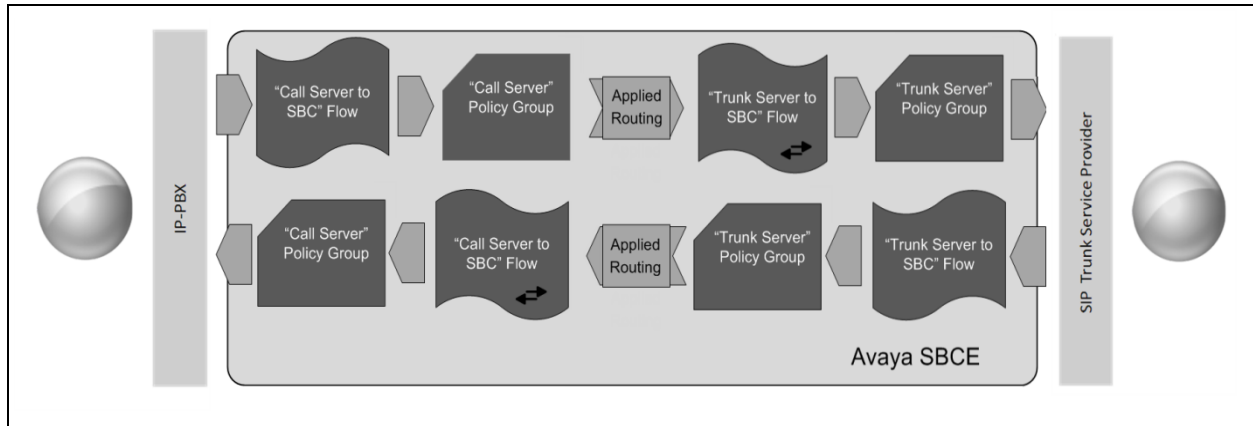
Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.

Add

Name	Media IP Network	Port Range	
Int_Media_Fixed	10.10.3.30 A1_Internal (A1, VLAN 0)	35000 - 40000	Edit Delete
Ext_Media	192.168.37.2 B1_External (B1, VLAN 0)	35000 - 40000	Edit Delete
Int_Media_Mobile	10.10.3.35 A1_Internal (A1, VLAN 0)	35000 - 40000	Edit Delete

7.5. Server Flows

Server Flows combine the previously defined profiles into outgoing flows from Session Manager to Vodafone Libertel's SIP Trunk and incoming flows from Vodafone Libertel's SIP Trunk to Session Manager. The following screen illustrates the flow through the Avaya SBCE to secure a SIP Trunk call.



Two server flows are required for outgoing traffic and two are required for incoming. This is so that traffic can be routed to both the Fixed and Mobile networks and can also be received from both Fixed and Mobile networks. This configuration ties all the previously entered information together so that calls can be routed from Session Manager to Vodafone Libertel SIP Trunk service and vice versa. The following screenshot shows all configured flows.

Subscriber Flows

Server Flows

Add

Click here to add a row description.

Server Configuration: Avaya

Update

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	Call_Server_Fixed	*	Ext_Sig	Int_Sig_Fixed	default-low	VLBV_Fixed	View	Clone	Edit	Delete
2	Call_Server_Mobile	*	Ext_Sig	Int_Sig_Mobile	default-low	VLBV_Mobile	View	Clone	Edit	Delete

Server Configuration: VLBV_Fixed

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	Trunk_Server_Fixed	*	Int_Sig_Fixed	Ext_Sig	default-low	Avaya	View	Clone	Edit	Delete

Server Configuration: VLBV_Mobile

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	Trunk_Server_Mobile	*	Int_Sig_Mobile	Ext_Sig	default-low	Avaya	View	Clone	Edit	Delete

To define a Server Flow for the Vodafone Libertel SIP Trunk, navigate to **Device Specific Settings → End Point Flows**.

- Click on the **Server Flows** tab.
- Select **Add Flow** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the server flow for Vodafone Libertel Fixed SIP Trunk, in the test environment **Trunk_Server_Fixed** was used.
- In the **Server Configuration** drop down menu, select the Server defined in **Section 7.2.4** for the Vodafone Libertel Fixed network.
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.4.1**.
- In the **Signalling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.4.1**.
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.4.2**.
- In the **Routing Profile** drop-down menu, select the routing profile of Session Manager defined in **Section 7.2.5**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the Vodafone Libertel SBC defined in **Section 7.2.6**.

Click **Finish** to save and exit.

The screenshot shows a dialog box titled "View Flow: Trunk_Server_Fixed" with a close button (X) in the top right corner. The dialog is divided into two main sections: "Criteria" and "Profile".

Criteria	
Flow Name	Trunk_Server_Fixed
Server Configuration	VLBV_Fixed
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Int_Sig_Fixed

Profile	
Signaling Interface	Ext_Sig
Media Interface	Ext_Media
End Point Policy Group	default-low
Routing Profile	Avaya
Topology Hiding Profile	VLBV
File Transfer Profile	None
Signaling Manipulation Script	None
Remote Branch Office	Any

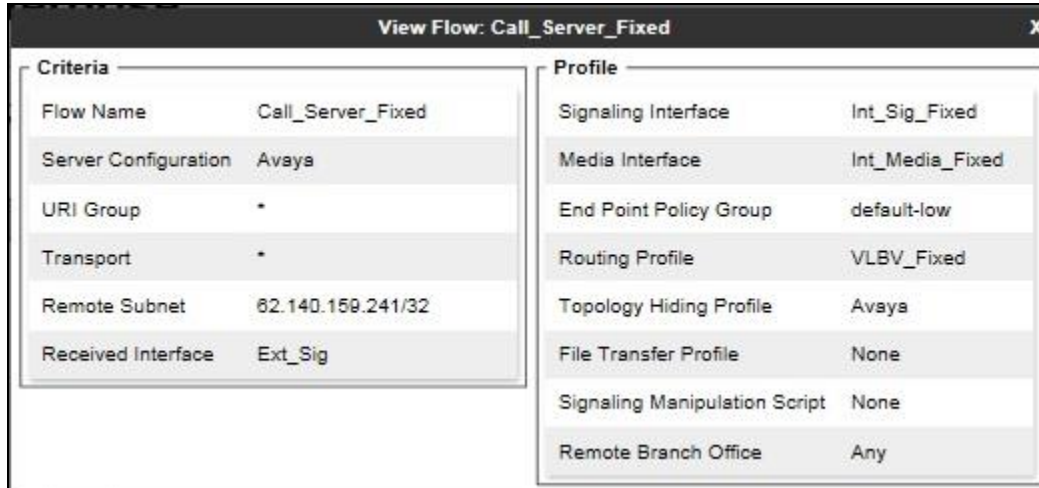
Repeat the process for an outgoing server flow for the Mobile network. The following screenshot is a view of the completed configuration Vodafone Libertel server flow for the Mobile SIP Trunk:

View Flow: Trunk_Server_Mobile			
Criteria		Profile	
Flow Name	Trunk_Server_Mobile	Signaling Interface	Ext_Sig
Server Configuration	VLBV_Mobile	Media Interface	Ext_Media
URI Group	*	End Point Policy Group	default-low
Transport	*	Routing Profile	Avaya
Remote Subnet	*	Topology Hiding Profile	VLBV
Received Interface	Int_Sig_Mobile	File Transfer Profile	None
		Signaling Manipulation Script	None
		Remote Branch Office	Any

To define an incoming server flow for Session Manager from the Fixed network, navigate to **Device Specific Settings → End Point Flows**.

- Click on the **Server Flows** tab.
- Select **Add Flow** and enter details in the pop-up menu.
- In the **Name** field enter a descriptive name for the server flow for Session Manager, in the test environment **Call_Server_Fixed** was used.
- In the **Server Configuration** drop down menu, select the Server defined in **Section 7.2.3** for Session Manager.
- In the **Remote Subnet** field, insert the Vodafone Libertel Fixed network IP address with subnet, **62.140.159.241/32** as per screenshot below.
- In the **Received Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3**.
- In the **Signalling Interface** drop-down menu, select the internal SIP signalling defined in **Section 7.4.1**.
- In the **Media Interface** drop-down menu, select the internal media interface defined in **Section 7.4.2**.
- In the **Routing Profile** drop-down menu, select the routing profile of the Vodafone Libertel Fixed SIP trunk defined in **Section 7.2.5**.
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of Session Manager defined in **Section 7.2.6**.

Click **Finish** to save and exit.



View Flow: Call_Server_Fixed	
Criteria	
Flow Name	Call_Server_Fixed
Server Configuration	Avaya
URI Group	*
Transport	*
Remote Subnet	62.140.159.241/32
Received Interface	Ext_Sig
Profile	
Signaling Interface	Int_Sig_Fixed
Media Interface	Int_Media_Fixed
End Point Policy Group	default-low
Routing Profile	VLBV_Fixed
Topology Hiding Profile	Avaya
File Transfer Profile	None
Signaling Manipulation Script	None
Remote Branch Office	Any

Repeat the process for an incoming Session Manager server flow for the Mobile network. The following screenshot is a view of the completed configuration Session Manager server flow for the Mobile SIP Trunk:

View Flow: Call_Server_Mobile			
Criteria		Profile	
Flow Name	Call_Server_Mobile	Signaling Interface	Int_Sig_Mobile
Server Configuration	Avaya	Media Interface	Int_Media_Mobile
URI Group	*	End Point Policy Group	default-low
Transport	*	Routing Profile	VLBV_Mobile
Remote Subnet	62.140.159.242/32	Topology Hiding Profile	Avaya
Received Interface	Ext_Sig	File Transfer Profile	None
		Signaling Manipulation Script	None
		Remote Branch Office	Any

8. Configure Vodafone Libertel B.V. SIP Trunk Equipment

The configuration of the Vodafone Libertel equipment used to support Vodafone Libertel's SIP Trunk is outside of the scope of these Application Notes and will not be covered. To obtain further information on Vodafone Libertel equipment and system configuration please contact an authorized Vodafone Libertel B.V. representative.

