



**Application Notes for Configuring Avaya Communication Server 1000E R7.5, Avaya Aura<sup>®</sup> Session Manager R6.1 and Avaya Aura<sup>®</sup> Session Border Controller to support BT Wholesale/HIPCOM SIP Trunk Service – Issue 1.0**

**Abstract**

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between BT Wholesale (BTW)/HIPCOM SIP Trunk Service and an Avaya SIP enabled Enterprise Solution. The Avaya solution consists of Avaya Aura<sup>®</sup> Session Manager, Avaya Communication Server 1000E and Avaya Aura<sup>®</sup> Session Border Controller.

BT is 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 lab.

# 1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between BT Wholesale/HIPCOM SIP Trunk Service and an Avaya SIP enabled enterprise solution. The Avaya solution consists of Avaya Aura<sup>®</sup> Session Manager, Avaya Communication Server 1000E (CS1K) connected to BT Wholesale/HIPCOM SIP Trunk Service via an Avaya Aura<sup>®</sup> Session Border Controller (SBC). Customers using this Avaya SIP-enabled enterprise solution with BT Wholesale/HIPCOM's SIP Trunk Service are able to place and receive PSTN calls via a dedicated Internet connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks. This approach normally results in lower cost for the enterprise.

## 2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using an Avaya SIP telephony solution consisting of CS1K, Session Manager and SBC. The enterprise site was configured to use the SIP Trunk Service provided by BTW/HIPCOM.

### 2.1. Interoperability Compliance Testing

The interoperability test included the following:

- Incoming calls to the enterprise site from the PSTN were routed to the DID numbers assigned by BTW/HIPCOM. Incoming PSTN calls were made to Unistim, SIP, Digital and analog telephones at the enterprise
- Outgoing calls from the enterprise to the PSTN were made from Unistim, SIP, Digital and analog telephones
- G.729 annex b (silence suppression) is not supported by BTW/HIPCOM's SIP Trunk Service and thus was not tested
- Calls using G.729 and G.711A codec's were tested
- Fax calls to/from a Group 3 fax machine to a PSTN connected fax machine using the T.38 mode
- 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

### 2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for BTW/HIPCOM SIP Trunk Service with the following observations.

- Incoming call to busy trunks or SIP Trunk signaling failure the following was observed - PSTN receives NU Tone eventually and 500 Service Unavailable sip message. The global parameter set on BTW/HIPCOM's SBC is 4 hunts per call, so if the call doesn't set up on the first try BTW/HIPCOM's SBC will re-try a further 3 times.

