



Application Notes for Configuring Avaya Communication Server 1000E, Avaya Aura® Session Manager and Avaya Aura® Session Border Controller to support Vodafone Netherlands Office Voice and Vodafone Netherlands OneVoice Corporate SIP Trunk Services - Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between Vodafone Netherlands Office Voice, Vodafone Netherlands OneVoice Corporate SIP Trunk Services and an Avaya SIP enabled enterprise solution. The Vodafone Netherlands Office Voice trunk is used for calls to and from fixed line PSTN locations, Vodafone Netherlands OneVoice Corporate trunk is used for calls to and from mobile telephone numbers as well as providing the ability for enterprise users to reach Vodafone mobile telephone numbers assigned to their account by dialing a four digit short code. The Avaya solution consists of Avaya Aura® Session Border Controller, Avaya Aura® Session Manager and Avaya Communication Server 1000E. Vodafone Netherlands are a member of the DevConnect Service Provider program.

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.

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between Vodafone Netherlands and an Avaya SIP enabled enterprise solution using Vodafone Netherlands Office Voice and Vodafone Netherlands OneVoice Corporate SIP Trunk Services. These services are offered in conjunction with each other as a total solution, for clarity these services will be collectively referred to in this document as Vodafone Netherlands SIP Trunk Solution. The Avaya solution consists of Avaya Aura® Session Border Controller (AASBC), Avaya Aura® Session Manager and Avaya Communication Server 1000E (CS1000E). Customers using this Avaya SIP enabled Enterprise solution with Vodafone Netherlands SIP Trunk Solution are able to place and receive calls via standards-based SIP trunks as an alternative to legacy Analogue or digital trunks.

The Vodafone Netherlands SIP Trunk Solution referenced within these Application Notes is designed for business customers. The solution provides two connections to the enterprise, Vodafone Netherlands Office Voice is a fixed line SIP trunk and Vodafone Netherlands OneVoice Corporate is a mobile SIP trunk. The Vodafone Netherlands Office Voice trunk is used for calls to and from fixed line PSTN locations, Vodafone Netherlands OneVoice Corporate trunk is used for calls to and from mobile telephone numbers as well as providing the ability for enterprise users to reach Vodafone mobile telephone numbers assigned to their account by dialing a four digit short code.

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 CS1000E, Session Manager and AASBC. The enterprise site was configured to use the SIP Trunk Solution provided by Vodafone Netherlands.

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

2.1. Interoperability Compliance Testing

The interoperability test included the following:

- Incoming PSTN calls to various phone types. Phone types included SIP, Unistim and digital telephones at the enterprise. All inbound PSTN calls were routed to the enterprise across the SIP trunk from the Service Provider.
- Outgoing calls from the enterprise site were completed via Vodafone Netherlands to PSTN destinations.
- Outgoing calls from the enterprise to the PSTN were made from SIP, Unistim and Digital telephones.
- Inbound and outbound PSTN calls to/from the Avaya one-X® Communicator soft phone.
- Calls to Emergency Services (112).

- Calls using G.729, and G.711A codec's.
- Fax calls to/from a fax machine at the enterprise to a PSTN connected fax machine.
- User features such as hold and resume, transfer, conference, call forwarding, etc.
- Caller ID Presentation and Caller ID Restriction.
- Call coverage and call forwarding for endpoints at the enterprise site.
- Transmission and response of SIP OPTIONS messages sent by Vodafone Netherlands requiring Avaya response and sent by Avaya requiring Vodafone Netherlands response.

2.2. Test Results

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

- No inbound toll free numbers were tested, however routing of inbound DID numbers and the relevant number translation was successfully tested.
- Mobile-X handoff works from twinned desk phone with patch p30260_1.ntl loaded on the CS1000E. INVITE sent to PSTN mobile contains no SDP information without the patch loaded, Vodafone do not support an INVITE with no SDP.
- Fax calls using T.38 for inbound and outbound with G.711 or G.729 do not work. Still under investigation.

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 Netherlands SIP trunk services, contact Vodafone Netherlands support at http://www.vodafone.nl/zakelijk/totaal_oplossingen/vast_en_mobiel/.

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an enterprise site connected to the Vodafone Netherlands SIP Trunk Solution. The Vodafone Netherlands Office Voice connection is represented in **Figure 1** as (Fixed) and the Vodafone Netherlands OneVoice Corporate connection is represented in **Figure 1** as (Mobile). Located at the Enterprise site is a Session Border Controller, Session Manager and CS1000E. Endpoints are Avaya 1140 series IP telephones, Avaya 1200 series (not shown in **Figure 1**) IP telephones (with Unistim and SIP firmware), Avaya one-X® Communicator, Avaya Digital telephone, Analogue telephone (not shown) and fax machine.

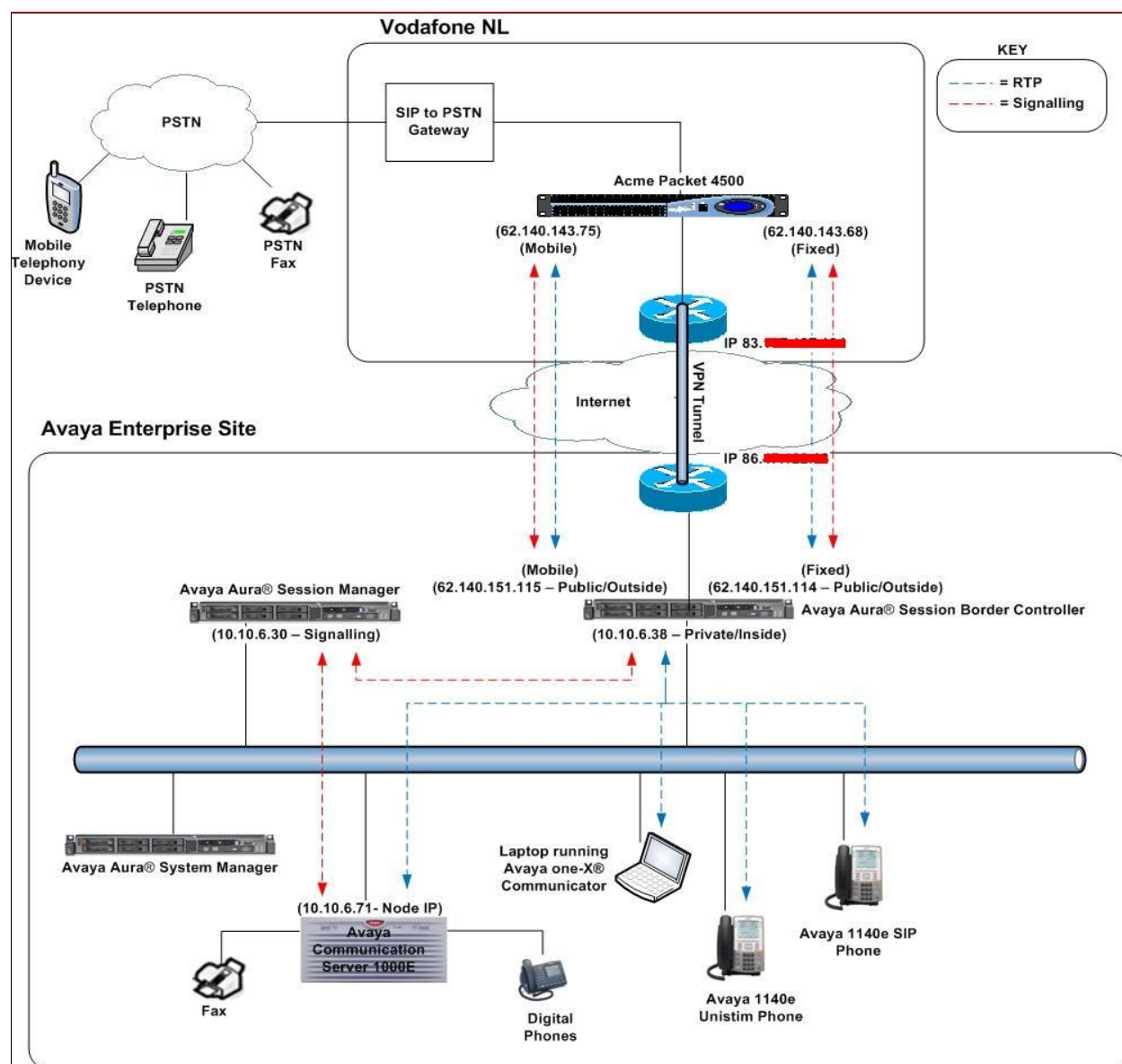


Figure 1: Avaya SIP Telephony Solution using Vodafone Netherlands Office Voice and Vodafone Netherlands OneVoice Corporate services

4. Equipment and Software Validated

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

Avaya Equipment	Software
Avaya S8800 Server	Avaya Aura® Session Manager R6.1 Service Pack 4 (6.1.4.0.614005)
Avaya S8800 Server	Avaya Aura® System Manager R6.1 Service Pack 4 (6.1.8.1.1551)
Avaya S8800 Server	Avaya Aura® Session Border Controller R6.1 (System Platform 6.0.3.3.3, Template E362M1)
Avaya Communication Server 1000E running on CP+PM server as co-resident configuration	Avaya Communication Server 1000E R7.5 Version 7.50.17 Deplst: X21 07.50Q All CS1000E patches listed in Appendix A
Avaya Communication Server 1000E Media Gateway	CSP Version: MGCC CD01 MSP Version: MGCM AB01 APP Version: MGCA BA07 FPGA Version: MGCF AA18 BOOT Version: MGCB BA07 DSP1 Version: DSP2 AB06
Avaya 1140e and 1230 Unistim Telephones	FW: 0625C8A
Avaya 1140e and 1230 SIP Telephones	FW: 04.01.13.00.bin
Avaya One-X ® Communicator	Version cs6.1.0.10-263
Avaya Analogue Telephone	N/A
Avaya M3904 Digital Telephone	N/A
Vodafone Netherlands	
Vodafone Office Voice	1.0
Vodafone OneVoice Corporate	1.0
ACME Packet Net-Net 4500	SCX6.2.0 MR-6 Patch 2 (Build 876)

5. Configure Avaya Communication Server 1000E

This section describes the steps required to configure Communication Server 1000E for SIP Trunking and also the necessary configuration for terminals (Analogue, SIP and IP phones). SIP trunks are established between Communication Server 1000E and Session Manager. These SIP trunks carry SIP signaling associated with Vodafone Netherlands SIP Trunk Service. For incoming calls, the Session Manager receives SIP messages from the AASBC, through which directs incoming SIP messages to Communication Server 1000E (see **Figure 1**). Once a SIP message arrives at Communication Server 1000E, 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 Communication Server 1000E and may be first subject to outbound features such as route selection, digit manipulation and class of service restrictions. Once Communication Server 1000E selects a SIP trunk, the SIP signaling is routed to the Session Manager. The Session Manager directs the outbound SIP messages to the SBC and on to

Vodafone's network. Specific Communication Server 1000E configuration as performed using Element Manager and the system terminal interface. The general installation of the Communication Server 1000E, System Manager and Session Manager is presumed to have been previously completed and is not discussed here. **Appendix A** has a list of all CS1000E patches, deplists and service packs loaded on the system.

5.1. Logging into the Avaya Communication Server 1000E

Log in using SSH to the ELAN ip address of the Call Server using a user with correct privileges. Once logged in type **csconsole** (not shown), this will take the user into the vxworks shell of the call server. Next type **logi** (not shown), the user will then be asked to login with correct credentials. Once logged in the user can then progress to load any overlay.

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 Communication Server 1000E 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 Vodafone Germany's 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 Communication Server 1000E.