9. Verification Steps

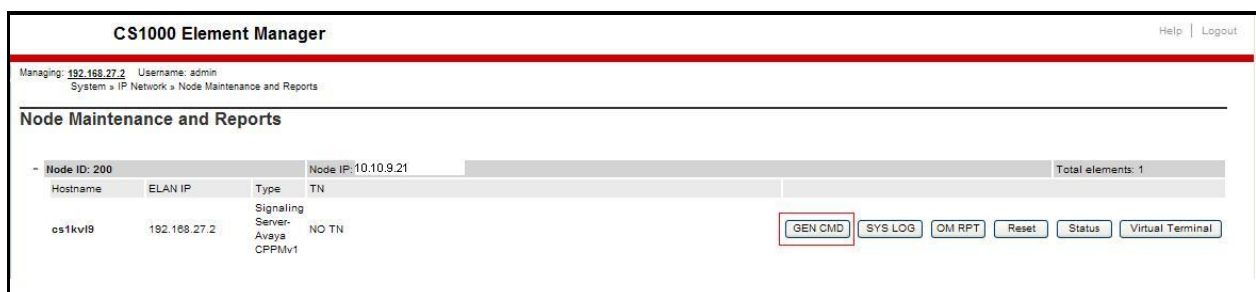
This section provides verification steps that may be performed in the field to verify that the solution is configured properly.

9.1. Avaya Communication Server 1000 Verification

This section illustrates sample verifications that may be performed using the Avaya CS1000 Element Manager GUI.

9.1.1. IP Network Maintenance and Reports Commands

From Element Manager, navigate to **System → IP Network → Maintenance and Reports** as shown below. In the resultant screen on the right, click the **Gen CMD** button.



The **General Commands** page is displayed. A variety of commands are available by selecting an appropriate Group and Command from the drop-down menus and selecting **Run**.

To check the status of the SIP Gateway to Session Manager in the sample configuration, select **Sip** from the Group menu and **SIPGwShow** from the **Command** menu. Click **Run**. The example output below shows that Session Manager has **SIPNPM Status “Active”**.

Managing: 192.168.27.2 Username: admin
System > IP Network > Node Maintenance and Reports > General Commands

General Commands

Element IP : 192.168.27.2 Element Type : Signaling Server-Avaya CPPMv1

Group: **Sip** Command: **SIPGwShow** SIP: **Sip** **RUN**

IP address: 192.168.27.2 Number of pings: 3 **PING**

```

SIPGWM Status : Active
Primary Proxy IP address : 10.10.3.55
Primary Proxy port : 5060
Primary Proxy Transport : TCP
Secondary Proxy IP address : 0.0.0.0
Secondary Proxy port : 5060
Secondary Proxy Transport : TCP
Primary Proxy2 IP address : 10.10.3.55
Primary Proxy2 port : 5060
Primary Proxy2 Transport : TCP
Active Proxy : Primary :Register Not Supported
Time To Next Registration : 0 Seconds
Channels Busy / Idle / Total : 0 / 34 / 34
Stack version : 5.5.0.13
TLS Security Policy : Security Disabled
  
```

The following screen shows a means to view registered SIP telephones. The screen shows the output of the **Command sigSetShowAll** in **Group SipLine**.

Managing: 192.168.27.2 Username: admin
System > IP Network > Node Maintenance and Reports > General Commands

General Commands

Element IP : 192.168.27.2 Element Type : Signaling Server-Avaya CPPMv1

Group: **SipLine** Command: **sigSetShowAll** **RUN**

IP address: 192.168.27.2 Number of pings: 3 **PING**

UserID	AuthId	TN	Clients	Calls	SetHandle	Pos ID	SIPL Type
----- IPv4 Endpoints -----							
6003	6003	100-00-03-03	1	0	0x91e82d0		SIP Lines
6002	6002	100-00-03-02	1	0	0x91c4158		SIP Lines
Total User Registered = 2 V4 Registered = 2 V6 Registered = 0							

The following screen shows a means to view IP UNISTim telephones. The screen shows the output of the **Command isetShow** in **Group Iset**.

Managing: 192.168.27.2 Username: admin
System > IP Network > Node Maintenance and Reports > General Commands

General Commands

Element IP : 192.168.27.2 Element Type : Signaling Server-Avaya CPPMv1

Group: **Iset** Command: **isetShow** Range: 0 500 **RUN**

IP address: 192.168.27.2 Number of pings: 3 **PING**

IP Address	NAT	Model Name	Type	RegType	State	Up
10.10.9.200	1230	IP Deskphone	1230	Regular	online	13
10.10.9.201	1140E	IP Deskphone	1140	Regular	online	13
Total sets = 2						

9.2. Verify Avaya Communication Server 1000 Operational Status

Expand **System** on the left navigation panel and select **Maintenance**. Select **LD 96 - D-Channel** from the **Select by Overlay** table and the **D-Channel Diagnostics** function from the **Select by Functionality** table as shown below.

AVAYA CS1000 Element Manager

Managing: 192.168.1.5 Username: admin
System > Maintenance

Maintenance

☒ Select by Overlay ☐ Select by Functionality

<Select by Overlay>

LD 30 - Network and Signaling
LD 32 - Network and Peripheral Equipment
LD 34 - Tone and Digit Switch
LD 36 - Trunk
LD 37 - Input/Output
LD 38 - Conference Circuit
LD 39 - Intergroup Switch and System Clock
LD 45 - Background Signaling and Switching
LD 46 - Multifrequency Sender
LD 48 - Link
LD 54 - Multifrequency Signaling
LD 60 - Digital Trunk Interface and Primary Rate Interface
LD 75 - Digital Trunk
LD 80 - Call Trace
LD 96 - D-Channel
LD 117 - Ethernet and Alarm Management
LD 135 - Core Common Equipment
LD 137 - Core Input/Output
LD 143 - Centralized Software Upgrade

<Select Group>

D-Channel Diagnostics
MSDL Diagnostics
TMDI Diagnostics

Select **Status for D-Channel (STAT DCH)** command and click **Submit** to verify status of virtual D-Channel as shown below. Verify the status of the following fields.

- **APPL_STATUS** Verify status is **OPER**
- **LINK_STATUS** Verify status is **EST ACTV**

AVAYA CS1000 Element Manager

Managing: 192.168.1.5 Username: admin
System > Maintenance > D-Channel Diagnostics

D-Channel Diagnostics

Diagnostic Commands	Command Parameters	Action
Status for D-Channel (STAT DCH)		Submit
Disable Automatic Recovery (DIS AUTO)	<input type="checkbox"/> ALL	Submit
Enable Automatic Recovery (ENL AUTO)	<input type="checkbox"/> FDL	Submit
Test Interrupt Generation (TEST 100)		Submit
Establish D-Channel (EST DCH)		Submit

DCH DES APPL_STATUS LINK_STATUS AUTO_RECVPDCH BDCH

C 001 SIP_DCH **OPER** **EST ACTV** AUTO

STAT DCH

Command executed successfully.

9.3. Verify Avaya Aura® Session Manager Operational Status

9.3.1. Verify Avaya Aura® Session Manager is Operational

Navigate to **Elements → Session Manager → Dashboard** (not shown) to verify the overall system status for Session Manager. Specifically, verify the status of the following fields as shown below.

Home / Elements / Session Manager Help ?

Session Manager Dashboard

This page provides the overall status and health summary of each administered Session Manager.

Session Manager Instances

Service State: [dropdown] Shutdown System: [dropdown] As of 2:33 PM

1 Item Show All Filter: Enable

<input type="checkbox"/>	Item	Type	Tests Pass	Alarms	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Data Replication	User Data Storage Status	Version
<input type="checkbox"/>	Session Manager	Core	✓	0/0/0	Up	Accept New Service	0/4	0	1/1	✓	✓	6.3.22.0.632205

Select : All, None

Navigate to **Elements → Session Manager → System Status → Security Module Status** (not shown) to view more detailed status information on the status of Security Module for the specific Session Manager. Verify the **Status** column displays **Up** as shown below.

Home / Elements / Session Manager / System Status / Security Module Status Help ?

Security Module Status

This page allows you to view the status of each Session Manager's Security Module and to perform certain actions.

Reset Synchronize Connection Status

1 Item Show All Filter: Enable

	Details	Session Manager	Type	Status	Connections	IP Address	VLAN	Default Gateway	NIC Bonding	Entity Links (expected / actual)	Certificate Used
<input type="radio"/>	Show	Session Manager	SM	Up	12	10.10.3.55/24	---	10.10.3.1	Disabled	4/4	SIP CA

Select : None

9.3.2. Verify SIP Entity Link Status

Navigate to **Elements → Session Manager → System Status → SIP Entity Monitoring** (not shown) to view more detailed status information for one of the SIP Entity Links. Select the SIP Entity for CS1000 from the **All Monitored SIP Entities** table (not shown) to open the **SIP Entity, Entity Link Connection Status** page.

Home / Elements / Session Manager / System Status / SIP Entity Monitoring									
SIP Entity Link Monitoring Status Summary									
This page provides a summary of Session Manager SIP entity link monitoring status.									
SIP Entities Status for All Monitoring Session Manager Instances									
Run Monitor									
1 Items Refresh Filter: Enable									
<input type="checkbox"/>	Session Manager	Type	Monitored Entities						
			Down	Partially Up	Up	Not Monitored	Deny	Total	
<input type="checkbox"/>	Session Manager	Core	0	0	4	0	0	4	
Select: All, None									

Verify the status of the SIP link is up between Session Manager and CS1000 by going through the same process as outlined above but selecting the SIP Entity for the Avaya SBCE in the **All Monitored SIP Entities** table.