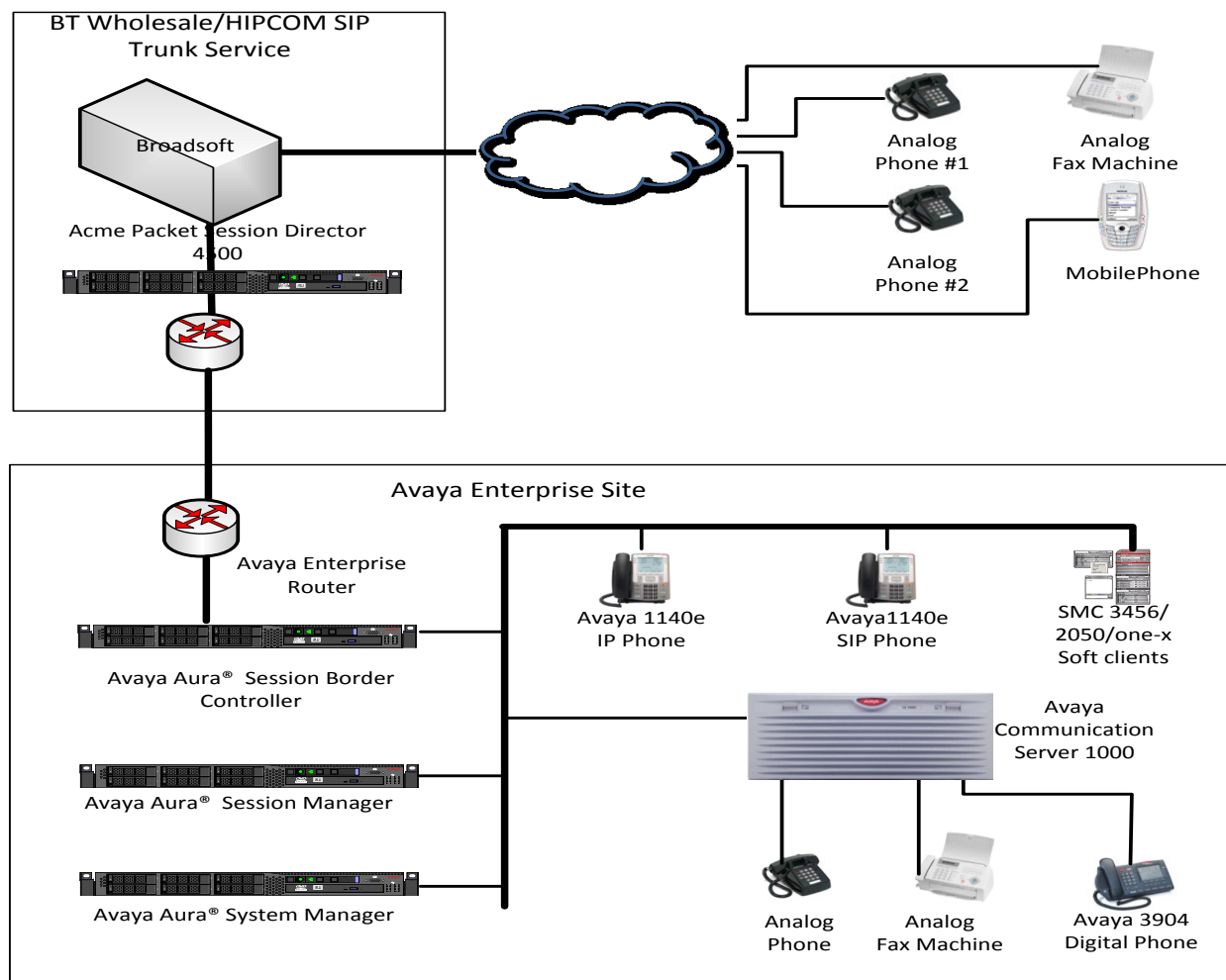
## 2.3. Support

For technical support on BTW/HIPCOM products please contact the following website:

<http://www.hipcom.co.uk/support> or <http://ipvoicesupport.btwholesale.com>.

## 3. Reference Configuration

**Figure 1** illustrates the test configuration. The test configuration shows an enterprise site connected to BTW/HIPCOM using SIP Trunks. Located at the enterprise site are Session Manager, SBC and a Communication Server 1000E. Endpoints are Avaya 1140 series IP telephones, Avaya 1200 series (not shown in **Figure 1**) IP telephones (with Unistim and SIP firmware), Avaya IP Softphones (SMC3456, 2050 and one-X Communicator), Avaya Digital telephone, Analog telephone and fax machine. For security purposes, any public IP addresses or PSTN routable phone numbers used in the compliance test are not shown in these Application Notes.