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

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

TRADITIONAL TELEPHONES 32767 LEFT 32766 USED 1
DECT USERS             32767 LEFT 32767 USED 0
IP USERS               32767 LEFT 32744 USED 23
BASIC IP USERS         32767 LEFT 32766 USED 1
TEMPORARY IP USERS     32767 LEFT 32767 USED 0
DECT VISITOR USER      10000 LEFT 10000 USED 0
ACD AGENTS             32767 LEFT 32752 USED 15
MOBILE EXTENSIONS      32767 LEFT 32767 USED 0
TELEPHONY SERVICES     32767 LEFT 32767 USED 0
CONVERGED MOBILE USERS 32767 LEFT 32767 USED 0
NORTEL SIP LINES       32767 LEFT 32765 USED 2
THIRD PARTY SIP LINES  32767 LEFT 32761 USED 6
SIP CONVERGED DESKTOPS 32767 LEFT 32767 USED 0
SIP CTI TR87           32767 LEFT 32767 USED 0
SIP ACCESS PORTS      32767 LEFT 32752 USED 15
```

Load overlay 21, and confirm the customer is setup to use **ISDN** trunks (see 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 Codec's for Voice and FAX operation

Vodafone Netherland SIP Trunk service supports G.711A/G.729A voice codec's transmissions. Using the Communication Server 1000E element manager sidebar, navigate to the **IP Network → IP Telephony Nodes → Node Details → Voice Gateway VGW and Codecs** property page and configure the Communication Server 1000E General codec settings as in the next screenshot. The values highlighted below are system defaults but are required for correct operation.

Node ID: 11 - Voice Gateway (VGW) and Codecs

General | Voice Codecs | Fax

General

Echo cancellation: ☒ Use canceller, with tail delay: 128 ▾

☒ Dynamic attenuation

Voice activity detection threshold: -17 (-20 - +10 DBM)

Idle noise level: -65 (-327 - +327 DBM)

Signaling options: ☒ DTMF tone detection

☐ Low latency mode

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

☒ Modem/Fax pass-through

☒ V.21 Fax tone detection

☐ R factor calculation

Scrolling down the page, configure **G.711** and **G.729** codec settings. G.711 is enabled as default and cannot be disabled or enabled on the CS1000E. However, G.729 can be enabled or disabled, in this test G.729 was enabled and system defaults were used for payload size, jitter and delay. The relevant settings are highlighted in the following screenshot.

Node ID: 11 - 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 80 (milliseconds)

Nominal Maximum

Maximum delay may be automatically adjusted based on nominal settings.

☐ Voice Activity Detection (VAD)

Codec G722: ☐ Enabled

Voice payload size: 20 (milliseconds per frame)

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

Nominal Maximum

Maximum delay may be automatically adjusted based on nominal settings.

Codec G729: ☒ Enabled

Voice payload size: 20 (milliseconds per frame)

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

Finally configure **Fax** settings as highlighted in the screenshot below. System defaults were used. Please note T.38 cannot be disabled or enabled at the Node level and by default is enabled. Turning T.38 on or off is done at the endpoint level, by using different class of service as shown in **Section 5.7 Configure Analogue, Digital and IP Telephones**.

Node ID: 11 - Voice Gateway (VGW) and Codecs

General | Voice Codecs | Fax

Codec G723.1: ☐ Enabled

Voice payload size: 30 (milliseconds per frame)

Voice playout (jitter buffer) delay: 60 120 (milliseconds)

Nominal Maximum

Maximum delay may be automatically adjusted based on nominal settings.

Coding rate: 5.3 (kbps)

Fax

Codec name: T.38 FAX

Maximum rate: 14400 (bps)

Fax TCF method: 2

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

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

Packet size: 30 (bps)

5.4. Virtual Trunk Gateway Configuration

Use Communication Server 1000E 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. At this stage the call server has an ip address and so too does the signalling server. The Node ip is the ip address that the IP phones use to register. When an entity link is added in Session Manager for the CS1000E it is the Node IPv4 address that is used (see **Section 6.5 – Define SIP Entities** for more details).

Node Details (ID: 11 - SIP Line, LTPS, PD, Gateway (SIPGw))

Node ID: * (0-9999)

Call server IP address: *

TLAN address type: ☒ IPv4 only
☐ IPv4 and IPv6

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

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

Node IPv6 address:

* Required Value. Save Cancel

Associated Signaling Servers & Cards

Select to add ▼ Add Remove Make Leader Print | Refresh

<input type="checkbox"/> Hostname ▲	Type	Deployed Applications	ELAN IP	TLAN IPv4	Role
<input type="checkbox"/> cpcm7-5	Signaling_Server	SIP Line, LTPS, Gateway, PD, Presence Publisher, IP Media Services	192.168.2.50	10.10.6.70	Leader

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, in this case **avaya.com**. The SIP Domain Name configured in the Signaling Server properties must match the Service Domain name configured in the Session Manager, see **Section 6.2**
- **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 **11**
- **Proxy or Redirect Server: Primary TLAN IP** address is the SIP signalling interface ip address of the Session Manager. The **Transport protocol** used for SIP, in this case is **TCP**
- **SIP URI Map: Public E.164 – National, Subscriber and Private – Vacant Number** are left blank. All other fields in the SIP URI Map are left with default values

Node ID: 11 - 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: cppm7-5 *
 Gateway password: *
 Application node ID: 11 * (0-9999)
 Enable failsafe NRS: ☐

Virtual Trunk Network Health Monitor

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

Proxy Or Redirect Server:

Proxy Server Route 1:

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

Port: (1 - 65535)

Transport protocol:

Options: ☐ Support registration
☐ Primary CDS proxy

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"/>	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"/>
	Unknown: <input type="text" value="UnknownUnknown"/>

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 that are not shared with other resources and best practice dictates that IP telephones and Media Gateways are all placed in a separate zone than SIP trunks. In the sample configuration SIP trunks use zone 20 and IP Telephones use zone 10, system defaults were used for each zone other than the parameter configured for **Zone Intent**. For SIP Trunks (zone 20), **VTRK** is configured for **Zone Intent**. For IP Telephones (zone 10), **MO** is configured for **Zone Intent**.

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.

AVAYA CS1000 Element Manager Help | Login

Managing: 192.168.0.2 Username: admin
System > IP Network > Zones > Bandwidth Zones

Bandwidth Zones

Zone	Intrazone Bandwidth	Intrazone Strategy	Interzone Bandwidth	Interzone Strategy	Resource Type	Zone Intent	Description
1 <input type="radio"/> 10	1000000	BQ	1000000	BQ	SHARED	MO	MAINOFFICE
2 <input type="radio"/> 20	1000000	BQ	1000000	BQ	SHARED	VTRK	VTRK

5.6. Configure SIP Trunks

Communication Server 1000E virtual trunks will be used for all inbound and outbound PSTN calls to Vodafone Netherland's SIP Trunk Service. Five separate steps are required to configure Communication Server 1000E virtual trunks:-

- Configure a D-Channel Handler (DCH); configure using the Communication Server 1000E system terminal and overlay 17
- Configure a SIP trunk Route Data Block (RDB); configure using the Communication Server 1000E system terminal and overlay 16
- Configure SIP trunk members; configure using the Communication Server 1000E system terminal and overlay 14
- Configure a Route List Block (RLB); configure using the Communication Server 1000E system terminal and overlay 86
- Configure Special Prefix Numbers (SPN's); configure using the Communication Server 1000E system terminal and overlay 90

The following is an example DCH configuration for SIP trunks. Load **Overlay 17** at the Communication Server 1000E 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 10
CTYP DCIP
DES  VIR_TRK
USR  ISLD
ISLM 4000
SSRC 1800
OTBF 32
NASA YES
IFC  SL1
CNEG 1
RLS  ID  5
RCAP ND2
MBGA NO
H323
OVLR NO
OVLS NO
```

Next, configure the SIP trunk Route Data Block (RDB) using the Communication Server 1000E 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 **SIP_VTRK**, which is zone 20. The remaining highlighted values are important for correct SIP trunk operation.

Overlay 16 TYPE: rdb CUST 00 ROUT 100 TYPE RDB CUST 00 ROUT 100 DES VIR_TRK TKTP TIE NPID_TBL_NUM 0 ESN NO RPA NO CNVT NO SAT NO RCLS EXT VTRK YES ZONE 0020 PCID SIP CRID NO NODE 11 DTRK NO ISDN YES MODE ISLD DCH 10 IFC SL1 PNI 00001 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 1600 TCPP NO PII NO AUXP NO TARG CLEN 1 BILN NO OABS INST IDC NO 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 Communication Server 1000E 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 160 0 0 0
DATE
PAGE
DES VIR_TRK
TN 160 0 00 00 VIRTUAL
TYPE IPTI
CDEN 8D
CUST 0
XTRK VTRK
ZONE 0020
TIMP 600
BIMP 600
AUTO_BIMP NO
NMUS NO
TRK ANLG
NCOS 0
RTMB 100 1
CHID 1
TGAR 1
STRI/STRO WNK WNK
SUPN YES
AST NO
IAPG 0
CLS TLD DTN CND ECD WTA LPR APN THFD XREP SPCD MSBT
P10 NTC
TKID
AACR NO

```

Configure a Digit Manipulation Index (DMI) in overlay 87. Load **Overlay 87** at the system terminal and type **new**, at the **FEAT** prompt type **dgt** and at the **DMI** prompt set this to a unique **DMI** value. **DMI 1** is used for all traffic outgoing to the PSTN. No digits were deleted as the **DEL** prompt is set to **0**. Call type (**CTYP**) set to **UKWN**.

```

Overlay 87
REQ new
FEAT dgt
DMI 1
DEL 0
ISPN NO
CTYP UKWN

```

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. This RLB was defined for international traffic and uses the **DMI 1** as previously entered in overlay 87.

Overlay 86		
new		
CUST	0	
FEAT	rlb	
RLI	66	
ELC	NO	
ENTR	0	
LTER	NO	
ROUT	100	
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	1	
CTBL	0	
ISDM	0	
		FCI 0
		FSNI 0
		BNE NO
		DORG NO
		SBOC NRR
		PROU 1
		IDBB DBD
		IOHQ NO
		OHQ NO
		CBQ NO
		ISSET 0
		NALT 5
		MFRL 0
		OVLL 0

Next, configure Trunk Steering Codes(s) (TSC) which users will dial to reach PSTN numbers. Use the Communication Server 1000E system terminal and overlay 87. The following are some example TSC 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	00	TSC	06
FLEN	14	FLEN	10
ITOH	NO	ITOH	NO
RLI	66	RLI	66

5.7. Configure Analogue, Digital and IP Telephones

A variety of telephone types were used during the testing, the following is the configuration for the Avaya 1140e Unistim IP telephone. Load overlay 20 at the system terminal and enter the following values. A unique five digit number is entered for the **KEY 00** and **KEY 01** value. The value for **CFG_ZONE** is the same value used in **Section 5.5** for **VIRTUALSETS**, which is zone 10.

Overlay 20 IP Telephone configuration

```
DES 1140
TN 096 0 01 16 VIRTUAL
TYPE 1140
CDEN 8D
CTYP XDLC
CUST 0
NUID
NHTN
CFG_ZONE 00010
CUR_ZONE 00010
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 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 CCBD 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 9074 0      MARP
      CPND
        CPND_LANG ROMAN
        NAME IP1140
        XPLN 10
        DISPLAY_FMT FIRST, LAST
01 MCR 9074 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 HBTB AHA IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
    DRDD EXR0
    USMD USRD ULAD CCBD RTDD RBDD RBHD PGND OCBD FLXD FTTC DNDY DNO3 MCBN
    FDSD NOVD 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 9072 0 MARP

CPND

CPND_LANG ROMAN

NAME Digital Set

XPLN 10

DISPLAY_FMT FIRST, LAST

01 MCR 9072 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

Analogue telephones are also configured using **Overlay 20**, the following example shows an Analogue port configured for Plain Ordinary Telephone Service (POTS) and also configured to allow T.38 Fax transmission. A unique value is entered for **DN**, this is the extension number. In the class of service (**CLS**) field **DTN** is required if the telephone uses DTMF dialing. Values **FAXA** and **MPTD** configure the port for T.38 Fax transmissions.