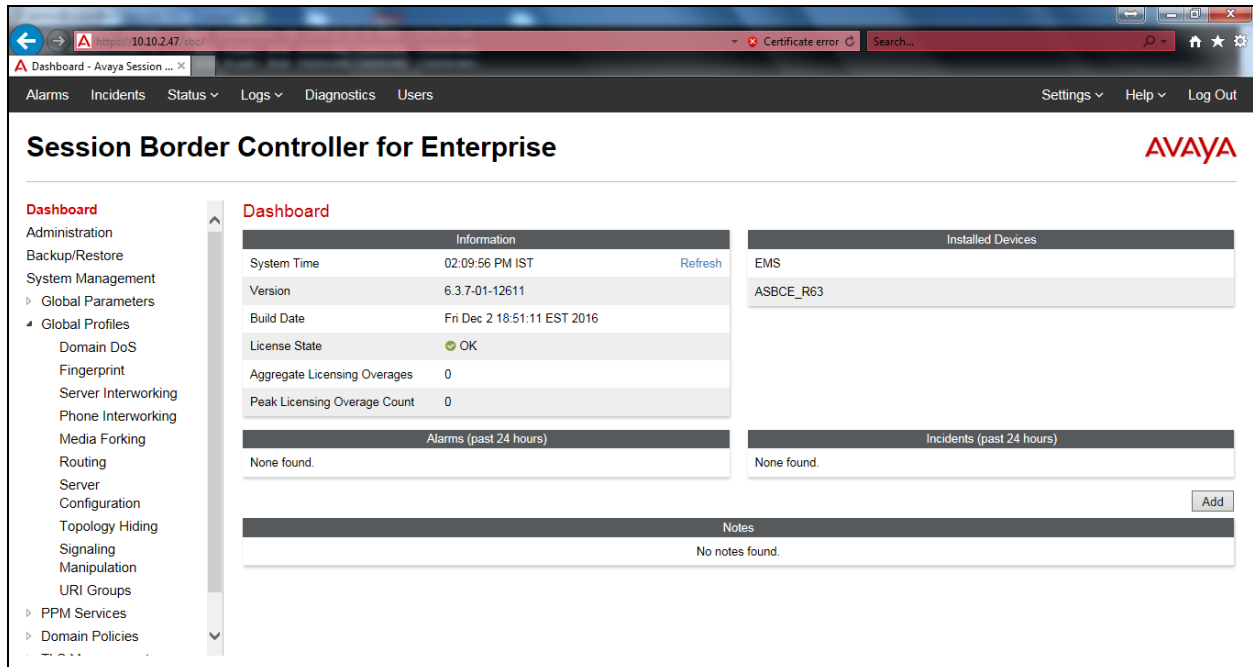
All Entity Links to SIP Entity: CS1000								
Summary View								
Status Details for the selected Session Manager:								
1 Items Refresh Filter: Enable								
	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
<input checked="" type="radio"/>	Session Manager	10.10.9.21	5060	TCP	FALSE	UP	200 OK	UP

9.4. Avaya Session Boarder Controller for Enterprise Verification

This section contains verification steps that may be performed using the Avaya Session Border Controller for Enterprise.

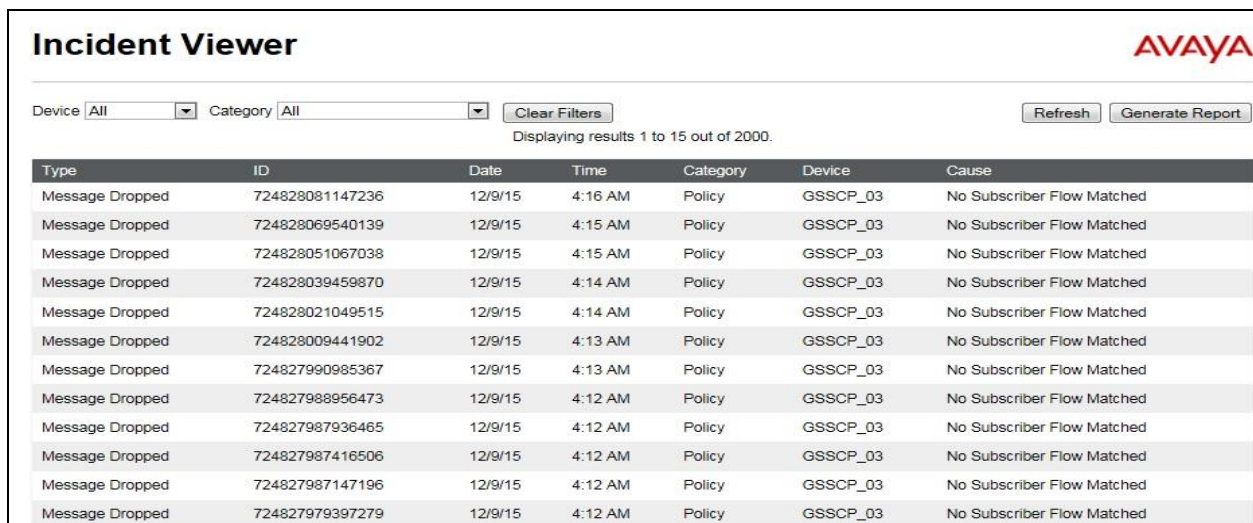
9.4.1. Incidents

The Incidents Log Viewer display alerts captured by the Avaya SBCE. Select the **Incidents** link along the top of the screen.



The screenshot shows the Avaya Session Border Controller for Enterprise Dashboard. The top navigation bar includes links for Alarms, Incidents, Status, Logs, Diagnostics, and Users. The main content area is divided into several sections: Information (System Time, Version, Build Date, License State, Aggregate Licensing Overages, Peak Licensing Overage Count), Installed Devices (EMS, ASBCE_R63), Alarms (past 24 hours), Incidents (past 24 hours), and Notes. The 'Incidents' link is highlighted in the top navigation bar.

The following screen shows example SIP messages that do not match a Server Flow for an incoming message.



The screenshot shows the Incident Viewer interface. It includes filters for Device (All) and Category (All), a Clear Filters button, and buttons for Refresh and Generate Report. The table displays 15 results out of 2000. The following table represents the data shown in the screenshot:

Type	ID	Date	Time	Category	Device	Cause
Message Dropped	724828081147236	12/9/15	4:16 AM	Policy	GSSCP_03	No Subscriber Flow Matched
Message Dropped	724828069540139	12/9/15	4:15 AM	Policy	GSSCP_03	No Subscriber Flow Matched
Message Dropped	724828051067038	12/9/15	4:15 AM	Policy	GSSCP_03	No Subscriber Flow Matched
Message Dropped	724828039459870	12/9/15	4:14 AM	Policy	GSSCP_03	No Subscriber Flow Matched
Message Dropped	724828021049515	12/9/15	4:14 AM	Policy	GSSCP_03	No Subscriber Flow Matched
Message Dropped	724828009441902	12/9/15	4:13 AM	Policy	GSSCP_03	No Subscriber Flow Matched
Message Dropped	724827990985367	12/9/15	4:13 AM	Policy	GSSCP_03	No Subscriber Flow Matched
Message Dropped	724827988956473	12/9/15	4:12 AM	Policy	GSSCP_03	No Subscriber Flow Matched
Message Dropped	724827987936465	12/9/15	4:12 AM	Policy	GSSCP_03	No Subscriber Flow Matched
Message Dropped	724827987416506	12/9/15	4:12 AM	Policy	GSSCP_03	No Subscriber Flow Matched
Message Dropped	724827987147196	12/9/15	4:12 AM	Policy	GSSCP_03	No Subscriber Flow Matched
Message Dropped	724827979397279	12/9/15	4:12 AM	Policy	GSSCP_03	No Subscriber Flow Matched

9.4.2. Trace Settings

The Trace Settings tool is for configuring and displaying call traces and packet captures for the Avaya SBCE.

To define the trace, navigate to **Device Specific Settings → Advanced Options → Troubleshooting → Trace** in the main menu on the left-hand side and select the **Packet Capture** tab.

- Select the SIP Trunk interface from the **Interface** drop down menu
- Select the signalling interface IP address from the **Local Address** drop down menu
- Enter the IP address of the network SBC in the **Remote Address** field or enter a * to capture all traffic
- Specify the **Maximum Number of Packets to Capture**, 10000 is shown as an example
- Specify the filename of the resultant pcap file in the **Capture Filename** field

The screenshot shows the 'Trace: ASBCE_R63' configuration page. On the left, a sidebar lists 'Devices' with 'ASBCE_R63' selected. The main area has two tabs: 'Packet Capture' (active) and 'Captures'. The 'Packet Capture Configuration' section includes the following fields:

Packet Capture Configuration	
Status	Ready
Interface	B1
Local Address <small>IP[:Port]</small>	All :
Remote Address <small>*, *:Port, IP, IP:Port</small>	*
Protocol	All
Maximum Number of Packets to Capture	10000
Capture Filename <small>Using the name of an existing capture will overwrite it.</small>	test.pcap

At the bottom of the configuration section are 'Start Capture' and 'Clear' buttons.

To view the trace, select the **Captures** tab and click on the relevant filename in the list of traces.

The screenshot shows the 'Trace: ASBCE_R63' page with the 'Captures' tab selected. A 'Refresh' button is in the top right. Below is a table listing the captured files:

File Name	File Size (bytes)	Last Modified	
test_20170601095310.pcap	4,096	June 1, 2017 3:53:28 PM IST	Delete

The trace is viewed as a standard pcap file in Wireshark. If the SIP trunk is working correctly, a SIP response in the form of a 200 OK will be seen from the Vodafone Libertel network.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Communication Server 1000 R7.6, Avaya Aura® Session Manager R6.3 and Avaya Session Border Controller for Enterprise R6.3 to Vodafone Libertel B.V.'s SIP Trunk Service. Vodafone Libertel B.V.'s SIP Trunk Service is a SIP-based Voice over IP solution providing businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. The service was successfully tested with a number of observations listed in **Section 2.2**.