**Figure 1: BT Wholesale/HIPCOM SIP Trunk topology with Avaya Communication Server 1000E**

## 4. Equipment and Software Validated

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

Equipment	Software
Avaya S8800 server	Avaya Aura® Session Manager R6.1 Build: 6.1.0.0.610023 Service Pack 3
Avaya S8800 server	Avaya Aura® System Manager R6.1 (6.1.0.0.7345 – 6.1.5.112) Service Pack 3
Avaya Communication Server 1000E running on CP+PM server as co-resident configuration	Avaya Communication Server 1000E R7.5, Version 7.50.17 Service Update: 7.50_17Nov23 Deplst: X21 07.50Q
Avaya Media S8800 server	Avaya Aura® Session Border Controller version 6.0.2.0.2 (E362P4)
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: DSP1 AB04
Avaya 1140e and 1230 Unistim Telephones	FW: 0625C8A
Avaya 1140e and 1230 SIP Telephones	FW: 04.01.13.00.bin
Avaya SMC 3456	Version 2.6 build 57666
Avaya one-X® Communicator	Avaya one-X® Communicator - cs6.1.0.10
Avaya 2050 IP Softphone	Release 4.0.2.0062
Avaya Analogue Telephone	N/A
Avaya M3904 Digital Telephone	N/A
BTW/HIPCOM SIP Trunk Service	Acme Packet 4500 Net-Net SBC ver SCX6.1.0 Broadsoft - ver 14 Sevice Pack 9 Configuration version - HIPCOM v8.1

## 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 (analog, SIP and IP phones). SIP trunks are established between Communication Server 1000E and Session Manager. These SIP trunks carry SIP Signaling associated with BTW/HIPCOM's SIP Trunk Service. For incoming calls, the Session Manager receives SIP messages from the SBC, through which the BTW/HIPCOM SIP Service 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 BTW/HIPCOM's network. Specific Communication Server 1000E configuration was 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.

### 5.1. Logging into the Avaya Communication Server 1000E

Login using SSH to the ELAN ip address of the Call Server using a user with correct privileges. Once logged in type **csconsole**, this will take the user into the vxworks shell of the call server. Next type **logi**, 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 BTW/HIPCOM'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
<b>SIP ACCESS PORTS</b>	<b>32767</b>	<b>LEFT 32752</b>	<b>USED</b>	<b>15</b>

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

BTW/HIPCOM SIP Trunk service supports G.711A voice codec and T.38 FAX transmissions. Using the Communication Server 1000E element manager sidebar, navigate to the **IP Network** → **IP Telephony Nodes** → **Node Details** → **VGW and Codecs** property page and configure the Communication Server 1000E General codec settings as in the next screenshot. The values highlighted are required for correct operation.

#### Node ID: 5000 - Voice Gateway (VGW) and Codecs

General | Voice Codescs | 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

Next, scroll down and configure the **G.711** and **G.729** codec settings. The relevant settings are highlighted in the following screenshot.

#### Node ID: 5000 - Voice Gateway (VGW) and Codecs

The screenshot shows the 'Voice Codecs' configuration page for Node ID 5000. The page has three tabs: 'General', 'Voice Codecs', and 'Fax'. The 'Voice Codecs' tab is selected. The settings are as follows:

- Codec G711:** ☒ Enabled (required)
  - Voice payload size: 20 (milliseconds per frame)
  - Voice playout (jitter buffer) delay: 40 (Nominal) / 80 (Maximum) (milliseconds)
  - Maximum delay may be automatically adjusted based on nominal settings.
- Codec G722:** ☐ Enabled
  - Voice payload size: 20 (milliseconds per frame)
  - Voice playout (jitter buffer) delay: 40 (Nominal) / 80 (Maximum) (milliseconds)
  - Maximum delay may be automatically adjusted based on nominal settings.
- Codec G729:** ☒ Enabled
  - Voice payload size: 30 (milliseconds per frame)
  - Voice playout (jitter buffer) delay: 60 (Nominal) / 120 (Maximum) (milliseconds)

At the bottom, there is a note: "Note: Changes made on this page will NOT be transmitted until the Node is also saved." and buttons for 'Save' and 'Cancel'.

Finally, configure the **Fax** settings as in the highlighted section of the next screenshot.