Overlay 20 - Analogue Telephone Configuration

```
DES 500
TN 100 0 00 03
TYPE 500
CDEN 4D
CUST 0
MRT

ERL 00000
WRLS NO
DN 9071
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 CCB D BNRD OCB D 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
```

5.8. Configure the SIP Line Gateway Service

SIP terminal operation requires the Communication Server 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 Communication Server 1000E system terminal and overlay 15 to activate SIP Line services, as in the following example where **SIPL_ON** is set to **YES**.

```
SLS_DATA
SIPL_ON YES
UAPR 78
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. The value for **SIP Domain Name** must match that configured in **Section 7.1**.

- **SIP line Gateway Application:** Enable the SIP line service on the Node, check the box to enable.
- **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: 192.168.2.50 Username: hardip
System » IP Network » IP Telephony Nodes » Node Details » SIP Line Configuration

Node ID: 11 - 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: Add

Monitor addresses: Remove

5.9. Configure SIP Line Telephones

When SIP Line service configuration is completed, use the Communication Server 1000E 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 set for **MAINOFFICE** in **Section 5.5**. A unique telephone number is entered for value **KEY 00**. The value for **KEY 01** is comprised of the **UAPR** value (set to 78 previously in this section) and the telephone number used in **KEY 00**.

Overlay 20 - SIP Telephone Configuration

```
DES SIPD
TN 096 0 01 15 VIRTUAL
TYPE UEXT
CDEN 8D
CTYP XDLC
CUST 0
UXTY SIPL
MCCL YES
SIPN 1
SIP3 0
FMCL 0
TLSV 0
SIPU 9079
NDID 5
SUPR NO
SUBR DFLT MWI RGA CWI MSB
UXID
NUID
NHTN
CFG_ZONE 00010
CUR_ZONE 00010
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---

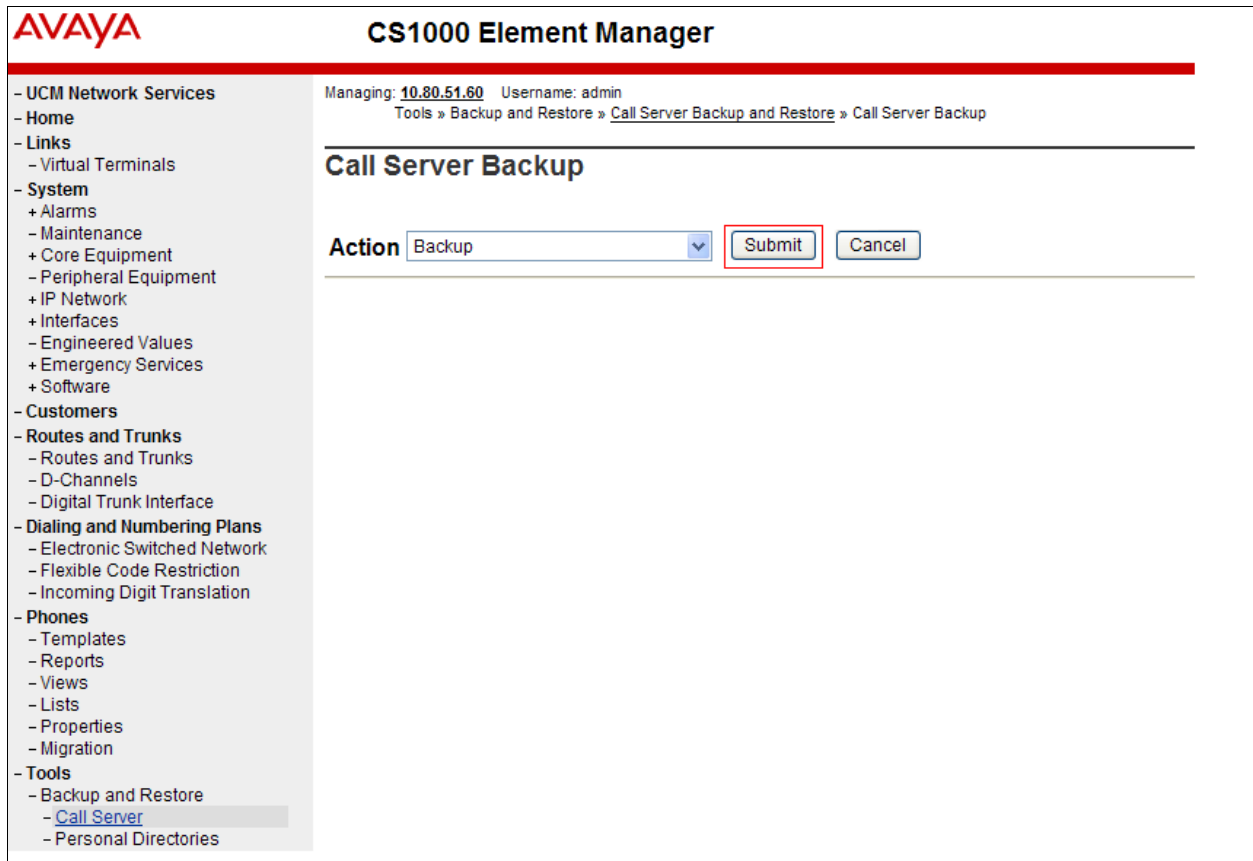
---continued from previous page---

```
UDI RCC HBTD AHA IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
DRDD EXR0
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 9079 0 MARP
    CPND
        CPND_LANG ROMAN
        NAME Sigma 1140
        XPLN 11
        DISPLAY_FMT FIRST, LAST*
01 HOT U 789079 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
```

5.10. 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. 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.



AVAYA **CS1000 Element Manager**

Managing: **10.80.51.60** Username: admin
Tools » Backup and Restore » Call Server Backup and Restore » Call Server Backup

Call Server Backup

Action

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

```
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.
```

Configuration of Communication Server 1000E is complete.

6. Configuring Avaya Aura® Session Manager

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

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

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.

The screenshot displays the Avaya Aura System Manager 6.1 web interface. At the top, the Avaya logo is on the left, the title "Avaya Aura™ System Manager 6.1" is in the center, and navigation links "Help | About | Change Password | Log off admin" are on the right. The main content area is divided into three columns, each with an orange header and a list of menu items:

- Users**
 - Administrators**: Manage Administrative Users
 - Groups & Roles**: Manage groups, roles and assign roles to users
 - Subscribers**: Manage users and shared resources associated with CS1000, including LDAP/file import and export
 - Synchronize and Import**: Synchronize users with the enterprise directory, import users from file
 - UCM Roles**: Manage UCM Roles, assign roles to users
 - User Management**: Manage users, shared user resources and provision users
- Elements**
 - Application Management**: Manage applications and application certificates
 - Communication Manager**: Manage Communication Manager objects
 - Conferencing**: Conferencing
 - Inventory**: Manage, discover, and navigate to elements, update element software
 - Messaging**: Manage Messaging System objects
 - Presence**: Presence
 - Routing**: Network Routing Policy
 - SIP AS 8.1**: SIP AS 8.1
 - Session Manager**: Session Manager Element Manager
- Services**
 - Backup and Restore**: Backup and restore System Manager database
 - Configurations**: Manage system wide configurations
 - Events**: Manage alarms, view and harvest logs
 - Licenses**: View and configure licenses
 - Replication**: Track data replication nodes, repair replication nodes
 - Scheduler**: Schedule, track, cancel, update and delete jobs
 - Security**: Manage Security Certificates
 - Templates**: Manage Templates for Communication Manager and Messaging System objects
 - UCM Services**: Manage UCM applications and navigation such as CS1000 deployment, patching, ISSS and SNMP

6.2. Administer SIP Domain

To add the SIP domain that will be used with Session Manager, select **Routing** from the **Home** tab menu (not shown) and in the resulting tab select **Domains** from left hand menu. Click the **New** button to create a new SIP domain entry. In the **Name** field enter the domain name (e.g., **avaya.com**) and optionally a description for the domain in the **Notes** field. Click **Commit** to save changes (Not shown). The screen below shows the SIP domain that was previously configured.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The top header displays the Avaya logo, the system name "Avaya Aura® System Manager 6.1", and links for "Help", "About", "Change Password", and "Log off admin". The left-hand navigation menu is expanded to show "Routing", with sub-items including "Domains", "Locations", "Adaptations", "SIP Entities", "Entity Links", "Time Ranges", "Routing Policies", "Dial Patterns", "Regular Expressions", and "Defaults". The "Domains" sub-item is selected. The main content area is titled "Domain Management" and includes a breadcrumb trail: "Home / Elements / Routing / Domains - Domain Management". Below the breadcrumb, there are buttons for "Edit", "New", "Duplicate", "Delete", and a "More Actions" dropdown. A table displays the domain entries, with one entry highlighted: "avaya.com" of type "sip". The table has columns for "Name", "Type", "Default", and "Notes". The "Default" column for "avaya.com" contains a checkbox. Below the table, there is a "Select" dropdown menu set to "All, None".

Name	Type	Default	Notes
avaya.com	sip	<input type="checkbox"/>	

6.3. Administer Locations

Locations can be used to identify logical and/or physical locations where SIP Entities reside, for the purposes of bandwidth management. One location is added to the sample configuration for all of the enterprise SIP entities. On the **Routing** tab select **Locations** from the left hand menu. Under **General**, in the **Name** field enter an informative name for the location and optionally a description for the location in the **Notes** field. Scroll to the bottom of the page and under **Location Pattern**, click **Add**, then enter an **IP Address Pattern** in the resulting new row, '*' is used to specify any number of allowed characters at the end of the string. Below is the location configuration used for the simulated enterprise.

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

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

Routing **Home / Elements / Routing / Locations - Location Details**

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

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

General

* **Name:**
Notes:

Overall Managed Bandwidth

Managed Bandwidth Units:
Total Bandwidth:

Per-Call Bandwidth Parameters

* **Default Audio Bandwidth:**

Location Pattern

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

1 Item [Refresh](#) [Filter: Enable](#)

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	*10.10.6.*	

Select : All, None

6.4. Administer Adaptation Module

Session Manager is installed with a module called DigitConversionAdapter, which can convert digit strings in various message headers as well as host names in the Request-URI (Uniform Resource Identifier). In this configuration the adaptation is used by the Session Manager to ensure ingress messages have the hostname **avaya.com** when they are sent to the CS1000E. Also the adaptation was used to strip MIME messages before being sent on to Vodafone. Vodafone does not support MIME. To add an adaptation, select **Adaptations** on the left panel menu and then click on the **New** button (not shown). Under **General**:

- **Adaptation Name:** Enter an informative name, in the sample configuration **strip + from incoming PSTN calls** was used
- **Module Name:** <click to add module> from the drop down list and enter “DigitConversionAdapter” in the resulting **New Module Name** field
- **Module Parameter:** Enter **fromto=true** to allow the From and To headers to be modified by Session Manager (i.e., in addition to other headers such as the P-Asserted-Identity and Request-URI headers)
Enter **MIME=no** to have Session Manager strip MIME message bodies on egress to Vodafone SBC, such that only SDP is present in the message body sent to Vodafone’s SBC

The whole string in module parameter is **MIME=no fromto=true**

The screenshot shows the Avaya Aura System Manager 6.1 web interface. The left sidebar contains a navigation menu with the following items: Routing, Domains, Locations, Adaptations (highlighted with a red box), SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'Home / Elements / Routing / Adaptations- Adaptation Details'. Below this, there is a 'Commit' button. The 'General' tab is selected, and a red box highlights the following fields: 'Adaptation name' with the value 'strip + from incoming PSTN calls', 'Module name' with a dropdown menu showing 'DigitConversionAdapter', and 'Module parameter' with the value 'MIME=no fromto=true'. Below these fields are 'Egress URI Parameters' and 'Notes' input fields.

Scroll down and make corresponding changes in the **Digit Conversion for Outgoing Calls from SM** section for calls from Vodafone to CS1000E users.

- **Matching Pattern:** In the sample configuration, + was used
- **Min:** Enter minimum number of digits (e.g., **1**)
- **Max:** Enter maximum number of digits (e.g., **36**)
- **Delete Digits:** Enter **1** to strip off +
- **Insert Digits:** Enter digits that need to be inserted
- **Address to modify:** Select **both**

Click **Commit** to save .

Digit Conversion for Outgoing Calls from SM

Add Remove

1 Item Refresh Filter: Enable

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
* +	* 1	* 36		* 1		both	

Select : All, None

* Input Required

Commit Cancel

6.5. Administer SIP Entities

A SIP Entity must be added for each SIP-based telephony system supported by a SIP connection to the 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 fields will need to be populated 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 signaling interface on the connecting system.
- In the **Type** field use **Session Manager** for a Session Manager SIP entity, **SIP TRUNK** for CS1000E SIP entity and **Gateway** for the AASBC SIP entity.
- In the adaptation field select the created adapation in **Section 6.4** for the CS1000E and AASBC 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 three SIP Entities.

- Session Manager SIP Entity
- Communication Server 1000E SIP Entity
- Session Border Controller 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 signaling interface.

AVAYA Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing x Home

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

SIP Entity Details

General

* Name: sesmgr02

* FQDN or IP Address: 10.10.6.30

Type: Session Manager

Notes:

Location: Enterprise

Outbound Proxy:

Time Zone: Etc/GMT

Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

The 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 **avaya.com** as the default domain.

Port

Add Remove

3 Items Refresh

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

Select : All, None

6.5.2. Avaya Communication Server 1000E SIP Entity

The following screens show the SIP entity for Communication Server 1000E. The **FQDN or IP Address** field is set to the IP address of the Node IP configured in **Section 5.4**. Note the adaptation created in **Section 6.4** is applied to this entity link.

AVAYA Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off ad

Routing x H

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

SIP Entity Details

Commit Car

General

* Name: cpcm7-5

* FQDN or IP Address: 10.10.6.71

Type: SIP Trunk

Notes:

Adaptation: strip + from incoming PSTN calls

Location: Enterprise

Time Zone: Europe/Dublin

Override Port & Transport with DNS SRV: ☐

6.5.3. Avaya Aura® Session Border Controller SIP Entity

The following screen shows the SIP Entity for the AASBC. The **FQDN or IP Address** field is set to the IP address of the AASBC private network interface. Note the adaptation created in **Section 6.4** is applied to this entity link.