11. Additional References

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

- [1] *Implementing Avaya Aura® System Manager Release 6.3*, Apr 2015
- [2] *Upgrading Avaya Aura® System Manager to Release 6.3*, May 2016
- [3] *Administering Avaya Aura® System Manager Release 6.3*, Feb 2017
- [4] *Implementing Avaya Aura® Session Manager Release 6.3*, Aug 2014
- [5] *Upgrading Avaya Aura® Session Manager Release 6.3*, Aug 2014
- [6] *Administering Avaya Aura® Session Manager Release 6.3*, May 2016
- [7] *Avaya Communication Server 1000 Installation and Commissioning*, Document Number NN43041-310
- [8] *Linux Platform Base and Applications Installation and Commissioning Avaya Communication Server 1000*, Document Number NN43001-315
- [9] *Software Input Output Reference – Maintenance Avaya Communication Server 1000*, Document Number NN43001-711
- [10] *Deploying Avaya Session Border Controller for Enterprise*, Release 6.3, August 2015
- [11] *Upgrading Avaya Session Border Controller for Enterprise*, Release 6.3, August 2015
- [12] *Administering Avaya Session Border Controller for Enterprise*, Release 6.3, Nov 2015
- [13] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>

12. Appendix A – Communication Server 1000 Software

Communication Server 1000 call server patches and plug ins

TID: 46379

VERSION 4121

System type is - Communication Server 1000/CPPM Linux
CPM - Pentium M 1.4 GHz

IPMGs Registered: 1
IPMGs Unregistered: 0
IPMGs Configured/unregistered: 0

RELEASE 7

ISSUE 65 P +

IDLE_SET DISPLAY NORTEL

DepList 1: core Issue: 01(created: 2015-09-28 04:19:50 (est))

MDP>LAST SUCCESSFUL MDP REFRESH :2015-11-12 14:50:17(Local Time)

MDP>USING DEPLIST ZIP FILE DOWNLOADED :2013-09-28 04:30:29(est)

SYSTEM HAS NO USER SELECTED PEPS IN-SERVICE

LOADWARE VERSION: PSWV 100+

INSTALLED LOADWARE PEPS : 1

PAT#	CR #	PATCH REF #	NAME	DATE	FILENAME
00	wi01057886	ISS1:1OF1	DSP2AB07	13/09/2013	DSP2AB07.LW

ENABLED PLUGINS : 2

PLUGIN	STATUS	PRS/CR_NUM	MPLR_NUM	DESCRIPTION
201	ENABLED	Q00424053	MPLR08139	PI:Cant XFER OUTG TRK TO OUTG TRK
501	ENABLED	Q02138637	MPLR30070	Enables blind transfer to a SIP endpoint even if SIP UPDATE is not supported by the far en

Communication Server 1000 call server deplists

VERSION 4121

RELEASE 7

ISSUE 65 P +

DepList 1: core Issue: 01 (created: 2013-05-28 04:19:50 (est))

IN-SERVICE PEPS

PAT#	CR #	PATCH REF #	NAME	DATE	FILENAME	SPECINS
000	wi01058359	ISS1:1OF1	p32331_1	16/11/2015	p32331_1.cpl	NO
001	wi01064599	iss1:1of1	p32580_1	16/11/2015	p32580_1.cpl	NO
002	wi01056067	ISS1:1OF1	p32457_1	16/11/2015	p32457_1.cpl	NO
003	wi01063263	ISS1:1OF1	p32573_1	16/11/2015	p32573_1.cpl	NO
004	wi01065842	ISS1:1OF1	p32478_1	16/11/2015	p32478_1.cpl	NO
005	wi01062607	ISS1:1OF1	p32503_1	16/11/2015	p32503_1.cpl	NO
006	wi01070756	ISS1:1OF1	p32444_1	16/11/2015	p32444_1.cpl	NO
007	wi01039280	ISS1:1OF1	p32423_1	16/11/2015	p32423_1.cpl	NO
008	wi01087543	ISS1:1OF1	p32662_1	16/11/2015	p32662_1.cpl	NO
009	wi00933195	ISS1:1OF1	p32491_1	16/11/2015	p32491_1.cpl	NO
010	wi01071379	ISS1:1OF1	p32522_1	16/11/2015	p32522_1.cpl	NO
011	wi01068669	ISS1:1OF1	p32333_1	16/11/2015	p32333_1.cpl	NO
012	wi01066991	ISS1:1OF1	p32449_1	16/11/2015	p32449_1.cpl	NO
013	wi01070474	iss1:1of1	p32407_1	16/11/2015	p32407_1.cpl	NO
014	WI0110261	ISS1:1OF1	p32758_1	16/11/2015	p32758_1.cpl	NO
015	wi01094305	ISS1:1OF1	p32640_1	16/11/2015	p32640_1.cpl	NO

016	wi01047890	ISS1:10F1	p32697_1	16/11/2015	p32697_1.cpl	NO
017	wi01055300	ISS1:10F1	p32543_1	16/11/2015	p32543_1.cpl	NO
018	wi01082456	ISS1:10F1	p32596_1	16/11/2015	p32596_1.cpl	NO
019	wi01058621	ISS1:10F1	p32339_1	16/11/2015	p32339_1.cpl	NO
020	wi01061484	ISS1:10F1	p32576_1	16/11/2015	p32576_1.cpl	NO
021	wi01078723	ISS1:10F1	p32532_1	16/11/2015	p32532_1.cpl	NO
022	wi01048457	ISS1:10F1	p32581_1	16/11/2015	p32581_1.cpl	NO
023	wi01075355	ISS1:10F1	p32594_1	16/11/2015	p32594_1.cpl	NO
024	wi01053597	ISS1:10F1	p32304_1	16/11/2015	p32304_1.cpl	NO
025	wi01045058	ISS1:10F1	p32214_1	16/11/2015	p32214_1.cpl	NO
026	wi01075359	ISS1:10F1	p32671_1	16/11/2015	p32671_1.cpl	NO
027	wi01025156	ISS1:10F1	p32136_1	16/11/2015	p32136_1.cpl	NO
028	wi01061481	ISS1:10F1	p32382_1	16/11/2015	p32382_1.cpl	NO
029	wi01035976	ISS1:10F1	p32173_1	16/11/2015	p32173_1.cpl	NO
030	wi01088775	ISS1:10F1	p32659_1	16/11/2015	p32659_1.cpl	NO
031	wi01070465	iss1:10f1	p32562_1	16/11/2015	p32562_1.cpl	NO
032	wi01088585	ISS1:10F1	p32656_1	16/11/2015	p32656_1.cpl	NO
033	wi01063864	ISS1:10F1	p32410_1	16/11/2015	p32410_1.cpl	YES
034	wi01034961	ISS1:10F1	p32144_1	16/11/2015	p32144_1.cpl	NO
035	wi01055480	ISS1:10F1	p32712_1	16/11/2015	p32712_1.cpl	NO
036	wi01034307	ISS1:10F1	p32615_1	16/11/2015	p32615_1.cpl	NO
037	wi01065118	ISS1:10F1	p32397_1	16/11/2015	p32397_1.cpl	NO
038	wi01075360	iss1:10f1	p32602_1	16/11/2015	p32602_1.cpl	NO
039	wi00884716	ISS1:10F1	p32517_1	16/11/2015	p32517_1.cpl	NO
040	wi01068851	ISS1:10F1	p32439_1	16/11/2015	p32439_1.cpl	NO
041	wi01053314	ISS1:10F1	p32555_1	16/11/2015	p32555_1.cpl	NO
042	wi01059388	iss1:10f1	p32628_1	16/11/2015	p32628_1.cpl	NO
043	wi01087528	ISS1:10F1	p32700_1	16/11/2015	p32700_1.cpl	NO
044	wi01072027	ISS1:10F1	p32689_1	16/11/2015	p32689_1.cpl	NO
045	wi01052428	ISS1:10F1	p32606_1	16/11/2015	p32606_1.cpl	NO
046	wi01053920	ISS1:10F1	p32303_1	16/11/2015	p32303_1.cpl	NO
047	wi01070468	iss1:10f1	p32418_1	16/11/2015	p32418_1.cpl	NO
048	wi01067822	ISS1:10F1	p32466_1	16/11/2015	p32466_1.cpl	YES
049	wi01060826	ISS1:10F1	p32379_1	16/11/2015	p32379_1.cpl	NO
050	wi01075352	ISS1:10F1	p32603_1	16/11/2015	p32603_1.cpl	NO
051	wi01043367	ISS1:10F1	p32232_1	16/11/2015	p32232_1.cpl	NO
052	wi01083584	ISS1:10F1	p32619_1	16/11/2015	p32619_1.cpl	NO
053	wi01060241	ISS1:10F1	p32381_1	16/11/2015	p32381_1.cpl	NO
054	wi01053195	ISS1:10F1	p32297_1	16/11/2015	p32297_1.cpl	NO
055	wi00897254	ISS1:10F1	p31127_1	16/11/2015	p31127_1.cpl	NO
056	wi01061483	ISS1:10F1	p32359_1	16/11/2015	p32359_1.cpl	NO
057	wi01085855	ISS1:10F1	p32658_1	16/11/2015	p32658_1.cpl	NO
058	wi01075353	ISS1:10F1	p32613_1	16/11/2015	p32613_1.cpl	NO
059	wi01070471	ISS1:10F1	p32415_1	16/11/2015	p32415_1.cpl	NO
060	wi01074003	ISS1:10F1	p32421_1	16/11/2015	p32421_1.cpl	NO
061	wi01060382	iss1:10f1	p32623_1	16/11/2015	p32623_1.cpl	YES
062	wi01068042	ISS1:10F1	p32669_1	16/11/2015	p32669_1.cpl	NO
063	wi01072023	ISS1:10F1	p32130_1	16/11/2015	p32130_1.cpl	YES
064	wi01065922	ISS1:10F1	p32516_1	16/11/2015	p32516_1.cpl	NO
065	wi01057403	ISS1:10F1	p32591_1	16/11/2015	p32591_1.cpl	NO
066	wi01069441	ISS1:10F1	p32097_1	16/11/2015	p32097_1.cpl	NO
067	wi01070473	ISS1:10F1	p32413_1	16/11/2015	p32413_1.cpl	NO
068	wi01056633	ISS1:10F1	p32322_1	16/11/2015	p32322_1.cpl	NO
069	wi01052968	ISS1:10F1	p32540_1	16/11/2015	p32540_1.cpl	NO
070	wi01072032	ISS1:10F1	p32448_1	16/11/2015	p32448_1.cpl	NO
071	wi01073100	ISS1:10F1	p32599_1	16/11/2015	p32599_1.cpl	NO
072	wi01035980	ISS1:10F1	p32558_1	16/11/2015	p32558_1.cpl	NO
073	wi01041453	ISS1:10F1	p32587_1	16/11/2015	p32587_1.cpl	NO
074	wi01032756	ISS1:10F1	p32673_1	16/11/2015	p32673_1.cpl	NO
075	wi01092300	ISS1:10F1	p32692_1	16/11/2015	p32692_1.cpl	NO
076	wi00996734	ISS1:10F1	p32550_1	16/11/2015	p32550_1.cpl	NO
077	wi01022599	ISS1:10F1	p32080_1	16/11/2015	p32080_1.cpl	NO
078	wi01060341	ISS1:10F1	p32578_1	16/11/2015	p32578_1.cpl	NO
079	wi01091447	ISS1:10F1	p32675_1	16/11/2015	p32675_1.cpl	NO
080	wi01070580	ISS1:10F1	p32380_1	16/11/2015	p32380_1.cpl	NO
081	wi01089519	ISS1:10F1	p32665_1	16/11/2015	p32665_1.cpl	NO
082	WI01077073	ISS1:10F1	p32534_1	16/11/2015	p32534_1.cpl	NO
083	wi01080753	ISS1:10F1	p32518_1	16/11/2015	p32518_1.cpl	NO
084	wi01065125	ISS1:10F1	p32416_1	16/11/2015	p32416_1.cpl	NO