#### Node ID: 5000 - Voice Gateway (VGW) and Codecs

The screenshot shows the 'Fax' configuration page for Node ID 5000. The page has three tabs: 'General', 'Voice Codecs', and 'Fax'. The 'Fax' tab is selected. The settings are as follows:

- Codec G723.1:** ☐ Enabled
  - Voice payload size: 30 (milliseconds per frame)
  - Voice playout (jitter buffer) delay: 60 (Nominal) / 120 (Maximum) (milliseconds)
  - Maximum delay may be automatically adjusted based on nominal settings.
  - Coding rate: 5.3 (kbps)
- Fax settings:**
  - 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: 20 (bps)

At the bottom, there is a note: "Note: Changes made on this page will NOT be transmitted until the Node is also saved." and buttons for 'Save' and 'Cancel'.



## 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. This is also where the SIP trunk connection is made to the Session Manager. When an entity link is added in Session Manager for the CS1K it is the Node ip that is used (see **Section 6.4 – Define SIP Entities** for more details).

**CS1000 Element Manager**

---

Managing: 192.168.0.2 Username: admin  
System » IP Network » IP Telephony Nodes » Node Details

**Node Details (ID: 5000 - 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**

[Print](#) | [Refresh](#)

<input type="checkbox"/> Hostname	Type	Deployed Applications	ELAN IP	TLAN IPv4	Role
<input type="checkbox"/> spcs1k	Signaling_Server	SIP Line, LTPS, Gateway, PD, Presence Publisher, IP Media Services	192.168.0.2	10.10.8.2	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**.
- **SIP domain name:** The SIP Domain Name is the SIP Service Domain. The SIP Domain Name configured in the Signaling Server properties must match the Service Domain name configured in the Session Manager
- **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 5000

- **Proxy or Redirect Server:** Primary TLAN ip address is the SM100 ip address of the Session Manager. The **Transport protocol** used for **SIP**, in this case is TCP
- **SIP URI Map:** **Public National** and **Private Unknown** are left blank. All other fields in the SIP URI Map are left with default values.

#### Node ID: 5000 - 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: spcs1k \*

Gateway password: \*

Application node ID: 5000 \* (0-9999)

Enable failsafe NRS: ☐

SIP ANAT: ☒ IPv4 ☐ IPv6

**Virtual Trunk Network Health Monitor**

☐ Monitor IP addresses (listed below)

Information will be captured for the IP addresses listed below.

Monitor IP:  Add

Monitor addresses:

Remove

---

**Proxy Or Redirect Server:**

Proxy Server Route 1:

Primary TLAN IP address: 10.10.8.56

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

Port: 5060 (1 - 65535)

Transport protocol: TCP ▼

Options: ☐ Support registration ☐ Primary CDS proxy

---

**SIP URI Map:**

Public E.164 domain names	Private domain names
National: <input type="text"/>	UDP: <input type="text"/>
Subscriber: subscriber	CDP: cdp.udp
Special number: PublicSpecial	Special number: PrivateSpecial
Unknown: PublicUnknown	Vacant number: PrivateUnknown
	Unknown: <input type="text"/>

## 5.5. Configure Bandwidth Zones

**Bandwidth Zones** are used for alternate call routing between IP stations and for Bandwidth Management. SIP trunks require a unique zone, not shared with other resources and best practice dictates that IP telephones, IP telephones and Media Gateways are all placed in separate zones. 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.

CS1000 Element Manager

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

**Bandwidth Zones**

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

Zone	Intrazone Bandwidth	Intrazone Strategy	Interzone Bandwidth	Interzone Strategy	Resource Type	Zone Intent	Description
1 10	1000000	BQ	1000000	BB	SHARED	MO	MAINOFFICE
2 20	1000000	BQ	1000000	BB	SHARED	VTRK	VTRK

## 5.6. Configure Incoming Digit Conversion Table

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

CS1000 Element Manager

Managing: 192.168.0.2 Username: admin  
Dialing and Numbering Plans » Incoming Digit Translation » Customer:00 » Digit Conversion Tree 0 Configuration

**Digit Conversion Tree 0 Configuration**

Regular IDC tree  
Send calling party DID disabled

Add... Delete IDC Delete IDC tree Refresh

Incoming Digits	Converted Digits	CPND Name	CPND Language
1 16159	8000		
2 16160	8889		
3 16161	8001		
4 16162	8050		

## 5.7. Configure SIP Trunks

Communication Server 1000E virtual trunks will be used for all inbound and outbound PSTN calls to BTW/HIPCOM'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 5.3**. The value for **ZONE** should match that used in **Section 5.4** for **SIP\_VTRK**. The remaining highlighted values are important for correct SIP trunk operation.