AVAYA Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off ad

Routing x H

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

SIP Entity Details

Commit Canc

General

* Name: AASBC01

* FQDN or IP Address: 10.10.6.38

Type: Gateway

Notes:

Adaptation: strip + from incoming PSTN calls

Location: Enterprise

Time Zone: Europe/Amsterdam

Override Port & Transport with DNS SRV: ☐

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

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 and in the resulting screen 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 the SIP Entity for SessionManager i.e. **sesmgr02**.
- 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 the **Trusted** tick box to make the other system trusted.
- In the **Protocol** field enter the transport protocol to be used to send SIP requests.

Click **Commit** to save changes (not shown). The following screen shows the Entity Links used in this configuration.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The left sidebar contains a menu with 'Entity Links' highlighted. The main content area displays the 'Entity Links' configuration page. At the top, there are buttons for 'Edit', 'New', 'Duplicate', 'Delete', and 'More Actions'. Below these buttons, a table lists 6 items. The table has columns for 'Name', 'SIP Entity 1', 'Protocol', 'Port', 'SIP Entity 2', 'Port', 'Connection Policy', and 'Notes'. Two rows are visible in the table, both with a 'Trusted' connection policy.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
AASBC01 TCP	sesmgr02	TCP	5060	AASBC01	5060	Trusted	
sesmgr02 cppm7-5 5060 TCP	sesmgr02	TCP	5060	cppm7-5	5060	Trusted	

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**, select the default **24/7** time range.

The following screen shows the routing policy for Communication Server 1000E

The screenshot shows the 'Routing Policy Details' form for a policy named 'cs1k7-5sig_server'. The left sidebar contains a menu with 'Routing Policies' highlighted. The main form area is divided into three sections: 'General', 'SIP Entity as Destination', and 'Time of Day'. In the 'General' section, the 'Name' field is populated with 'cs1k7-5sig_server'. In the 'SIP Entity as Destination' section, a table lists the destination entities. In the 'Time of Day' section, a table shows the time range '24/7' is selected.

Routing Policy Details

General

* Name: cs1k7-5sig_server

Disabled: ☐

Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
cppm7-5	10.10.6.71	SIP Trunk	

Time of Day

Add Remove View Gaps/Overlaps

1 Item Refresh Filter: En

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
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

The following screen shows the routing policy for the AASBC

AVAYA

Avaya Aura® System Manager 6.1

Help | About | Change Password | Log off admin

Routing

Home

Routing

Domains

Locations

Adaptations

SIP Entities

Entity Links

Time Ranges

Routing Policies

Dial Patterns

Regular Expressions

Defaults

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

Routing Policy Details

Help ?

Commit

Cancel

General

* Name: CallsToSBC

Disabled: ☐

Notes: Calls routing to swisscom

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
AASBC01	10.10.6.38	Gateway	

Time of Day

Add

Remove

View Gaps/Overlaps

1 Item Refresh

Filter: Enable

Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
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 dialed number or prefix to be matched
- In the **Min** field enter the minimum length of the dialed number
- In the **Max** field enter the maximum length of the dialed number
- In the **SIP Domain** field select **-ALL-** to allow calls from any domain to match the dial pattern

Under **Originating Locations and Routing Policies**. Click **Add**, in the resulting screen (not shown), under **Originating Location** select **ALL** and under **Routing Policies** select the appropriate routing policy defined in **Section 6.7**. Click the **Commit** button to save. The following screen shows an example dial pattern configured for AASBC which will route the calls out to the Vodafone Netherlands SIP Trunk Solution.

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

Dial Pattern Details

General

* Pattern: 06

* Min: 2

* Max: 36

Emergency Call: ☐

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	CallsToSBC	0	<input type="checkbox"/>	AASBC01	

Select : All, None

The following screen shows an example dial pattern configured for Communication Server 1000E.

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

Dial Pattern Details [Help](#)

General

* Pattern:
* Min:
* Max:
Emergency Call: ☐
SIP Domain:
Notes:

Originating Locations and Routing Policies

1 Item | Refresh Filter: Enable

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	cs1k7-5sig_server	0	<input type="checkbox"/>	cppm7-5	

Select : All, None

7. Configure Avaya Aura® Session Border Controller

This section describes the configuration of the AASBC. This configuration is done in two parts. The first part is done during the AASBC installation via the installation wizard. These Application Notes will not cover the AASBC installation in its entirety but will include the use of the installation wizard. For information on installing the System Platform and the loading of the AASBC template see [1] & [2]. The second part of the configuration is done after the installation is complete using the AASBC web interface.

7.1. Installation Wizard

During the installation of the AASBC template, the installation wizard will prompt the installer for information that will be used to create the initial configuration of the AASBC. The first screen of the installation wizard is the Network Settings screen. Fill in the fields as described below and shown in the following screen:

- In the **IP Address** field enter the IP address of the private side of the AASBC
- In the **Hostname** field enter a host name for the AASBC
- Specify a domain in the **Domain** and **Default Domain** fields

Click **Next Step** (not shown) to continue

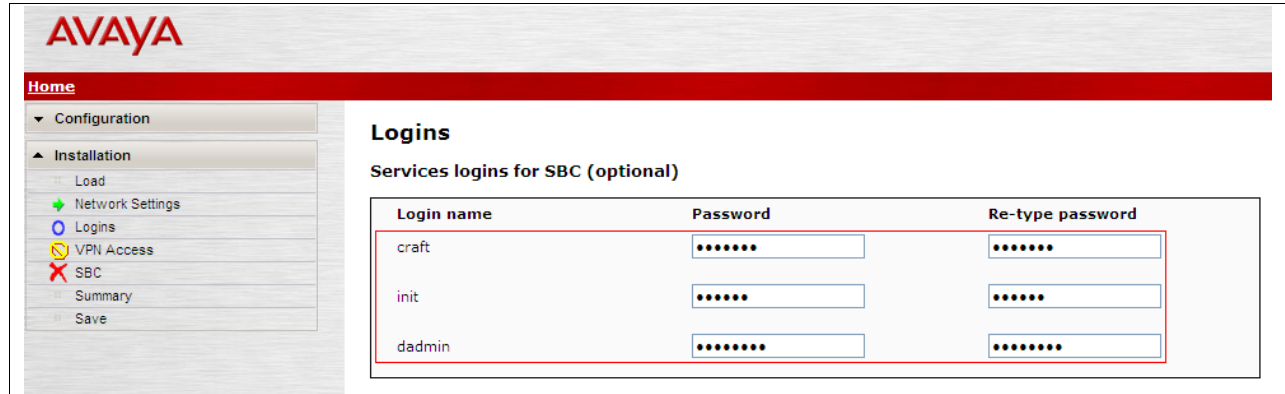
The screenshot shows the Avaya Aura Session Border Controller (AASBC) Network Settings installation wizard. The interface has a red header with the Avaya logo and a navigation menu on the left. The main content area is titled "Network Settings" and "Enter network settings". It contains several input fields for network configuration, including Domain-0 IP Address, CDom IP Address, Gateway IP Address, Network Mask, Primary DNS, Secondary DNS (Optional), Default Search List (Optional), and HTTPS Proxy (Optional). Below these fields is a table for Virtual Machine settings, which includes columns for Virtual Machine, IP Address, Hostname, and Domain. The table has one row for the SBC virtual machine. A red box highlights the Domain and Default Domain fields in the table. An "Apply to all VMs" button is located at the bottom right of the table.

Virtual Machine	IP Address	Hostname	Domain
SBC	10.10.6.38	AASBC01Vlan6	avaya.com (Optional)

Default Domain: avaya.com (Optional)

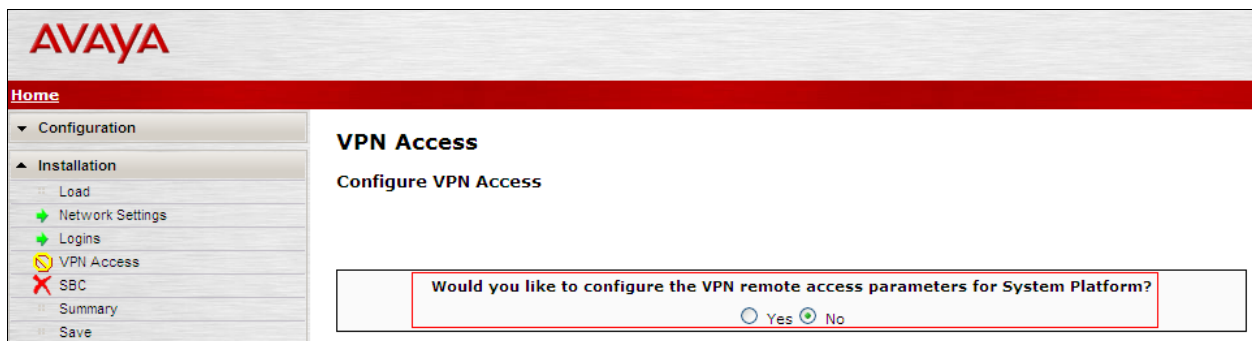
Apply to all VMs

From the **Logins** screen specify passwords for the services logins to the AASBC.



Login name	Password	Re-type password
craft	*****	*****
init	*****	*****
dadmin	*****	*****

VPN remote access to the AASBC was not part of the compliance test. Thus, on the VPN Access screen, select **No** to the question, **Would you like to configure the VPN remote access parameters for System Platform?**



Would you like to configure the VPN remote access parameters for System Platform?

☐ Yes ☒ No

On the **SBC** screen, in the **SIP Service Provider Data** section fill in the fields as described below and shown in the following screen:

- In the **Service Provider** select the name of the Service Provider to which the AASBC will connect. This will allow the wizard to select a configuration file customized for this Service Provider. At the time of the compliance test, a customized configuration file did not exist for Vodafone Netherlands. Thus, **Generic** was chosen
- In the **Port** field enter the port number that Vodafone Netherlands uses to listen for SIP traffic
- In the **IP Address1** field enter the IP addresses provided by Vodafone Netherlands for the Vodafone Office Voice SIP Trunk Service (fixed). The IP address for the Vodafone OneVoice Corporate SIP Trunk Service (mobile) used during testing will be added after the AASBC template is installed (**Section 7.3**)
- In the **Signaling/Media Network1** field enter the Vodafone Netherlands provided subnet where media traffic will originate. An additional subnet can be provided for **Signaling/Media Network2**
- In the **Media Netmask** field enter the netmask corresponding to the Media Network
- Scroll down to continue

The screenshot shows the Avaya SBC configuration interface. On the left is a navigation menu with options: Home, Configuration, Installation, Load, Network Settings, Logins, VPN Access, SBC, Summary, and Save. The main area is titled 'SBC' and 'Session Border Controller Data'. Within this, there is a section for 'SIP Service Provider Data'. This section contains several input fields: 'Service Provider' (a dropdown menu set to 'Generic'), 'Port' (a text box with '5060'), 'IP Address1' (a text box with '62.140.143.68'), 'Signalling/Media Network1' (a text box with '62.140.143.0'), and 'Signalling/Media Netmask1' (a text box with '255.255.255.0'). Below these are optional fields: 'IP Address2 (Optional)', 'Signalling/Media Network2 (Optional)', 'Signalling/Media Netmask2 (Optional)', and 'Hunting (Optional)' (a dropdown menu). A red rectangle highlights the 'Service Provider', 'Port', 'IP Address1', 'Signalling/Media Network1', and 'Signalling/Media Netmask1' fields.

Further down on the same **SBC** screen, in the **SBC Network Data** section fill in the fields as described below:

- In the **Public IP Address** field enter the enterprise IP address that will be used for the Vodafone Netherlands Office Voice SIP Trunk Service on the public side of the AASBC
- In the **Public Net Mask** field enter the netmask associated with the public network to which the AASBC connects
- In the **Public Gateway** field enter the default gateway of the public network

In the **Enterprise SIP Server** section fill in the fields as described below:

- In the **SIP Domain** field enter the enterprise SIP domain
- In the **IP Address** field enter the IP address of the Enterprise SIP Server to which the AASBC will connect. In the case of the compliance test, this is the IP address of the Session Manager SIP signaling interface
- In the **Transport1** field select the transport protocol to be used for SIP traffic between the AASBC and Session Manager

Click **Next Step** to continue. A summary screen will be displayed (not shown). Check the displayed values and click **Next Step** again to install the template with the values entered.