Communication Server 1000 signaling server service updates

In System service updates: 41

PATCH#	IN_SERVICE	DATE	SPECINS	REMOVABLE	NAME
0	Yes	14/07/14	YES	YES	cs1000-csmWeb-7.65.16.22-2.i386.000
1	Yes	14/10/15	YES	YES	cs1000-dmWeb-7.65.16.23-4.i386.000
3	Yes	15/10/15	NO	YES	cs1000-sps-7.65.16.23-1.i386.000
4	Yes	14/07/14	YES	YES	cs1000-patchWeb-7.65.16.22-4.i386.000
5	Yes	14/10/15	YES	YES	cs1000-linuxbase-7.65.16.23-19.i386.000
7	Yes	14/07/14	YES	YES	cs1000-csoneksvrmgr-7.65.16.22-5.i386.000
8	Yes	27/09/13	NO	YES	cs1000-pd-7.65.16.21-00.i386.000
9	Yes	27/09/13	NO	YES	cs1000-shared-carrdtct-7.65.16.21-
01.i386.000					
10	Yes	27/09/13	NO	YES	cs1000-shared-tpselect-7.65.16.21-
01.i386.000					
11	Yes	14/07/14	YES	YES	cs1000-baseWeb-7.65.16.22-4.i386.000
12	Yes	27/09/13	NO	yes	cs1000-dbcom-7.65.16.21-00.i386.000
16	Yes	14/10/15	NO	YES	cs1000-Jboss-Quantum-7.65.16.23-5.i386.000
17	Yes	15/10/15	YES	YES	cs1000-cs-7.65.P.100-03.i386.000
18	Yes	15/10/15	NO	YES	bash-3.2-33.el5_11.4.i386.000
19	Yes	15/10/15	YES	YES	cs1000-shared-pbx-7.65.16.23-1.i386.000
20	Yes	15/10/15	YES	YES	cs1000-emWeb_6-0-7.65.16.23-3.i386.000
21	Yes	15/10/15	NO	YES	libxml2-2.6.26-2.1.25.el5_11.i386.000
22	Yes	15/10/15	NO	YES	libxml2-python-2.6.26-
2.1.25.el5_11.i386.000					
23	Yes	02/04/14	NO	YES	cs1000-shared-omm-7.65.16.21-2.i386.000
24	Yes	15/10/15	NO	YES	freetype-2.2.1-32.el5_9.1.i386.000
26	Yes	15/10/15	NO	YES	cs1000-cs1000WebService_6-0-7.65.16.23-
1.i386.000					
27	Yes	14/07/14	YES	YES	cs1000-oam-logging-7.65.16.22-4.i386.000
28	Yes	15/10/15	YES	YES	cs1000-ftrpkg-7.65.16.23-1.i386.000
29	Yes	15/10/15	NO	YES	cs1000-cppmUtil-7.65.16.23-4.i686.000
30	Yes	02/10/13	NO	YES	cs1000-snmp-7.65.16.21-00.i686.000
31	Yes	14/07/14	YES	YES	cs1000-csv-7.65.16.22-2.i386.000
33	Yes	14/07/14	YES	YES	cs1000-nrsm-7.65.16.22-3.i386.000
34	Yes	14/07/14	YES	YES	cs1000-mscTone-7.65.16.22-2.i386.000
35	Yes	14/07/14	YES	YES	cs1000-mscMusc-7.65.16.22-4.i386.000
36	Yes	14/07/14	YES	YES	cs1000-mscConf-7.65.16.22-2.i386.000
38	Yes	02/04/14	YES	YES	cs1000-emWebLocal_6-0-7.65.16.22-1.i386.000
39	Yes	15/10/15	NO	YES	tzdata-2015a-1.el5.i386.000
40	Yes	02/04/14	YES	YES	cs1000-ipsec-7.65.16.22-1.i386.000
41	Yes	15/10/15	YES	YES	cs1000-tps-7.65.16.23-15.i386.000
43	Yes	15/10/15	YES	YES	kernel-2.6.18-406.el5.i686.000
44	Yes	15/10/15	YES	YES	cs1000-vtrk-7.65.16.23-76.i386.000
45	Yes	15/10/15	YES	YES	cs1000-bcc-7.65.16.23-10.i386.000
47	Yes	14/07/14	YES	YES	cs1000-mscAnnc-7.65.16.22-2.i386.000
48	Yes	14/07/14	YES	YES	cs1000-mscAttn-7.65.16.22-2.i386.000
49	Yes	14/07/14	NO	YES	cs1000-gk-7.65.16.22-1.i386.000
53	Yes	14/07/14	YES	YES	cs1000-shared-xmsg-7.65.16.22-1.i386.000

Communication Server 1000 system software

Product Release: 7.65.16.00

Base Applications

base	7.65.16	[patched]
NTAFS	7.65.16	
sm	7.65.16	
cs1000-Auth	7.65.16	
Jboss-Quantum	n/a	[patched]
cnd	7.65.16	
lhmonitor	7.65.16	
baseAppUtils	7.65.16	
dfoTools	7.65.16	
c ppmUtil	n/a	[patched]
oam-logging	n/a	[patched]
dmWeb	n/a	[patched]
baseWeb	n/a	[patched]
ipsec	n/a	[patched]
Snmp-Daemon-TrapLib	n/a	[patched]
ISECSH	7.65.16	
patchWeb	n/a	[patched]
EmCentralLogic	7.65.16	

Application configuration: CS+SS+NRS+EM

Packages:

CS+SS+NRS+EM

Configuration version:	7.65.16-00	
cs	7.65.16	[patched]
dbcom	7.65.16.21	[patched]
cslogin	7.65.16	
sigServerShare	7.65.16	[patched]
csv	7.65.16	[patched]
tps	7.65.16	[patched]
vtrk	7.65.16	[patched]
pd	7.65.16.21	[patched]
sps	7.65.16	[patched]
ncs	7.65.16	
gk	7.65.16	[patched]
nrsm	7.65.16	[patched]
nrsmWebService	7.65.16	
managedElementWebService	7.65.16	
EmConfig	7.65.16	
emWeb_6-0	7.65.16	[patched]
emWebLocal_6-0	7.65.16	[patched]
csmWeb	7.65.16	[patched]
bcc	7.65.16	[patched]
ftrpkg	7.65.16	[patched]
cs1000WebService_6-0	7.65.16	[patched]
mscAnnc	7.65.16	[patched]
mscAttn	7.65.16	[patched]
mscConf	7.65.16	[patched]
mscMusc	7.65.16	[patched]
mscTone	7.65.16	[patched]

13. Appendix B – Inbound & Outbound CallFlow Examples

[1] Avaya Enterprise → Vodafone Libertel B.V. Fixed (PSTN) SIP Trunk

```
339368475ms SIP Tx: TCP 192.168.37.2:4115 -> 62.140.159.241:5060
INVITE sip:0035391482424@62.140.159.241;user=phone SIP/2.0
Via: SIP/2.0/TCP 192.168.37.2:5060;rport;
branch=z9hG4bKf6957bb997fe052b04a5d0e09f57d754
From: "0387002093" <sip:0387002093@62.140.159.241;user=phone>;
tag=be96d972f75e0dc9
To: <sip:0035391482424@62.140.159.241;user=phone>
Call-ID: 67e4ff67ba66e9ed5d0417bed3f3b029
CSeq: 1257368408 INVITE
Contact: "0387002093"
<sip:0387002093@192.168.37.2:5060;transport=tcp>
Max-Forwards: 70
Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,INFO,NOTIFY,UPDATE
Supported: timer,100rel
User-Agent: Nortel CS1000 SIP GW release 7.0
P-Asserted-Identity: "0387002093"
<sip:0387002093@192.168.37.2:5060>
Content-Type: application/sdp
Content-Length: 247

v=0
o=UserA 804038831 352566035 IN IP4 192.168.37.2
s=Session SDP
c=IN IP4 192.168.37.2
t=0 0
m=audio 40788 RTP/AVP 8 18 101
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
```

```
339368491ms SIP Rx: TCP 62.140.159.241:5060 -> 192.168.37.2:4115
SIP/2.0 100 Trying
From: "0387002093" <sip:0387002093@62.140.159.241;user=phone>;
tag=be96d972f75e0dc9
To: <sip:0035391482424@62.140.159.241;user=phone>
CSeq: 1257368408 INVITE
Call-ID: 67e4ff67ba66e9ed5d0417bed3f3b029
Via: SIP/2.0/TCP 192.168.37.2:5060;rport=4115;
branch=z9hG4bKf6957bb997fe052b04a5d0e09f57d754
Content-Length: 0
```