<b>Overlay 16</b> TYPE: RDB CUST 00 ROUT 100 TYPE RDB CUST 00 <b>ROUT 100</b> DES VIR_TRK <b>TKTP TIE</b> NPID_TBL_NUM 0 ESN NO RPA NO CNVT NO SAT NO RCLS EXT <b>VTRK YES</b> <b>ZONE 00020</b> <b>PCID SIP</b> CRID NO <b>NODE 5000</b> DTRK NO <b>ISDN YES</b> <b>MODE ISLD</b> <b>DCH 10</b> <b>IFC SL1</b> 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 <b>ICOG IAO</b> SRCH LIN TRMB YES STEP	<b>ACOD 1600</b> TCPP NO PII NO AUXP NO TARG CLEN 1 BILN NO OABS INST <b>IDC YES</b> 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
new 30
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 00020
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 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.

<b>Overlay 86</b> <b>new</b> CUST 0 FEAT rlb <b>RLI 24</b> ELC NO ENTR 0 LTER NO <b>ROUT 100</b> 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 0 CTBL 0 ISDM 0	FCI 0 FSNI 0 BNE NO DORG NO SBOC NRR PROU 1 IDBB DBD IOHQ NO OHQ NO CBQ NO  ISET 0 NALT 5 MFRL 0 OVLL 0
-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------

Next, configure Special Prefix Number(s) (SPN) which users will dial to reach PSTN numbers. Use the Communication Server 1000E system terminal and overlay 90. The following are some example SPN 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.

SPN 999 FLEN 3 ITOH NO CLTP NONE <b>RLI 24</b> SDRR NONE ITEI NONE	SPN 90 FLEN 7 ITOH NO CLTP NONE <b>RLI 24</b> SDRR NONE ITEI NONE	SPN 2 FLEN 7 ITOH NO CLTP NONE <b>RLI 24</b> SDRR NONE ITEI NONE	SPN 15 FLEN 3 ITOH NO CLTP NONE <b>RLI 24</b> SDRR NONE ITEI NONE
--------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------	------------------------------------------------------------------------------------	-------------------------------------------------------------------------------------

## 5.8. Configure Analog, Digital and IP Telephones

A variety of telephone types were used during the testing, the following is the configuration for the Avaya 1140e 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 5.4** for **VIRTUALSETS**.

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

---continued on next page---



---continued from previous page---

```
DVLD CROD CROD
CPND_LANG ENG
RCO 0
HUNT 0
LHK 0
PLEV 02
PUID
DANI NO
AST 00
IAPG 1
AACS NO
ITNA NO
DGRP
MLWU_LANG 0
MLNG ENG
DNDR 0
KEY 00 MCR 8000 0      MARP
      CPND
        CPND_LANG ROMAN
          NAME IP1140
          XPLN 10
          DISPLAY_FMT FIRST, LAST
01 MCR 8000 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 CCBF RTDD RBDD RBHD PGND OCBF 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 8866 0      MARP

CPND

CPND\_LANG ROMAN

NAME Digital Set

XPLN 10

DISPLAY\_FMT FIRST, LAST

**01** MCR 8866 0

CPND

CPND\_LANG ROMAN

NAME Digital Set

XPLN 10

DISPLAY\_FMT FIRST, LAST

02 DSP

03 MSB

04

05

06

07

08

09

10

11

12

13

14

15

16

17 TRN

18 AO6

19 CFW 16

20 RGA

21 PRK

22 RNP

23

24 PRS

25 CHG

26 CPN

27 CLT

28 RLT

29

30

31

Analog telephones are also configured using **Overlay 20**, the following example shows an analog port configured 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. **DTN** is required if the telephone uses DTMF dialing. Values **FAXA** and **MPTD** configure the port for T.38 Fax transmissions.

**Overlay 20 - Analog Telephone Configuration**

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

ERL 00000
WRLS NO
DN 8888
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 CCBF BNRD OCBF RTDD RBDD RBHD FAXA CNUD CNAD PGND FTTC
    FDSD NOVD CDMR PRED MCDD T87D SBMD PKCH MPTD
PLEV 02
PUID
AACS NO
MLWU_LANG 0
FTR DCFW 4
```