SBC Network Data			
Interface	IP Address	Net Mask	Gateway
Private (Management)	10.10.6.38	255.255.255.0	10.10.6.1
Public	62.140.151.114	255.255.255.240	62.140.151.113

Enterprise SIP Server		
SIP Domain avaya.com		
IP Address1 10.10.6.30	Transport1 TCP	
IP Address2 (Optional) 	Transport2 (Optional) 	Hunting (Optional)

7.2. Access Avaya Aura® Session Border Controller

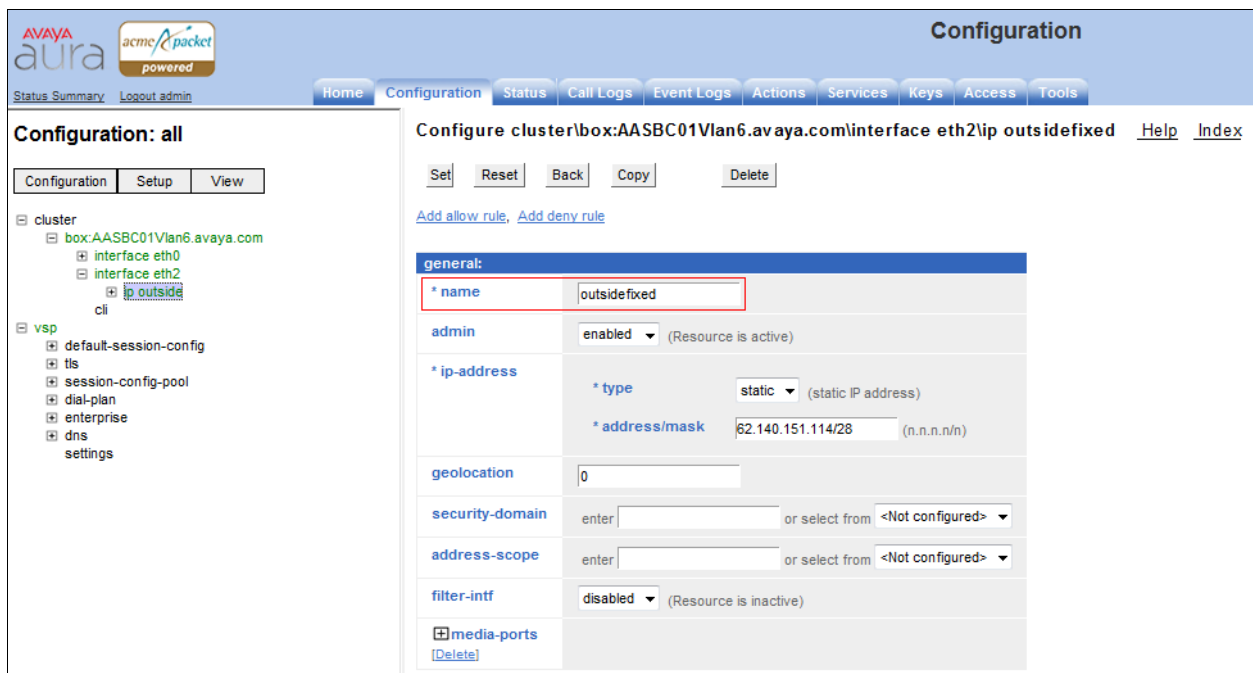
Access the AASBC using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the private IP address configured in **Section 7.1**. Log in with the appropriate credentials.



The image shows the login page for the Acme Packet Net-Net OS-E management interface. The title is "Acme Packet Net-Net OS-E". Below the title, a message states: "To access the NNOS-E management interface, you must first log in. Please provide your user name and password." There are two input fields: "Username:" and "Password:". Below these fields is a "Login" button.

7.3. Configure Outside Interfaces

To allow two logical connections to be created between the enterprise and Vodafone Netherlands an additional IP address is created on the outside interface of the AASBC. Rename the IP address configuration created in **Section 7.1** by expanding **cluster** → **box:AASBC01Vlan6.avaya.com** → **interface eth2** → **ip outside** and enter a descriptive name in the **name** field. The name **outsidefixed** is used as this is the IP address that will be used for the Vodafone Office Voice SIP Trunk Service. Scroll down to continue.



The image shows the Avaya Aura Configuration page for the interface eth2. The page title is "Configuration". The breadcrumb trail is "Configure cluster\box:AASBC01Vlan6.avaya.com\interface eth2\ip outsidefixed". The page has tabs for "Set", "Reset", "Back", "Copy", and "Delete". There are links for "Add allow rule" and "Add deny rule". The "general" section is expanded, showing the following fields:

- * name: outsidefixed
- admin: enabled (Resource is active)
- * ip-address:
 - * type: static (static IP address)
 - * address/mask: 62.140.151.114/28 (n.n.n.n/n)
- geolocation: 0
- security-domain: enter [] or select from <Not configured>
- address-scope: enter [] or select from <Not configured>
- filter-intf: disabled (Resource is inactive)
- media-ports: [Delete]

Further down on the same screen in the **routing** section click the edit link relating to the **route external-sip-media-1** route.

<div> <div>+</div> <div>routing</div> </div> <div> <div>Delete</div> </div>	route					
		route	admin	destination	gateway	metric
	<a>Edit <a>Delete	<a>route Default	disabled	default	0.0.0.0	1
	<a>Edit <a>Delete	<a>route external-sip-media-1	enabled	network 62.140.143.0/24	62.140.151.113	1

Add route

In the resulting screen in the **destination** section, select **host** from the **type** drop down menu. In the **address** field enter the IP address of the Vodafone Netherlands Office Voice SIP trunk service.

Configure clusterbox:AASBC01Vlan6.avaya.cominterface eth2lip outsidefixedlroutingroute external-sip-media-1

Help Index

Set
Reset
Back
Copy
Delete

admin	<div>enabled</div> <div>(Resource is active)</div>
* route-name	external-sip-media-1
* destination	<div> <div>* type</div> <div>host</div> <div>(host route)</div> </div> <div> <div>* address</div> <div>62.140.143.68</div> <div>(n.n.n.n)</div> </div>
* gateway	<div>62.140.151.113</div> <div>(n.n.n.n)</div>
metric	<div>1</div> <div>(from 0 to 1,000,default=1)</div>

Set
Reset
Back
Copy

To create another IP address configuration navigate to **box:AASBC01Vlan6.avaya.com** → **interface eth2** → **ip outsidexfixed** and click **copy** (Not shown). In the resulting screen update the fields as shown below:

- In the **name** field enter a descriptive name. The name **outsidemobile** is used as this is the IP address that will be used for the Vodafone OneVoice Corporate SIP Trunk Service. Scroll down to continue.
- In the **address/mask** field enter the IP address that will be used on the public side of the AASBC for the Vodafone OneVoice Corporate SIP Trunk Service.

Scroll down to continue.

The screenshot shows the Avaya Aura Configuration interface. The left sidebar shows a tree view with 'cluster' expanded, showing 'box:AASBC01Vlan6.avaya.com' and its interfaces. The main area is titled 'Configure cluster:box:AASBC01Vlan6.avaya.cominterface eth2ip outsidemobile'. It has buttons for 'Set', 'Reset', 'Back', 'Copy', and 'Delete'. Below these are links for 'Add allow rule' and 'Add deny rule'. The 'general' section contains the following fields:

- * name**: outsidemobile
- admin**: enabled (Resource is active)
- * ip-address**:
 - * type**: static (static IP address)
 - * address/mask**: 62.140.151.115/28 (n.n.n.n/n)
- geolocation**: 0
- security-domain**: enter [] or select from <Not configured>
- address-scope**: enter [] or select from <Not configured>
- filter-intf**: disabled (Resource is inactive)

Further down on the same screen in the **routing** section click the edit link relating to the **route external-sip-media-1** route.

The screenshot shows the 'routing' section with a 'route' table. The table has columns: route, admin, destination, gateway, and metric. The 'route external-sip-media-1' row is highlighted with a red box.

route	admin	destination	gateway	metric
Edit Delete route Default	disabled	default	0.0.0.0	1
Edit Delete route external-sip-media-1	enabled	network 62.140.143.0/24	62.140.151.113	1

Below the table is a link: [Add route](#)

In the resulting screen in the **destination** section, select **host** from the drop down menu for **type**. In the **address** field enter the IP address of the Vodafone Netherlands OneVoice Corporate SIP trunk service.

Configure cluster|box:AASBC01Vlan6.avaya.com|interface eth2|ip outsidemobile|routing|route external-sip-media-1
[Help](#) [Index](#)

Set Reset Back Copy Delete

admin	enabled (Resource is active)
* route-name	external-sip-media-1
* destination	<div>* type host (host route)</div> <div>* address 62.140.143.75 (n.n.n.n)</div>
* gateway	62.140.151.113 (n.n.n.n)
metric	1 (from 0 to 1,000,default=1)

Set Reset Back Copy

7.4. Session Config Pool

Navigate to **vsp** → **session-config-pool** → **entry ToTelco** and extend the entry in the **name** field to **ToTelcoFixed**.

AVAYA aura acme packet powered Configuration

Status Summary Logout admin Home Configuration Status Call Logs Event Logs Actions Services Keys Access Tools

Configuration: all Configuration Setup View

- cluster
 - box:AASBC01Vlan6.avaya.com
 - interface eth0
 - interface eth2
 - ip outsidefixed
 - ip outsidemobile
 - cli
- vsp
 - default-session-config
 - tls
 - session-config-pool
 - entry ToTelco
 - entry ToPBX
 - entry Discard
 - dial-plan

Configure vsp|session-config-pool|entry ToTelco Show advanced Help Index

Set Reset Back Copy Delete

[Set QoS](#)

basic:

sip-directive	Configure
sip-settings	Configure
log-alert	Configure
registration	Configure
* name	ToTelcoFixed

7.4.1. Stripping SIP Headers

The AASBC can be used to strip SIP headers to prevent the header from being sent to the public SIP Service Provider. To strip a SIP header navigate to **vsp** → **session-config-pool** → **entry ToTelco** → **header-settings** and click on the **Edit blocked-header** link.

The screenshot shows the Avaya Aura Configuration interface. The left sidebar displays a tree view under 'Configuration: all' with the path: cluster > box:AASBC01Vlan6.avaya.com > interface eth2 > ip outsidemobile > cli > vsp > session-config-pool > entry ToTelcoFixed. The main content area is titled 'Configure vspsession-config-poolentry ToTelcoFixedheader-settings'. It contains a table with the following rows: 'allowed-header' (Edit allowed-header), 'blocked-header' (Edit blocked-header, highlighted with a red box), 'altered-header' (Add altered-header), 'reg-ex-header' (Add reg-ex-header), 'header-normalization' (Add header-normalization), 'altered-body' (Add altered-body), and 'reg-ex-collector' (Add reg-ex-collector). Buttons for 'Set', 'Reset', 'Back', and 'Delete' are visible at the top of the main area.

In the resulting page click the **Add** button to open a new entry field and enter the name of the header to be removed, repeat this action for all the headers to be removed. Click the **OK** button when finished.

The screenshot shows the Avaya Aura Configuration interface, specifically the 'Configure vspsession-config-poolentry ToTelcoFixedheader-settings blocked-header' page. The left sidebar shows the same navigation path as the previous screenshot. The main content area has a title bar 'Configure vspsession-config-poolentry ToTelcoFixedheader-settings blocked-header' and a 'Back' button. Below this is a list of headers to be blocked: 'P-Charging-Vector', 'P-Location', and 'Alert-Info', each followed by an 'X' icon. A red box highlights the 'Add' button and the 'Remove All' button. An 'OK' button is located at the bottom of the main area.

The following screen shows the headers being stripped during testing.

The screenshot shows the AVAYA aura Configuration page. The left sidebar shows the navigation tree with 'vsp' expanded, and 'session-config-pool' selected. The main content area is titled 'Configure vspsession-config-poolentry ToTelcoFixedHeader-settings'. It has buttons for 'Set', 'Reset', 'Back', and 'Delete'. Below these are three sections: 'allowed-header', 'blocked-header', and 'altered-header'. The 'blocked-header' section is highlighted with a red box and contains a list of headers: 'P-Charging-Vector', 'P-Location', and 'Alert-Info'. There are also links for 'Edit allowed-header', 'Edit blocked-header', and 'Add altered-header'.

Navigate to **vsp** → **session-config-pool** → **entry ToTelco** → **from-uri-specification** and enter the IP address used on the public side of the AASBC for the Vodafone Netherlands Office Voice SIP trunk into the first host field. This will ensure that the host part of the From header is always set as the entered IP address. Click **Set** to save changes.

The screenshot shows the AVAYA aura Configuration page. The left sidebar shows the navigation tree with 'vsp' expanded, and 'session-config-pool' selected. The main content area is titled 'Configure vspsession-config-poolentry ToTelcofrom-uri-specification'. It has buttons for 'Set', 'Reset', 'Back', and 'Delete'. Below these are several fields: 'user', 'host', 'port', 'display', and 'user-agent-aware-display-'. The 'host' field is highlighted with a red box and contains the IP address '62.140.143.114'. The 'user' field has a dropdown menu with 'from-uri' selected. The 'port' and 'display' fields have dropdown menus with 'from-uri' selected. The 'user-agent-aware-display-' field has a dropdown menu with 'disabled' selected.