339370425ms SIP Rx: TCP 62.140.159.241:5060 -> 192.168.37.2:4115
SIP/2.0 183 Session Progress
From: "0387002093" <sip:0387002093@62.140.159.241;user=phone>;
tag=be96d972f75e0dc9
To: <sip:0035391482424@62.140.159.241;user=phone>;tag=7A7A4D58-670
CSeq: 1257368408 INVITE
Call-ID: 67e4ff67ba66e9ed5d0417bed3f3b029
Contact: <sip:0035391482424@62.140.159.241:5060;transport=tcp>
Record-Route: <sip:62.140.159.241:5060;ipcs-line=13549;lr;
transport=tcp>
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, REGISTER
Supported: replaces
Via: SIP/2.0/TCP 192.168.37.2:5060;rport=4115;
branch=z9hG4bKf6957bb997fe052b04a5d0e09f57d754
Date: Tue, 06 Nov 2018 12:58:51 GMT
Server: Cisco-SIPGateway/IOS-15.4.3.M3
Allow-Events: telephone-event
Content-Disposition: session;handling=required
Content-Type: application/sdp
Content-Length: 219

v=0
o=- 4956075 4956075 IN IP4 62.140.159.241
s=-
t=0 0
a=sendrecv
m=audio 35014 RTP/AVP 8 101
c=IN IP4 62.140.159.241
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=maxptime:40
a=ptime:20

339370482ms SIP Rx: TCP 62.140.159.241:5060 -> 192.168.37.2:4115
SIP/2.0 180 Ringing
From: "0387002093" <sip:0387002093@62.140.159.241;user=phone>;
tag=be96d972f75e0dc9
To: <sip:0035391482424@62.140.159.241;user=phone>;tag=7A7A4D58-670
CSeq: 1257368408 INVITE
Call-ID: 67e4ff67ba66e9ed5d0417bed3f3b029
Contact: <sip:0035391482424@62.140.159.241:5060;transport=tcp>
Record-Route: <sip:62.140.159.241:5060;ipcs-line=13549;lr;
transport=tcp>
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, REGISTER
Supported: replaces
Via: SIP/2.0/TCP 192.168.37.2:5060;rport=4115;
branch=z9hG4bKf6957bb997fe052b04a5d0e09f57d754
Date: Tue, 06 Nov 2018 12:58:51 GMT
Server: Cisco-SIPGateway/IOS-15.4.3.M3
Allow-Events: telephone-event
Content-Length: 0

339372413ms SIP Rx: TCP 62.140.159.241:5060 -> 192.168.37.2:4115
SIP/2.0 200 OK
From: "0387002093" <sip:0387002093@62.140.159.241;user=phone>;
tag=be96d972f75e0dc9
To: <sip:0035391482424@62.140.159.241;user=phone>;tag=7A7A4D58-670
CSeq: 1257368408 INVITE
Call-ID: 67e4ff67ba66e9ed5d0417bed3f3b029
Contact: <sip:0035391482424@62.140.159.241:5060;transport=tcp>
Record-Route: <sip:62.140.159.241:5060;ipcs-line=13549;lr;
transport=tcp>
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, REGISTER
Supported: replaces
Supported: sdp-anat
Supported: timer
Via: SIP/2.0/TCP 192.168.37.2:5060;rport=4115;
branch=z9hG4bKf6957bb997fe052b04a5d0e09f57d754
Date: Tue, 06 Nov 2018 12:58:51 GMT
Require: timer
Server: Cisco-SIPGateway/IOS-15.4.3.M3
Allow-Events: telephone-event
Session-Expires: 1800;refresher=uac
Content-Disposition: session;handling=required
Content-Type: application/sdp
Content-Length: 219

v=0
o=- 4956075 4956075 IN IP4 62.140.159.241
s=-
t=0 0
a=sendrecv
m=audio 35014 RTP/AVP 8 101
c=IN IP4 62.140.159.241
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=maxptime:40
a=ptime:20

339372413ms SIP Tx: TCP 192.168.37.2:4115 -> 62.140.159.241:5060
ACK sip:0035391482424@62.140.159.241:5060;transport=tcp SIP/2.0
Via: SIP/2.0/TCP 192.168.37.2:5060;rport;
branch=z9hG4bKa33d6a5cda6bf6747b0d911b2666844e
Route: <sip:62.140.159.241:5060;ipcs-line=13549;lr;transport=tcp>
From: "0387002093" <sip:0387002093@62.140.159.241;user=phone>;
tag=be96d972f75e0dc9
To: <sip:0035391482424@62.140.159.241;user=phone>;tag=7A7A4D58-670
Call-ID: 67e4ff67ba66e9ed5d0417bed3f3b029
CSeq: 1257368408 ACK
Max-Forwards: 70
Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,INFO,NOTIFY,UPDATE
User-Agent: Nortel CS1000 SIP GW release 7.0
Content-Length: 0

339375270ms SIP Tx: TCP 192.168.37.2:4115 -> 62.140.159.241:5060
BYE sip:0035391482424@62.140.159.241:5060;transport=tcp SIP/2.0
Via: SIP/2.0/TCP 192.168.37.2:5060;rport;
branch=z9hG4bK0329406ce41e14d35aba3a8ff64789bb
Route: <sip:62.140.159.241:5060;ipcs-line=13549;lr;transport=tcp>
From: "0387002093" <sip:0387002093@62.140.159.241;user=phone>;
tag=be96d972f75e0dc9
To: <sip:0035391482424@62.140.159.241;user=phone>;tag=7A7A4D58-670
Call-ID: 67e4ff67ba66e9ed5d0417bed3f3b029
CSeq: 1257368409 BYE
Contact: "0387002093" <sip:0387002093@192.168.37.2:5060;
transport=tcp>
Max-Forwards: 70
Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,INFO,NOTIFY,UPDATE
Supported: timer,100rel
User-Agent: Nortel CS1000 SIP GW release 7.0
Reason: Q.850;cause=16;text="Normal call clearing"
Content-Length: 0

339375315ms SIP Rx: TCP 62.140.159.241:5060 -> 192.168.37.2:4115
SIP/2.0 200 OK
From: "0387002093" <sip:0387002093@62.140.159.241;user=phone>;
tag=be96d972f75e0dc9
To: <sip:0035391482424@62.140.159.241;user=phone>;tag=7A7A4D58-670
CSeq: 1257368409 BYE
Call-ID: 67e4ff67ba66e9ed5d0417bed3f3b029
Record-Route: <sip:62.140.159.241:5060;ipcs-line=13549;lr;
transport=tcp>
Supported: replaces
Via: SIP/2.0/TCP 192.168.37.2:5060;rport=4115;
branch=z9hG4bK0329406ce41e14d35aba3a8ff64789bb
Date: Tue, 06 Nov 2018 12:58:58 GMT
Server: Cisco-SIPGateway/IOS-15.4.3.M3
Reason: Q.850;cause=16
P-RTP-Stat: PS=244,OS=41968,PR=142,OR=24424,PL=0,JI=0,LA=0,DU=2
Content-Length: 0

[2] Vodafone Libertel B.V. Fixed (PSTN) SIP Trunk → Avaya Enterprise

```
338595311ms SIP Rx: TCP 62.140.159.241:44182 -> 192.168.37.2:5060
INVITE sip:0387002091@192.168.37.2:5060 SIP/2.0
From: <sip:0306097600@62.140.159.241>;tag=7A6E77DC-21FA
To: <sip:0387002091@192.168.37.2>
CSeq: 101 INVITE
Call-ID: BE2E8CE8-E0F811E8-9366CE79-EFCBD256@62.140.159.241
Contact: <sip:0306097600@62.140.159.241:5060;transport=tcp>
Record-Route: <sip:62.140.159.241:5060;ipcs-
line=13516;lr;transport=tcp>
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, REGISTER
Supported: timer, resource-priority, replaces
User-Agent: Vodafone-NL-SIP-Gateway-V1.1
Max-Forwards: 66
Via: SIP/2.0/TCP 62.140.159.241:5060;branch=z9hG4bK-s1632-
001408967006-1--s1632-
Expires: 180
Date: Tue, 06 Nov 2018 12:45:58 GMT
Timestamp: 1541508358
Allow-Events: telephone-event
P-Preferred-Identity: <sip:0306097600@62.140.159.241>
Session-Expires: 1800
Min-SE: 1800
Content-Disposition: session;handling=required
Content-Type: application/sdp
oc-mode: ERS_SIP
P-Early-Media: supported
Content-Length: 264

v=0
o=- 9228764 9228764 IN IP4 62.140.159.241
s=-
t=0 0
a=sendrecv
m=audio 35012 RTP/AVP 18 8 96
c=IN IP4 62.140.159.241
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=yes
a=rtpmap:8 PCMA/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=maxptime:40
a=ptime:20
```

338595317ms SIP Tx: TCP 192.168.37.2:5060 -> 62.140.159.241:44182
SIP/2.0 180 Ringing
Via: SIP/2.0/TCP 62.140.159.241:5060;branch=z9hG4bK-s1632-001408967006-1--s1632-
Record-Route: <sip:62.140.159.241:5060;ipcs-line=13516;lr;transport=tcp>
From: <sip:0306097600@62.140.159.241>;tag=7A6E77DC-21FA
Call-ID: BE2E8CE8-E0F811E8-9366CE79-EFCBD256@62.140.159.241
CSeq: 101 INVITE
Contact: "Extn89111"
sip:0387002091@192.168.37.2:5060;transport=tcp>
Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,INFO,NOTIFY,UPDATE
P-Asserted-Identity: "Extn89111"
<sip:0387002091@192.168.37.2:5060>
Supported: timer,100rel
Server: Nortel CS1000 SIP GW release 7.0
To: <sip:0387002091@192.168.37.2>;tag=fb5e3ce210f82f3d
Content-Length: 0