## 5.9. Configure the SIP Line Gateway Service

SIP terminal operation requires the 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 6.1**.

- **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**

AVAYA CS1000 Element Manager

Managing: 192.168.0.2 Username: admin  
System » IP Network » IP Telephony Nodes » Node Details » SIP Line Configuration

**Node ID: 5000 - 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

## 5.10. 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 **SIPLINEZONE** in **Section 5.4**. 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 8889
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 8889 0 MARP
    CPND
        CPND_LANG ROMAN
        NAME Sigma 1140
        XPLN 11
        DISPLAY_FMT FIRST, LAST*
01 HOT U 788889 MARP 0
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16
17 TRN
18 AO6
19 CFW 16
20 RGA
21 PRK
22 RNP
23 *
24 PRS
25 CHG
26 CPN
27
28
29
30
31
```

## 5.11. Save Configuration

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

The screenshot shows the AVAYA CS1000 Element Manager web interface. On the left is a navigation tree with categories like UCM Network Services, System, Customers, Routes and Trunks, Dialing and Numbering Plans, Phones, and Tools. The 'Tools' category is expanded, showing 'Backup and Restore' and 'Call Server'. The main content area is titled 'Call Server Backup'. It shows the managing IP as 10.80.51.60 and the username as admin. Below the title, there is an 'Action' dropdown menu set to 'Backup', and two buttons: 'Submit' (highlighted with a red box) and 'Cancel'.

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.

```
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. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager to receive and route calls over the SIP trunk between Communication Server 1000E and Session Manager. These instructions assume other administration activities have already been completed such as defining the SIP entity for Session Manager, defining the network connection between System Manager and Session Manager, and adding SIP endpoints. The following administration activities will be described.

- Define SIP Domain
- Define Location for Avaya Communication Server 1000E
- Configure the Adaptation Module.
- Define SIP Entities
- Define Entity Links
- Define Routing Policies
- Define Dial Patterns

Configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL **http://<ip-address>/SMGR**, where <ip-address> is the IP address of System Manager. Login with the appropriate credentials. Some administration screens have been abbreviated for clarity.

## 6.1. Define SIP domains

Expand **Elements** → **Routing** and select **Domains** from the left navigation menu, click **New** (not shown). Enter the following values and use default values for remaining fields.

- **Name** Enter the Domain Name specified for the SIP Gateway in **Section 5.3**. In the sample configuration, **avaya.com** was used
- **Type** Verify **sip** is selected
- **Notes** Add a brief description [Optional]

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

AVAYA Avaya Aura™ System Manager 6.1

Help | About | Change Password | Log off admin

Routing \* Home

Home / Elements / Routing / Domains- Domain Management

Domain Management

Commit Cancel Help ?

1 Item Refresh Filter: Enable

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

## 6.2. Define Location for Avaya Communication Server 1000E

Locations are used to identify logical and/or physical locations where SIP Entities reside, for purposes of bandwidth management or location-based routing. Expand **Elements** → **Routing** and select **Locations** from the left navigational menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Name** Enter a descriptive name for the location
- **Notes** Add a brief description [Optional]

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

- **IP Address Pattern** Enter the logical pattern used to identify the location. For the sample configuration, **10.10.8.\*** was used
- **Notes** Add a brief description [Optional]

Click **Commit** to save. The screenshot below shows the Location defined for Communication Server 1000E in the sample configuration.