Navigate to **vsp** → **session-config-pool** → **entry ToTelco** and click **Copy** (not shown). This will produce an exact copy of the session config including the stripped SIP headers. In the resulting screen alter the entry in the **name** field to **ToTelcomobile**.

Navigate to **vsp** → **session-config-pool** → **entry ToTelcomobile** → **from-uri-specification** and enter the IP address used on the public side of the AASBC for the Vodafone Netherlands OneVoice Corporate SIP trunk into the first **host** field. This will ensure that the host part of the From header is always set as the entered IP address. Click **Set** to save changes.

7.5. SIP Servers

Navigate to **vsp** → **enterprise** → **servers** → **sip-gateway Telco** and alter the entry in the **name** field to **Telcofixed**. Click **Set** to save changes.

The screenshot shows the Avaya Aura Configuration interface. The left sidebar shows a tree view with 'Configuration: all' expanded, and 'vsp' → 'enterprise' → 'servers' → 'sip-gateway Telco' selected. The main content area is titled 'Configure vsplenterprise\servers\sip-gateway Telco'. It has buttons for 'Set', 'Reset', 'Back', 'Copy', and 'Delete'. Below these are links for 'Manage connections', 'Log instant messages', 'Record media', 'Record files', 'Set up accounting', 'Change "from:" URI', and 'Change "to:" URI'. The 'general' section contains a form with the following fields: 'name' (set to 'Telcofixed'), 'admin' (set to 'enabled'), 'domain' (empty), and 'failover-detection' (set to 'ping').

Navigate to **vsp** → **enterprise** → **servers** → **sip-gateway Telcofixed** and click **Copy** (Not shown). In the resulting screen alter the entry in the **name** field to **Telcomobile**. In the **outbound-session-config-pool-entry** field select the **ToTelcomobile** session config created in **Section 7.4** from the drop down menu. Click **Set** to save changes.

The screenshot shows the Avaya Aura Configuration interface for 'sip-gateway Telcomobile'. The left sidebar shows the tree view with 'sip-gateway Telcomobile' selected. The main content area is titled 'Configure vsplenterprise\servers\sip-gateway Telcomobile'. It has buttons for 'Set', 'Reset', 'Back', 'Copy', and 'Delete'. Below these are links for 'Manage connections', 'Log instant messages', 'Record media', 'Record files', 'Set up accounting', 'Change "from:" URI', and 'Change "to:" URI'. The 'general' section contains a form with the following fields: 'name' (set to 'Telcomobile'), 'admin' (set to 'enabled'), 'domain' (empty), and 'failover-detection' (set to 'ping'). The 'servers' section shows a 'server-pool' entry with a 'Delete' button. The 'policy' section contains a form with the following fields: 'inbound-session-config-pool-entry' (empty) and 'outbound-session-config-pool-entry' (set to 'vsp\session-config-pool\entry ToTelcoMobile').

Navigate to **vsp** → **enterprise** → **servers** → **sip-gateway Telcomobile** → **server-pool** → **server Telco1** and enter the IP address provided by Vodafone Netherlands for the Vodafone Netherlands OneVoice Corporate SIP trunk connection in to the **host** field. Click **Set** to save changes.

The screenshot shows the Avaya Aura Configuration web interface. The top navigation bar includes links for Home, Configuration, Status, Call Logs, Event Logs, Actions, Services, Keys, Access, and Tools. The left sidebar shows a tree view of the configuration hierarchy: Configuration (all) > vsp > enterprise > servers > sip-gateway Telcomobile > server-pool > server Telco1. The main content area is titled 'Configure vsplenterpriselserverslsip-gateway Telcomobileserver-poolserver Telco1'. It features a 'General' section with fields for 'server-name' (Telco1), 'admin' (enabled), 'host' (62.140.143.75), 'transport' (UDP), and 'port' (5060). Below the 'General' section is a 'Policy' section with links for 'outbound-normalization' and 'inbound-normalization'. The 'host' field is highlighted with a red border.

Configuration: all

Configuration Setup View

cluster

- box:AASBC01Vlan6.avaya.com

vsp

- default-session-config
- tls
- session-config-pool
- dial-plan
- enterprise
 - servers
 - sip-gateway PBX
 - sip-gateway Telcofixed
 - vsp\session-config-pool\entry
 - server-pool
 - server Telco1
 - sip-gateway Telcomobile
 - vsp\session-config-pool\entry
 - server-pool
 - server Telco1
- dns
- settings

Configure vsplenterpriselserverslsip-gateway Telcomobileserver-poolserver Telco1 Show advanced Help

Index

Set Reset Back Copy Delete

General:

* server-name Telco1

admin enabled (Resource is active)

* host 62.140.143.75 (host name or n.n.n.n)

transport transport UDP (User Datagram Protocol)

port 5060 (at minimum 1, default=5060)

Policy:

outbound-normalization Add outbound-normalization

inbound-normalization Add inbound-normalization

7.6. Dial Plan Configuration

The dial plan is used to define how calls route between SIP entities. For the compliance test four routes are required.

- The route **FromTelcofixed** will be used to route fixed calls from Vodafone Netherlands to the Session Manager.
- The route **FromPBXfixed** will be used to route fixed calls from the Session Manager to Vodafone Netherlands.
- The route **FromTelcomobile** will be used to route mobile calls from Vodafone Netherlands to the Session Manager.
- The route **FromPBXmobile** will be used to route mobile calls from the Session Manager to Vodafone Netherlands.

Navigate to **vsp** → **dial-plan** → **source-route FromTelco** (not shown) and alter the entry in the **name** field to **FromTelcofixed**. Click **Set** to save changes.

The screenshot shows the Avaya Aura Configuration web interface. The left sidebar displays a tree view of the configuration hierarchy: **Configuration: all** > **cluster** > **box:AASBC01Vlan6.avaya.com** > **vsp** > **dial-plan** > **route Default** > **source-route FromTelcofixed**. The main content area is titled **Configure vsp\dial-plan\source-route FromTelcofixed**. It includes buttons for **Set**, **Reset**, **Back**, **Copy**, and **Delete**. Below these is a **general:** section with the following fields:
- *** name**: **FromTelcofixed** (highlighted with a red box)
- **description**: (empty text field)
- *** source-match**: (empty text field)
- *** type**: **server** (dropdown menu)
- *** source-server**: **vsp\enterprise\servers\sip-gateway Telcofixed** (dropdown menu)
- **peer**:
- **type**: **server** (dropdown menu)
- **server**: **vsp\enterprise\servers\sip-gateway PBX** (dropdown menu)
- **location-match-preferred**: **up-to-outbound-peer** (dropdown menu)
- **priority**: **100** (text field)
- **condition-list**: **Configure** (link)
- **condition-list-match-secondary**: **false** (dropdown menu)

Navigate to **vsp** → **dial-plan** → **source-route FromTelcofixed** and click **Copy** (not shown). In the resulting screen alter the entry in the **name** field to **FromTelcomobile**. In the **source-server** field select the **Telcomobile** SIP server created in **Section 7.5**. Click **Set** to save changes.

The screenshot shows the Avaya Aura Configuration interface. The left sidebar shows the navigation tree with 'vsp' expanded and 'dial-plan' selected. The main content area is titled 'Configure vsp\dial-plan\source-route FromTelcomobile'. The 'general' tab is active, showing the following fields:

- * name:** FromTelcomobile
- description:** (empty)
- * source-match:** (empty)
- * type:** server
- * source-server:** vsp\enterprise\servers\sip-gateway Telcomobile
- peer:**
 - type:** server
 - server:** vsp\enterprise\servers\sip-gateway PBX
- location-match-preferred:** up-to-outbound-peer
- priority:** 100

Navigate to **vsp** → **dial-plan** → **source-route FromTelcofixed** and alter the entry in the **name** field to **FromPBXfixed**. Click **Set** to save changes.

The screenshot shows the Avaya Aura Configuration interface. The left sidebar shows the navigation tree with 'vsp' expanded and 'dial-plan' selected. The main content area is titled 'Configure vsp\dial-plan\source-route FromPBXfixed'. The 'general' tab is active, showing the following fields:

- * name:** FromPBXfixed
- description:** (empty)
- * source-match:** (empty)
- * type:** server
- * source-server:** vsp\enterprise\servers\sip-gateway PBX
- peer:**
 - type:** server
 - server:** vsp\enterprise\servers\sip-gateway Telcofixed
- location-match-preferred:** up-to-outbound-peer
- priority:** 100

Navigate to **vsp** → **dial-plan** → **source-route FromPBXfixed** and click **Copy** (not shown). In the resulting screen update the fields as shown below:

- Alter the entry in the **name** field to **FromPBXmobile**.
- Under the **source-match** section, select **condition-list** from the drop down box in the **type** field.
- Under the peer section, in the **server** field select the **Telcomobile** SIP server created in **Section 7.5**

Click **Set** to save changes and then click the **configure** link under the **condition-list** section.

The screenshot shows the Avaya Aura Configuration interface. The left sidebar shows a tree view with 'vsp' expanded, and 'source-route FromPBXmobile' selected. The main content area is titled 'Configure vsp\dial-plan\source-route FromPBXmobile'. It has buttons for 'Set', 'Reset', 'Back', 'Copy', and 'Delete'. The configuration fields are as follows:

general:	
* name	FromPBXmobile
description	
* source-match	* type: condition-list
peer	type: server (Peer is a SIP server) server: vsp\enterprise\servers\sip-gateway Telcomobile
location-match-preferred	up-to-outbound-peer (Outbound peer determines whether preferred)
priority	100 (from 0 to 999,999, default=100)
condition-list	Configure
condition-list-match-secondary	false

In the resulting screen select the **operation OR** from the drop down menu and click the **Add-to-uri-condition** link under the **to-uri-condition** section.

The screenshot shows the Avaya Aura Configuration interface for the 'condition-list' configuration. The left sidebar shows 'vsp' expanded, and 'condition-list' selected. The main content area is titled 'Configure vsp\dial-plan\source-route FromPBXmobile\condition-list'. It has buttons for 'Set', 'Reset', 'Back', and 'Delete'. The configuration fields are as follows:

operation	OR
mode	evaluate (The Net-Net OS-E runs the conditions to determine whether to apply session configuration settings.)
sip-message-condition	Add sip-message-condition
from-uri-condition	Add from-uri-condition
to-uri-condition	Add to-uri-condition
request-uri-condition	Add request-uri-condition

In the resulting screen define the dial patterns that the condition list should match by updating the fields as shown below:

- For **attribute** select **user** from the drop down menu. This means that the condition will try to match the user part of the uri.
- For **match** select **contains** from the drop down menu. This means that the condition list will match anything that contains the entry in the value field.
- In the **value** field enter the digits to match using regular expression.

Click **Create** to save the condition.

Configuration: all

Configuration | Setup | View

cluster

- box:AASBC01Vlan6.avaya.com
- vsp
 - default-session-config
 - tls
 - session-config-pool
 - dial-plan
 - route Default
 - source-route FromTelcofixed
 - source-route FromPBXmobile

Create vspldial-plan|source-route FromPBXmobile|condition-list|to-uri-condition - Step 1 of 1: Edit to-uri-condition

Please provide some basic information for to-uri-condition. Then press "Create".

* attribute: user (particular resource located at host)

* match: contains (allow values which contain the specified expression)

* value: ^00316 (regular expression)

Create Reset Cancel

The AASBC can be used to create the regular expression for the **value** field. Click the **(regular expression)** link next to the **value** field as seen in the previous screen. The following pop up box is displayed. Enter the digits to be matched and select the appropriate radio button for the type of match. The example below will match any digits beginning with 210, this will produce a regular expression of **^210**.

(regular expression)

You can set the match option so that the system matches the entire string, the beginning or end of the string, or any part of the string.

Enter String Pattern: 210

Match option: ☐ Exact Match ☒ Match Beginning ☐ Match End ☐ Match Any

OK Cancel

The following screen shows the to-uri-conditions used during the compliance test.