338598622ms SIP Tx: TCP 192.168.37.2:5060 -> 62.140.159.241:44182
SIP/2.0 200 OK
Via: SIP/2.0/TCP 62.140.159.241:5060;branch=z9hG4bK-s1632-001408967006-1--s1632-
Record-Route: <sip:62.140.159.241:5060;ipcs-line=13516;lr;transport=tcp>
From: <sip:0306097600@62.140.159.241>;tag=7A6E77DC-21FA
Call-ID: BE2E8CE8-E0F811E8-9366CE79-EFCBD256@62.140.159.241
CSeq: 101 INVITE
Contact: "Extn89111"
<sip:0387002091@192.168.37.2:5060;transport=tcp>
Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,INFO,NOTIFY,UPDATE
P-Asserted-Identity: "Extn89111"
<sip:0387002091@192.168.37.2:5060>
Supported: timer,100rel
Server: Nortel CS1000 SIP GW release 7.0
Min-SE: 1800
Require: timer
Session-Expires: 1800;refresher=uac
To: <sip:0387002091@192.168.37.2>;tag=fb5e3ce210f82f3d
Content-Type: application/sdp
Content-Length: 199

v=0
o=UserA 1876054572 2072633803 IN IP4 192.168.37.2
s=Session SDP
c=IN IP4 192.168.37.2
t=0 0
m=audio 40784 RTP/AVP 8 96
a=rtpmap:8 PCMA/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15

338598674ms SIP Rx: TCP 62.140.159.241:44182 -> 192.168.37.2:5060
ACK sip:0387002091@192.168.37.2:5060;transport=tcp SIP/2.0
From: <sip:0306097600@62.140.159.241>;tag=7A6E77DC-21FA
To: <sip:0387002091@192.168.37.2>;tag=fb5e3ce210f82f3d
CSeq: 101 ACK
Call-ID: BE2E8CE8-E0F811E8-9366CE79-EFCBD256@62.140.159.241
Record-Route: <sip:62.140.159.241:5060;ipcs-
line=13516;lr;transport=tcp>
Supported: replaces
Max-Forwards: 69
Via: SIP/2.0/TCP 62.140.159.241:5060;branch=z9hG4bK-s1632-
000026971994-1--s1632-
Date: Tue, 06 Nov 2018 12:45:58 GMT
Allow-Events: telephone-event
Content-Length: 0

338600653ms SIP Tx: TCP 192.168.37.2:4115 -> 62.140.159.241:5060
BYE sip:0306097600@62.140.159.241:5060;transport=tcp SIP/2.0
Via: SIP/2.0/TCP 192.168.37.2:5060;rport;
branch=z9hG4bKcd2dab7310c61e43e5c68a8ca3d1c653
Route: <sip:62.140.159.241:5060;ipcs-line=13516;lr;transport=tcp>
From: <sip:0387002091@192.168.37.2>;tag=fb5e3ce210f82f3d
To: <sip:0306097600@62.140.159.241>;tag=7A6E77DC-21FA
Call-ID: BE2E8CE8-E0F811E8-9366CE79-EFCBD256@62.140.159.241
CSeq: 102 BYE
Contact: "Extn89111"
<sip:0387002091@192.168.37.2:5060;transport=tcp>
Max-Forwards: 70
Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,INFO,NOTIFY,UPDATE
Supported: timer,100rel
User-Agent: Nortel CS1000 SIP GW release 7.0
Reason: Q.850;cause=16;text="Normal call clearing"
Content-Length: 0

338600699ms SIP Rx: TCP 62.140.159.241:5060 -> 192.168.37.2:4115
SIP/2.0 200 OK
From: <sip:0387002091@192.168.37.2>;tag=fb5e3ce210f82f3d
To: <sip:0306097600@62.140.159.241>;tag=7A6E77DC-21FA
CSeq: 102 BYE
Call-ID: BE2E8CE8-E0F811E8-9366CE79-EFCBD256@62.140.159.241
Record-Route: <sip:62.140.159.241:5060;ipcs-
line=13516;lr;transport=tcp>
Supported: replaces
Via: SIP/2.0/TCP 192.168.37.2:5060;rport=4115;
branch=z9hG4bKcd2dab7310c61e43e5c68a8ca3d1c653
Date: Tue, 06 Nov 2018 12:46:03 GMT
Server: Cisco-SIPGateway/IOS-15.4.3.M3
Reason: Q.850;cause=16
P-RTP-Stat: PS=94,OS=16168,PR=93,OR=15996,PL=0,JI=0,LA=0,DU=2
Content-Length: 0

[3] Avaya Enterprise → Vodafone Libertel B.V. Mobile SIP Trunk

```
339368475mS SIP Tx: TCP 192.168.37.2:4115 -> 62.140.159.242:5060
INVITE sip:7091@62.140.159.242;user=phone SIP/2.0
Via: SIP/2.0/TCP 192.168.37.2:5060;rport;
branch=z9hG4bKf6957bb997fe052b04a5d0e09f57d754
From: "2091" <sip:2091@62.140.159.242;user=phone>;
tag=bf10d972f75e0de7
To: <sip:7091@62.140.159.242;user=phone>
Call-ID: 22e4dd67ba66e9ed5d0518fed3k3c017
CSeq: 1257368408 INVITE
Contact: "2091" <sip:2091@192.168.37.2:5060;transport=tcp>
Max-Forwards: 70
Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,INFO,NOTIFY,UPDATE
Supported: timer,100rel
User-Agent: Nortel CS1000 SIP GW release 7.0
P-Asserted-Identity: "2091" <sip:2091@192.168.37.2:5060>
Content-Type: application/sdp
Content-Length: 247
```

```
v=0
o=UserA 804038831 352566035 IN IP4 192.168.37.2
s=Session SDP
c=IN IP4 192.168.37.2
t=0 0
m=audio 40788 RTP/AVP 8 18 101
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
```

```
339368491mS SIP Rx: TCP 62.140.159.242:5060 -> 192.168.37.2:4115
SIP/2.0 100 Trying
From: "2091" <sip:2091@62.140.159.242;user=phone>;
tag=bf10d972f75e0de7
To: <sip:7091@62.140.159.242;user=phone>
CSeq: 1257368408 INVITE
Call-ID: 22e4dd67ba66e9ed5d0518fed3k3c017
Via: SIP/2.0/TCP 192.168.37.2:5060;rport=4115;
branch=z9hG4bKf6957bb997fe052b04a5d0e09f57d754
Content-Length: 0
```

339370425ms SIP Rx: TCP 62.140.159.242:5060 -> 192.168.37.2:4115
SIP/2.0 183 Session Progress
From: "2091" <sip:2091@62.140.159.242;user=phone>;
tag=bf10d972f75e0de7
To: <sip:7091@62.140.159.242;user=phone>;tag=7A7A4D58-670
CSeq: 1257368408 INVITE
Call-ID: 22e4dd67ba66e9ed5d0518fed3k3c017
Contact: <sip:7091@62.140.159.242:5060;transport=tcp>
Record-Route: <sip:62.140.159.242:5060;ipcs-line=13549;lr;
transport=tcp>
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, REGISTER
Supported: replaces
Via: SIP/2.0/TCP 192.168.37.2:5060;rport=4115;
branch=z9hG4bKf6957bb997fe052b04a5d0e09f57d754
Date: Tue, 06 Nov 2018 13:08:31 GMT
Server: Cisco-SIPGateway/IOS-15.4.3.M3
Allow-Events: telephone-event
Content-Disposition: session;handling=required
Content-Type: application/sdp
Content-Length: 219

v=0
o=- 4956075 4956075 IN IP4 62.140.159.242
s=-
t=0 0
a=sendrecv
m=audio 35014 RTP/AVP 8 101
c=IN IP4 62.140.159.242
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=maxptime:40
a=ptime:20

339370482ms SIP Rx: TCP 62.140.159.242:5060 -> 192.168.37.2:4115
SIP/2.0 180 Ringing
From: "2091" <sip:2091@62.140.159.242;user=phone>;
tag=bf10d972f75e0de7
To: <sip:7091@62.140.159.242;user=phone>;tag=7A7A4D58-670
CSeq: 1257368408 INVITE
Call-ID: 22e4dd67ba66e9ed5d0518fed3k3c017
Contact: <sip:7091@62.140.159.242:5060;transport=tcp>
Record-Route: <sip:62.140.159.242:5060;ipcs-line=13549;lr;
transport=tcp>
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, REGISTER
Supported: replaces
Via: SIP/2.0/TCP 192.168.37.2:5060;rport=4115;
branch=z9hG4bKf6957bb997fe052b04a5d0e09f57d754
Date: Tue, 06 Nov 2018 13:08:31 GMT
Server: Cisco-SIPGateway/IOS-15.4.3.M3
Allow-Events: telephone-event
Content-Length: 0

339372413ms SIP Rx: TCP 62.140.159.242:5060 -> 192.168.37.2:4115
SIP/2.0 200 OK
From: "2091" <sip:2091@62.140.159.242;user=phone>;
tag=bf10d972f75e0de7
To: <sip:7091@62.140.159.242;user=phone>;tag=7A7A4D58-670
CSeq: 1257368408 INVITE
Call-ID: 22e4dd67ba66e9ed5d0518fed3k3c017
Contact: <sip:7091@62.140.159.242:5060;transport=tcp>
Record-Route: <sip:62.140.159.242:5060;ipcs-line=13549;lr;
transport=tcp>
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, REGISTER
Supported: replaces
Supported: sdp-anat
Supported: timer
Via: SIP/2.0/TCP 192.168.37.2:5060;rport=4115;
branch=z9hG4bKf6957bb997fe052b04a5d0e09f57d754
Date: Tue, 06 Nov 2018 13:08:31 GMT
Require: timer
Server: Cisco-SIPGateway/IOS-15.4.3.M3
Allow-Events: telephone-event
Session-Expires: 1800;refresher=uac
Content-Disposition: session;handling=required
Content-Type: application/sdp
Content-Length: 219

v=0
o=- 4956075 4956075 IN IP4 62.140.159.242
s=-
t=0 0
a=sendrecv
m=audio 35014 RTP/AVP 8 101
c=IN IP4 62.140.159.242
a=rtpmap:8 PCMA/8000
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-15
a=maxptime:40
a=ptime:20