Configuration: all

Configuration | Setup | View

- cluster
 - box: AASBC01Vlan6.avaya.com
- vsp
 - default-session-config
 - tls
 - session-config-pool
 - dial-plan
 - route Default
 - source-route FromTelcofixed
 - source-route FromPBXmobile
 - source-route FromTelcomobile
 - source-route FromPBXfixed
 - enterprise
 - dns
 - settings

Configure vspldial-plan|source-route FromPBX|mobile|condition-list [Help](#) [Index](#)

Set Reset Back Delete

Press "Set" to keep these values.

operation OR

mode evaluate (The Net-Net OS-E runs the conditions to determine whether to apply session configuration settings.)

sip-message-condition [Add sip-message-condition](#)

from-uri-condition [Add from-uri-condition](#)

to-uri-condition

		attribute
▼	Edit Delete	user contains *00316
▲▼	Edit Delete	user contains *210
▲▼	Edit Delete	user contains *06
▲	Edit Delete	user contains ^+316

[Add to-uri-condition](#)

7.7. Mobile-X Mid call features

To allow Mobile-X mid-call features to work using DTMF tones from the mobile device, the tones need to be passed to the CS1000E as SIP INFO messages. In order to do this RFC2833 tones are converted into INFO messages using the AASBC. Navigate to **vsp → session-config-pool → entryToPBX → in-dtmf-translation** and click **Configure** (not shown). In the resulting screen update the fields as shown below and then click on **Set** to save:

Configuration: all

Configuration | Setup | View

- cluster
 - box: AASBC01Vlan6.avaya.com
- vsp
 - default-session-config
 - tls
 - session-config-pool
 - entry ToTelcoFixed
 - entry ToPBX
 - to-uri-specification
 - request-uri-specification
 - in-dtmf-translation
 - out-dtmf-translation
 - header-settings
 - entry Discard
 - entry ToTelcoMobile
 - dial-plan
 - enterprise
 - dns
 - settings

Configure vsp|session-config-pool|entry ToPBX|in-dtmf-translation [Show basic](#)

Set Reset Back Delete

info rfc-2833 (RFC-2833 packets)

drop-info true

rfc-2833 info (SIP INFO message)

drop-rfc-2833 true

info-dtmf-body dtmf-relay (SIP INFO message with DTMF-relay body)

timeout-rfc-2833 1000 ms

Set Reset Back

[Help](#) [Index](#)

Navigate to **vsp** → **session-config-pool** → **entryToPBX** → **out-dtmf-translation** and click **Configure** (not shown). In the resulting screen update the fields as shown below and then click on **Set** to save:

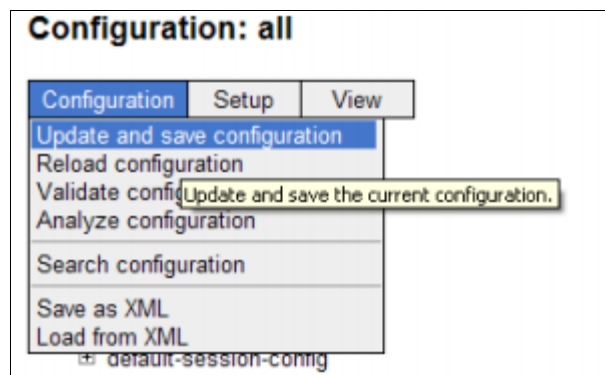
The screenshot shows the Avaya Aura Configuration interface. The left pane displays a tree structure under 'Configuration: all' with 'out-dtmf-translation' selected. The main pane shows the configuration for 'Configure vsp\session-config-pool\entry ToPBX\out-dtmf-translation'. The configuration fields are as follows:

Field	Value	Description
info	rfc-2833	(RFC-2833 packets)
drop-info	true	
rfc-2833	info	(SIP INFO message)
drop-rfc-2833	true	
info-dtmf-body	dtmf-relay	(SIP INFO message with DTMF-relay body)
timeout-rfc-2833	1000	ms

Buttons at the top of the main pane include Set, Reset, Back, and Delete. Buttons at the bottom include Set, Reset, and Back. A 'Show basic' button is also present in the top right of the main pane.

7.8. Save the Configuration

To save the configuration, click on **Configuration** in the left pane to display the configuration menu. Next, select **Update and save configuration**.



8. Verification Steps

8.1. Verify Avaya Communication Server 1000E 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 Group** table as shown below.

AVAYA CS1000 Element Manager Help | Log

Managing: 10.80.51.60 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**

D-Channel Diagnostics

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

DCH|DES|APPL_STATUS|LINK_STATUS|AUTO_RECV|PDCH|BDCH

☐ 010 Vtrk OPER EST ACTV AUTO




STAT DCH 010

Command executed successfully.

8.2. Verify Avaya Aura® Session Manager Operational Status

8.2.1. 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.

- **Tests Pass** 
- **Security Module** 
- **Service State** 

Home / Elements / Session Manager- Session Manager

Session Manager

Dashboard

Session Manager

Administration

Communication Profile Editor

Network Configuration

Device and Location Configuration

Application Configuration

System Status

System Tools

Home / Elements / Session Manager- Session Manager


Session Manager Dashboard

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

Session Manager Instances

Service State Shutdown System As of 3:07 PM

1 Item Refresh Show ALL Filter: Enable

<input type="checkbox"/>	Session Manager	Type	Alarms	Tests Pass	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Version
<input type="checkbox"/>	Session Manager	Core	0/1/63		Up	Accept New Service	0/2	0	0	6.1.4.0.614

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.

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 Certificate Management Connection Status

1 Item Refresh Show ALL Filter: Enable

	Details	Session Manager	Type	Status	Connections	IP Address	VLAN	Default Gateway	NIC Bonding	Entity Links (expected / actual)	Certificate Used
	Show	sesmgr02	SM	Up	13	10.10.6.30/24	---	10.10.6.1	Disabled	6/6	SIP CA

Select : None

8.2.2. 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 Network Routing Server from the **All Monitored SIP Entities** table (not shown) to open the **SIP Entity, Entity Link Connection Status** page. In the **All Entity Links to SIP Entity: cppm7-5** table, verify the **Conn. Status** for the link is **Up** as shown below.

SIP Entity, Entity Link Connection Status							
This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.							
All Entity Links to SIP Entity: cppm7-5							
Summary View							
1 Item Refresh Filter: Enable							
Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
► Show	sesmgr02	10.10.6.71	5060	TCP	Up	200 OK	Up

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

SIP Entity, Entity Link Connection Status							
This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.							
All Entity Links to SIP Entity: AASBC01							
Summary View							
1 Item Refresh Filter: Enable							
Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
► Show	sesmgr02	10.10.6.38	5060	TCP	Up	200 OK	Up

8.3. Verify Avaya Aura ® Session Border Controller

From the AASBC **Actions** tab it is possible to send a SIP OPTIONS message to a specified IP address to confirm the correct response. Select **sip** from the left hand menu and select **ping** from the drop down menu in the **type** field. Enter the required IP address in the **server** field and specify the appropriate **transport** type and **port**. Click **Invoke** and the result of the test are shown towards the top of the page.

The screenshot shows the Avaya Aura AASBC web interface. The top navigation bar includes 'Home', 'Configuration', 'Status', 'Call Logs', 'Event Logs', 'Actions' (selected), 'Services', 'Keys', 'Access', and 'Tools'. The left sidebar lists various actions, with 'sip' selected. The main content area is titled 'sip' and 'Actions for SIP transport connections'. A 'Success' message is displayed, indicating a successful SIP OPTIONS test. Below the message is a form for configuring the test, with fields for 'type' (set to 'ping'), 'server' (62.140.143.75), 'transport' (UDP), and 'port' (5060). An 'Invoke' button is at the bottom right of the form.

Success

Sending OPTIONS to 62.140.143.75:5060 UDP
Success! Received OPTIONS Response 200:
From: sip:62.140.151.115
To: sip:62.140.143.75
Contact: <sip:62.140.143.75>

* action

* type (Query a SIP endpoint with SIP option)

* server

transport (User Datagram Protocol)

port (at minimum 1,default=5060)

1. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active.
2. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active.
3. Verify that the user on the PSTN can end an active call by hanging up.
4. Verify that an endpoint at the enterprise site can end an active call by hanging up.

9. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Communication Server 1000E, Avaya Aura® Session Manager and Avaya Aura® Session Border Controller to Vodafone Netherlands SIP Trunk Solution comprising of Vodafone Office Voice and Vodafone OneVoice Corporate. Vodafone Netherlands SIP Trunk Solution is a SIP-based Voice over IP solution providing businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. Vodafone Vodafone Netherlands SIP Trunk Solution comprising of Vodafone Office Voice and Vodafone OneVoice Corporate passed compliance testing. Please refer to **Section 2.2** for any observations or workarounds relating the testing covered by these Application Notes.

10. References

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

- [1] *Installing and Configuring Avaya Aura® System Platform*, Release 6, June 2010.
- [2] *Administering Avaya Aura® System Platform*, Release 6, June 2010.
- [3] *Installing and Upgrading Avaya Aura® System Manager Release 6.1*, November 2010.
- [4] *Installing and Configuring Avaya Aura® Session Manager*, January 2011, Document Number 03-603473
- [5] *Administering Avaya Aura® Session Manager*, March 2011, Document Number 03-603324.
- [6] *Avaya Aura® Session Border Controller System Administration*, September 2010
- [7] *Installing and Configuring Avaya Aura Session Border Controller*, May 2011
- [8] *IP Peer Networking Installation and Commissioning*, Release 7.5, Document Number NN43001-313, available at <http://support.avaya.com>
- [9] *Unified Communications Management Common Services Fundamentals*, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-116, available at <http://support.avaya.com>
- [10] *Co-resident Call Server and Signaling Server Fundamentals*, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-509, available at <http://support.avaya.com>
- [11] *Signaling Server and IP Line Fundamentals*, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-125, available at <http://support.avaya.com>
- [12] *RFC 3261 SIP: Session Initiation Protocol*, <http://www.ietf.org/>

Additional Vodafone product documentation is available at http://www.vodafone.nl/zakelijk/totaal_oplossingen/vast_en_mobiel/

Appendix A – Avaya Communication Server 1000E Software

Communication Server 1000E call server patches and plug ins

TID: 46379

VERSION 4121

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

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

RELEASE 7

ISSUE 50 Q +

IDLE_SET_DISPLAY NORTEL

DepList 1: core Issue: 01 (created: 2011-09-13 15:12:45 (est))

MDP>LAST SUCCESSFUL MDP REFRESH :2011-10-11 13:28:54 (Local Time)

MDP>USING DEPLIST ZIP FILE DOWNLOADED :2011-09-21 10:45:48 (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	wi00839337	ISS1:10F1	DSP2AB06	16/04/2012	DSP2AB06.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 end

Communication Server 1000E call server deplists

VERSION 4121

RELEASE 7

ISSUE 50 Q +

DepList 1: core Issue: 01 (created: 2011-09-13 15:12:45 (est))

IN-SERVICE PEPS

PAT#	CR #	PATCH REF #	NAME	DATE	FILENAME	SPECINS
000	wi00869243	ISS1:10F1	p30848_1	07/11/2011	p30848_1.cpl	NO
001	WI00843571	ISS1:10F1	p30627_1	07/11/2011	p30627_1.cpl	NO
002	wi00856702	ISS1:10F1	p30573_1	07/11/2011	p30573_1.cpl	NO
003	WI00836292	ISS1:10F1	p30554_1	07/11/2011	p30554_1.cpl	NO
004	wi00897176	ISS1:10F1	p30418_1	07/11/2011	p30418_1.cpl	NO
005	wi00853178	ISS1:10F1	p30719_1	07/11/2011	p30719_1.cpl	NO
006	wi00866570	ISS1:10F1	p30477_1	07/11/2011	p30477_1.cpl	NO
007	wi00905600	ISS1:10F1	p31201_1	07/11/2011	p31201_1.cpl	NO
008	wi00900766	ISS1:10F1	p31159_1	07/11/2011	p31159_1.cpl	NO
009	wi00834382	ISS1:10F1	p30548_1	07/11/2011	p30548_1.cpl	NO
010	wi00865477	ISS1:10F1	p30897_1	07/11/2011	p30897_1.cpl	YES
011	wi00835294	ISS1:10F1	p30565_1	07/11/2011	p30565_1.cpl	NO
012	wi00875701	ISS1:10F1	p30942_1	07/11/2011	p30942_1.cpl	NO
013	wi00903085	ISS1:10F1	p31164_1	07/11/2011	p31164_1.cpl	NO
014	wi00839134	ISS1:10F1	p30698_1	07/11/2011	p30698_1.cpl	YES
015	wi00865477	ISS1:10F1	p30890_1	07/11/2011	p30890_1.cpl	YES
016	wi00877367	ISS1:10F1	p30534_1	07/11/2011	p30534_1.cpl	NO
017	wi00852365	ISS1:10F1	p30707_1	07/11/2011	p30707_1.cpl	NO
018	WI00854150	ISS1:10F1	p30468_1	07/11/2011	p30468_1.cpl	NO

019	WI00853473	ISS1:10F1	p30625_1	07/11/2011	p30625_1.cpl	NO
020	wi00865477	ISS1:10F1	p30895_1	07/11/2011	p30895_1.cpl	YES
021	wi00841273	ISS1:10F1	p30713_1	07/11/2011	p30713_1.cpl	NO
022	wi00905097	ISS1:10F1	p31194_1	07/11/2011	p31194_1.cpl	NO
023	wi00865477	ISS1:10F1	p30893_1	07/11/2011	p30893_1.cpl	YES
024	wi00838073	ISS1:10F1	p30588_1	07/11/2011	p30588_1.cpl	NO
025	wi00879508	ISS1:10F1	p30956_1	07/11/2011	p30956_1.cpl	NO
026	wi00871969	ISS1:10F1	p30768_1	07/11/2011	p30768_1.cpl	NO
027	wi00853658	ISS1:10F1	p30990_1	07/11/2011	p30990_1.cpl	NO
028	wi00856410	ISS1:10F1	p30749_1	07/11/2011	p30749_1.cpl	NO
029	wi00906163	ISS1:10F1	p31205_1	07/11/2011	p31205_1.cpl	NO
030	wi00907697	ISS1:10F1	p31227_1	07/11/2011	p31227_1.cpl	NO
031	wi00896420	ISS1:10F1	p30867_1	07/11/2011	p30867_1.cpl	NO
032	wi00839821	ISS1:10F1	p30619_1	07/11/2011	p30619_1.cpl	NO
033	wi00860279	ISS1:10F1	p30789_1	07/11/2011	p30789_1.cpl	NO
034	wi00865477	ISS1:10F1	p30891_1	07/11/2011	p30891_1.cpl	YES
035	WI00889786	ISS1:10F1	p30750_1	07/11/2011	p30750_1.cpl	NO
036	wi00863876	ISS1:10F1	p30787_1	07/11/2011	p30787_1.cpl	NO
037	wi00921340	ISS1:10F1	p31266_1	07/11/2011	p31266_1.cpl	NO
038	wi00900668	ISS1:10F1	p30456_1	07/11/2011	p30456_1.cpl	NO
039	wi00908598	ISS1:10F1	p31235_1	07/11/2011	p31235_1.cpl	NO
040	wi00896680	ISS1:10F1	p30357_1	07/11/2011	p30357_1.cpl	NO
041	wi00869695	ISS1:10F1	p30654_1	07/11/2011	p30654_1.cpl	NO
042	wi00854130	ISS1:10F1	p30443_1	07/11/2011	p30443_1.cpl	NO
043	wi00883604	ISS1:10F1	p30973_1	07/11/2011	p30973_1.cpl	NO
044	wi00905297	ISS1:10F1	p31195_1	07/11/2011	p31195_1.cpl	NO
045	wi00854415	ISS1:10F1	p30593_1	07/11/2011	p30593_1.cpl	NO
046	wi00827950	ISS2:10F1	p30471_2	07/11/2011	p30471_2.cpl	NO
047	wi00859123	ISS1:10F1	p30648_1	07/11/2011	p30648_1.cpl	NO
048	wi00897082	ISS1:10F1	p31124_1	07/11/2011	p31124_1.cpl	NO
049	wi00906022	ISS1:10F1	p31202_1	07/11/2011	p31202_1.cpl	NO
050	wi00859499	ISS1:10F1	p30694_1	07/11/2011	p30694_1.cpl	NO
051	wi00871739	ISS1:10F1	p30856_1	07/11/2011	p30856_1.cpl	NO
052	wi00894443	ISS1:10F1	p31093_1	07/11/2011	p31093_1.cpl	NO
053	wi00850521	ISS1:10F1	p30709_1	07/11/2011	p30709_1.cpl	YES
054	wi00839255	ISS1:10F1	p30591_1	07/11/2011	p30591_1.cpl	NO
055	wi00908933	ISS1:10F1	p31239_1	07/11/2011	p31239_1.cpl	NO
056	wi00865477	ISS1:10F1	p30892_1	07/11/2011	p30892_1.cpl	YES
057	wi00905660	ISS1:10F1	p27968_1	07/11/2011	p27968_1.cpl	NO
058	wi00841980	ISS1:10F1	p30618_1	07/11/2011	p30618_1.cpl	NO
059	wi00879526	ISS1:10F1	p31007_1	07/11/2011	p31007_1.cpl	NO
060	wi00895090	ISS1:10F1	p31105_1	07/11/2011	p31105_1.cpl	NO
061	wi00865477	ISS1:10F1	p30894_1	07/11/2011	p30894_1.cpl	YES
062	wi00898168	ISS1:10F1	p31131_1	07/11/2011	p31131_1.cpl	NO
063	wi00895181	ISS1:10F1	p31106_1	07/11/2011	p31106_1.cpl	NO
064	wi00832106	ISS1:10F1	p30550_1	07/11/2011	p30550_1.cpl	NO
065	wi00881777	ISS1:10F1	p25747_1	07/11/2011	p25747_1.cpl	NO
066	wi00836182	ISS1:10F1	p30450_1	07/11/2011	p30450_1.cpl	NO
067	wi00686981	ISS1:10F1	p30706_1	07/11/2011	p30706_1.cpl	NO
068	wi00852389	ISS1:10F1	p30641_1	07/11/2011	p30641_1.cpl	NO
069	wi00858335	ISS1:10F1	p30819_1	07/11/2011	p30819_1.cpl	NO
070	WI00836334	ISS1:10F1	p30481_1	07/11/2011	p30481_1.cpl	NO
071	wi00887744	ISS2:10F1	p31026_2	07/11/2011	p31026_2.cpl	NO
072	wi00865477	ISS1:10F1	p30896_1	07/11/2011	p30896_1.cpl	YES
073	wi00865477	ISS1:10F1	p30898_1	07/11/2011	p30898_1.cpl	YES
074	wi00903437	ISS1:10F1	p31167_1	07/11/2011	p31167_1.cpl	NO
075	wi00888680	ISS1:10F1	p30399_1	07/11/2011	p30399_1.cpl	NO
076	wi00842409	ISS1:10F1	p30621_1	07/11/2011	p30621_1.cpl	NO
077	wi00857362	ISS1:10F1	p30782_1	07/11/2011	p30782_1.cpl	NO
078	wi00882293	ISS1:10F1	p31010_1	07/11/2011	p31010_1.cpl	NO
079	wi00894243	ISS1:10F1	p31087_1	07/11/2011	p31087_1.cpl	NO
080	WI00900213	ISS1:10F1	p30656_1	07/11/2011	p30656_1.cpl	NO
081	wi00897096	ISS1:10F1	p30676_1	07/11/2011	p30676_1.cpl	NO
082	wi00899584	ISS1:10F1	p30809_1	07/11/2011	p30809_1.cpl	NO
083	WI00839794	ISS1:10F1	p28647_1	07/11/2011	p28647_1.cpl	NO
084	wi00857566	ISS1:10F1	p30766_1	07/11/2011	p30766_1.cpl	NO
085	wi00903381	ISS1:10F1	p30421_1	07/11/2011	p30421_1.cpl	NO
086	wi00873382	ISS1:10F1	p30832_1	07/11/2011	p30832_1.cpl	NO
087	wi00876855	ISS1:10F1	p30952_1	07/11/2011	p30952_1.cpl	NO
088	wi00886321	ISS1:10F1	p31009_1	07/11/2011	p31009_1.cpl	NO
089	wi00826075	ISS1:10F1	p30452_1	07/11/2011	p30452_1.cpl	NO

090	wi00875425	ISS1:10F1	p30943_1	07/11/2011	p30943_1.cpl	NO
091	wi00833910	ISS2:10F1	p30492_2	07/11/2011	p30492_2.cpl	NO
092	wi00921295	ISS1:10F1	p31265_1	07/11/2011	p31265_1.cpl	NO
093	wi00824257	ISS1:10F1	p30447_1	07/11/2011	p30447_1.cpl	NO
094	wi00898652	ISS1:10F1	p31158_1	07/11/2011	p31158_1.cpl	NO
095	wi00836981	ISS1:10F1	p30613_1	07/11/2011	p30613_1.cpl	NO
096	wi00877442	ISS1:10F1	p30844_1	07/11/2011	p30844_1.cpl	NO
097	wi00884699	ISS1:10F1	p31000_1	07/11/2011	p31000_1.cpl	YES
098	wi00840590	ISS1:10F1	p30767_1	07/11/2011	p30767_1.cpl	NO
099	wi00854409	ISS1:10F1	p30479_1	07/11/2011	p30479_1.cpl	NO
100	wi00832626	ISS2:10F1	p30560_2	07/11/2011	p30560_2.cpl	NO
101	wi00837461	ISS1:10F1	p30597_1	07/11/2011	p30597_1.cpl	NO
102	wi00905550	ISS1:10F1	p31220_1	07/11/2011	p31220_1.cpl	NO
103	wi00868729	ISS1:10F1	p31163_1	07/11/2011	p31163_1.cpl	NO
104	wi00843623	ISS1:10F1	p30731_1	07/11/2011	p30731_1.cpl	YES
105	wi00888396	ISS1:10F1	p31027_1	07/11/2011	p31027_1.cpl	NO
106	wi00853031	ISS1:10F1	p30531_1	07/11/2011	p30531_1.cpl	NO

MDP>LAST SUCCESSFUL MDP REFRESH :2011-10-11 13:28:54 (Local Time)

MDP>USING DEPLIST ZIP FILE DOWNLOADED :2011-09-21 10:45:48 (est)

Communication Server 1000E signaling server service updates

Product Release: 7.50.17.00

In system patches: 2

PATCH#	NAME	IN SERVICE	DATE	SPECINS	TYPE	RPM
14	p30260_1	Yes	13/12/11	NO	FRU	cs1000-pi-control-1.00.00.00-00.noarch
15	p30253_1	Yes	02/03/12	NO	FRU	cs1000-pi-control-1.00.00.00-00.noarch

In System service updates: 15

PATCH#	IN_SERVICE	DATE	SPECINS	REMOVABLE	NAME
0	Yes	22/09/11	NO	YES	cs1000-linuxbase-7.50.17.16-3.i386.000
1	Yes	22/09/11	NO	YES	cs1000-baseWeb-7.50.17.16-1.i386.001
2	Yes	22/09/11	NO	YES	cs1000-patchWeb-7.50.17.16-2.i386.000
3	Yes	22/09/11	NO	YES	cs1000-kcv-7.50.17.16-1.i386.000
4	Yes	26/09/11	NO	YES	cs1000-dbcom-7.50.17-02.i386.000
5	Yes	26/09/11	NO	yes	cs1000-sps-7.50.17.16-01.i386.000
6	Yes	26/09/11	NO	YES	cs1000-shared-pbx-7.50.17.16-1.i386.000
7	Yes	26/09/11	NO	YES	cs1000-dmWeb-7.50.17.16-1.i386.000
8	Yes	26/09/11	NO	YES	cs1000-tps-7.50.17.16-5.i386.000
9	Yes	26/09/11	NO	YES	cs1000-ipsec-7.50.17.16-1.i386.000
10	Yes	26/09/11	NO	YES	cs1000-bcc-7.50.17.16-19.i386.000
11	Yes	26/09/11	NO	YES	cs1000-Jboss-Quantum-7.50.17.16-5.i386.000
12	Yes	26/09/11	NO	YES	cs1000-ftrpkg-7.50.17.16-5.i386.000
13	Yes	26/09/11	NO	YES	cs1000-emWeb_6-0-7.50.17.16-7.i386.000
16	Yes	02/03/12	NO	YES	cs1000-vtrk-7.50.17.16-46.i386.000

Communication Server 1000E system software

Product Release: 7.50.17.00

Base Applications

base	7.50.17	[patched]
NTAFS	7.50.17	
sm	7.50.17	
cs1000-Auth	7.50.17	
Jboss-Quantum	7.50.17	[patched]
lhmonitor	7.50.17	
baseAppUtils	7.50.17	[patched]
dfoTools	7.50.17	
nnnm	7.50.17	
cppmUtil	7.50.17	
oam-logging	7.50.17	
dmWeb	n/a	[patched]
baseWeb	n/a	[patched]
ipsec	n/a	[patched]
Snmp-Daemon-TrapLib	7.50.17	
ISECSH	7.50.17	
patchWeb	n/a	[patched]
EmCentralLogic	7.50.17	

Application configuration: CS+SS+EM

Packages:

CS+SS+EM		
Configuration version:	7.50.17-00	
cs	7.50.17	
dbcom	7.50.17	[patched]
cslogin	7.50.17	
sigServerShare	7.50.17	[patched]
csv	7.50.17	
tps	7.50.17.16	[patched]
vtrk	7.50.17.16	[patched]
pd	7.50.17	
sps	7.50.17.16	[patched]
ncs	7.50.17	
gk	7.50.17	
EmConfig	7.50.17	
emWeb_6-0	7.50.17	[patched]
emWebLocal_6-0	7.50.17	
csmWeb	7.50.17	
bcc	7.50.17	[patched]
ftrpkg	7.50.17	[patched]
cs1000WebService_6-0	7.50.17	
managedElementWebService	7.50.17	
mscAnnc	7.50.17	
mscAttn	7.50.17	
mscConf	7.50.17	
mscMusc	7.50.17	
mscTone	7.50.17	

©2012 Avaya Inc. All Rights Reserved.

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

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