339372413ms SIP Tx: TCP 192.168.37.2:4115 -> 62.140.159.242:5060
ACK sip:7091@62.140.159.242:5060;transport=tcp SIP/2.0
Via: SIP/2.0/TCP 192.168.37.2:5060;rport;
branch=z9hG4bKa33d6a5cda6bf6747b0d911b2666844e
Route: <sip:62.140.159.242:5060;ipcs-line=13549;lr;transport=tcp>
From: "2091" <sip:2091@62.140.159.242;user=phone>;
tag=bf10d972f75e0de7
To: <sip:7091@62.140.159.242;user=phone>;tag=7A7A4D58-670
Call-ID: 22e4dd67ba66e9ed5d0518fed3k3c017
CSeq: 1257368408 ACK
Max-Forwards: 70
Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,INFO,NOTIFY,UPDATE
User-Agent: Nortel CS1000 SIP GW release 7.0
Content-Length: 0

339375270ms SIP Tx: TCP 192.168.37.2:4115 -> 62.140.159.242:5060
BYE sip:7091@62.140.159.242:5060;transport=tcp SIP/2.0
Via: SIP/2.0/TCP 192.168.37.2:5060;rport;
branch=z9hG4bK0329406ce41e14d35aba3a8ff64789bb
Route: <sip:62.140.159.242:5060;ipcs-line=13549;lr;transport=tcp>
From: "2091" <sip:2091@62.140.159.242;user=phone>;
tag=bf10d972f75e0de7
To: <sip:7091@62.140.159.242;user=phone>;tag=7A7A4D58-670
Call-ID: 22e4dd67ba66e9ed5d0518fed3k3c017
CSeq: 1257368409 BYE
Contact: "2091" <sip:2091@192.168.37.2:5060;
transport=tcp>
Max-Forwards: 70
Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,INFO,NOTIFY,UPDATE
Supported: timer,100rel
User-Agent: Nortel CS1000 SIP GW release 7.0
Reason: Q.850;cause=16;text="Normal call clearing"
Content-Length: 0

339375315ms SIP Rx: TCP 62.140.159.242:5060 -> 192.168.37.2:4115
SIP/2.0 200 OK
From: "2091" <sip:2091@62.140.159.242;user=phone>;
tag=bf10d972f75e0de7
To: <sip:7091@62.140.159.242;user=phone>;tag=7A7A4D58-670
CSeq: 1257368409 BYE
Call-ID: 22e4dd67ba66e9ed5d0518fed3k3c017
Record-Route: <sip:62.140.159.242:5060;ipcs-line=13549;lr;
transport=tcp>
Supported: replaces
Via: SIP/2.0/TCP 192.168.37.2:5060;rport=4115;
branch=z9hG4bK0329406ce41e14d35aba3a8ff64789bb
Date: Tue, 06 Nov 2018 13:08:31 GMT
Server: Cisco-SIPGateway/IOS-15.4.3.M3
Reason: Q.850;cause=16
P-RTP-Stat: PS=244,OS=41968,PR=142,OR=24424,PL=0,JI=0,LA=0,DU=2
Content-Length: 0

[4] Vodafone Libertel B.V. Mobile SIP Trunk → Avaya Enterprise

```
338595311ms SIP Rx: TCP 62.140.159.242:44182 -> 192.168.37.2:5060
INVITE sip:2091@192.168.37.2:5060 SIP/2.0
From: <sip:7091@62.140.159.242>;tag=5F6E87DC-45BG
To: <sip:2091@192.168.37.2>
CSeq: 101 INVITE
Call-ID: FD2E8CE4-A0F922E8-7326FE79-KFCBC234@62.140.159.242
Contact: <sip:7091@62.140.159.242:5060;transport=tcp>
Record-Route: <sip:62.140.159.242:5060;ipcs-
line=13516;lr;transport=tcp>
Allow: INVITE, OPTIONS, BYE, CANCEL, ACK, PRACK, REGISTER
Supported: timer, resource-priority, replaces
User-Agent: Vodafone-NL-SIP-Gateway-V1.1
Max-Forwards: 66
Via: SIP/2.0/TCP 62.140.159.242:5060;branch=z9hG4bK-s1632-
001408967006-1--s1632-
Expires: 180
Date: Tue, 06 Nov 2018 13:11:34 GMT
Timestamp: 1541508358
Allow-Events: telephone-event
P-Preferred-Identity: <sip:7091@62.140.159.242>
Session-Expires: 1800
Min-SE: 1800
Content-Disposition: session;handling=required
Content-Type: application/sdp
oc-mode: ERS_SIP
P-Early-Media: supported
Content-Length: 264

v=0
o=- 9228764 9228764 IN IP4 62.140.159.242
s=-
t=0 0
a=sendrecv
m=audio 35012 RTP/AVP 18 8 96
c=IN IP4 62.140.159.242
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=yes
a=rtpmap:8 PCMA/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=maxptime:40
a=ptime:20
```

338595317ms SIP Tx: TCP 192.168.37.2:5060 -> 62.140.159.242:44182
SIP/2.0 180 Ringing
Via: SIP/2.0/TCP 62.140.159.242:5060;branch=z9hG4bK-s1632-001408967006-1--s1632-
Record-Route: <sip:62.140.159.242:5060;ipcs-line=13516;lr;transport=tcp>
From: <sip:7091@62.140.159.242>;tag=5F6E87DC-45BG
Call-ID: FD2E8CE4-A0F922E8-7326FE79-KFCBC234@62.140.159.242
CSeq: 101 INVITE
Contact: "Extn89111"
sip:2091@192.168.37.2:5060;transport=tcp>
Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,INFO,NOTIFY,UPDATE
P-Asserted-Identity: "Extn89111"
<sip:2091@192.168.37.2:5060>
Supported: timer,100rel
Server: Nortel CS1000 SIP GW release 7.0
To: <sip:2091@192.168.37.2>;tag=fb5e3ce210f82f3d
Content-Length: 0

338598622ms SIP Tx: TCP 192.168.37.2:5060 -> 62.140.159.242:44182
SIP/2.0 200 OK
Via: SIP/2.0/TCP 62.140.159.242:5060;branch=z9hG4bK-s1632-001408967006-1--s1632-
Record-Route: <sip:62.140.159.242:5060;ipcs-line=13516;lr;transport=tcp>
From: <sip:7091@62.140.150.241>;tag=5F6E87DC-45BG
Call-ID: FD2E8CE4-A0F922E8-7326FE79-KFCBC234@62.140.159.242
CSeq: 101 INVITE
Contact: "Extn89111"
<sip:2091@192.168.37.2:5060;transport=tcp>
Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,INFO,NOTIFY,UPDATE
P-Asserted-Identity: "Extn89111"
<sip:2091@192.168.37.2:5060>
Supported: timer,100rel
Server: Nortel CS1000 SIP GW release 7.0
Min-SE: 1800
Require: timer
Session-Expires: 1800;refresher=uac
To: <sip:2091@192.168.37.2>;tag=fb5e3ce210f82f3d
Content-Type: application/sdp
Content-Length: 199

v=0
o=UserA 1876054572 2072633803 IN IP4 192.168.37.2
s=Session SDP
c=IN IP4 192.168.37.2
t=0 0
m=audio 40784 RTP/AVP 8 96
a=rtpmap:8 PCMA/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15

338598674ms SIP Rx: TCP 62.140.159.242:44182 -> 192.168.37.2:5060
ACK sip:2091@192.168.37.2:5060;transport=tcp SIP/2.0
From: <sip:7091@62.140.159.242>;tag=5F6E87DC-45BG
To: <sip:2091@192.168.37.2>;tag=fb5e3ce210f82f3d
CSeq: 101 ACK
Call-ID: FD2E8CE4-A0F922E8-7326FE79-KFCBC234@62.140.159.242
Record-Route: <sip:62.140.159.242:5060;ipcs-
line=13516;lr;transport=tcp>
Supported: replaces
Max-Forwards: 69
Via: SIP/2.0/TCP 62.140.159.242:5060;branch=z9hG4bK-s1632-
000026971994-1--s1632-
Date: Tue, 06 Nov 2018 13:11:34 GMT
Allow-Events: telephone-event
Content-Length: 0

338600653ms SIP Tx: TCP 192.168.37.2:4115 -> 62.140.159.242:5060
BYE sip:7091@62.140.159.242:5060;transport=tcp SIP/2.0
Via: SIP/2.0/TCP 192.168.37.2:5060;rport;
branch=z9hG4bKcd2dab7310c61e43e5c68a8ca3d1c653
Route: <sip:62.140.159.242:5060;ipcs-line=13516;lr;transport=tcp>
From: <sip:2091@192.168.37.2>;tag=fb5e3ce210f82f3d
To: <sip:7091@62.140.159.242>;tag=5F6E87DC-45BG
Call-ID: FD2E8CE4-A0F922E8-7326FE79-KFCBC234@62.140.159.242
CSeq: 102 BYE
Contact: "Extn89111"
<sip:2091@192.168.37.2:5060;transport=tcp>
Max-Forwards: 70
Allow: INVITE,ACK,CANCEL,OPTIONS,BYE,INFO,NOTIFY,UPDATE
Supported: timer,100rel
User-Agent: Nortel CS1000 SIP GW release 7.0
Reason: Q.850;cause=16;text="Normal call clearing"
Content-Length: 0

338600699ms SIP Rx: TCP 62.140.159.242:5060 -> 192.168.37.2:4115
SIP/2.0 200 OK
From: <sip:2091@192.168.37.2>;tag=fb5e3ce210f82f3d
To: <sip:7091@62.140.159.242>;tag=5F6E87DC-45BG
CSeq: 102 BYE
Call-ID: FD2E8CE4-A0F922E8-7326FE79-KFCBC234@62.140.159.242
Record-Route: <sip:62.140.159.242:5060;ipcs-
line=13516;lr;transport=tcp>
Supported: replaces
Via: SIP/2.0/TCP 192.168.37.2:5060;rport=4115;
branch=z9hG4bKcd2dab7310c61e43e5c68a8ca3d1c653
Date: Tue, 06 Nov 2018 13:11:34 GMT
Server: Cisco-SIPGateway/IOS-15.4.3.M3
Reason: Q.850;cause=16
P-RTP-Stat: PS=94,OS=16168,PR=93,OR=15996,PL=0,JI=0,LA=0,DU=2
Content-Length: 0

©2018 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.