The screenshot displays the configuration interface for a location. On the left is a navigation menu with options: Adaptations, SIP Entities, Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'General' and includes a note about Call Admission Control. Below this are fields for 'Name' (set to 'SipLab8') and 'Notes'. The 'Overall Managed Bandwidth' section shows 'Managed Bandwidth Units' as 'Kbit/sec' and an empty 'Total Bandwidth' field. The 'Per-Call Bandwidth Parameters' section shows 'Default Audio Bandwidth' as '80 Kbit/sec'. The 'Location Pattern' section has 'Add' and 'Remove' buttons and a table with 2 items. The table has columns for 'IP Address Pattern' and 'Notes'. The first row shows '10.10.2.\*' and the second row shows '10.10.8.\*', both highlighted with red boxes. At the top right of the configuration area, there is a note: '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'.

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

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**

2 Items Refresh  Filter: Enable

<input type="checkbox"/>	IP Address Pattern	Notes
<input type="checkbox"/>	* 10.10.2.*	<input type="text"/>
<input type="checkbox"/>	* 10.10.8.*	<input type="text"/>

### 6.3. Configure 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 SBC to ensure ingress messages have the hostname **avaya.com** when they are sent to the Session Manager and to the CSIK. 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
- **Module Name:** <click to add module> from the drop down list and enter **DigitConversionAdapter** in the resulting **New Module Name** field
- **Module Parameter:** Enter the modification parameters to be used. In this configuration the modification parameters used was **iodstd=avaya.com**

**iodstd** (or **ingressOverrideDestinationDomain**) replaces **the domain in** a Request-URI and Notify/message-summary body with the given value for ingress only. The reason why this was added was that incoming calls to the enterprise had BTW/HIPCOM's domain name in the SIP messages. The domain on the enterprise is avaya.com so this Adaption Module changed incoming SIP messages destined for the enterprise to a recognised domain.

The screenshot shows the configuration interface for the DigitConversionAdapter module. On the left is a sidebar menu with 'Adaptations' highlighted. The main area is titled 'General' and contains a form for configuring the adaptation. The form fields are: 'Adaptation name' (text box with 'ChangeURI'), 'Module name' (dropdown menu with 'DigitConversionAdapter'), 'Module parameter' (text box with 'iodstd=avaya.com'), 'Egress URI Parameters' (text box), and 'Notes' (text box). Below the form are two sections: 'Digit Conversion for Incoming Calls to SM' and 'Digit Conversion for Outgoing Calls from SM'. Each section has 'Add' and 'Remove' buttons, a '0 Items' status, a 'Refresh' button, and a 'Filter' button. Below each section is a table with columns: Matching Pattern, Min, Max, Phone Context, Delete Digits, Insert Digits, and Address to modify.

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify
------------------	-----	-----	---------------	---------------	---------------	-------------------

## 6.4. Define SIP Entities

A SIP Entity must be added for Communication Server 1000E and also for the SBC. Expand **Elements** → **Routing** and select **SIP Entities** from the left navigation menu. 2 new SIP Entities will need to be added as noted above. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Name** Enter an identifier for the SIP Entity
- **FQDN or IP Address** Enter TLAN IP address of Communication Server 1000E Node identified in **Section 5.3**. For the SBC enter the private interface IP address
- **Type** Select **Other** for the Communication Server 1000E and **gateway** for the SBC
- **Notes** Enter a brief description [Optional]
- **Adaptations** CS1000Adapter defined in **Section 6.3**
- **Location** Select the Location defined for Communication Server 1000E in **Section 6.2** and also apply this same location to the SBC

In the **SIP Link Monitoring** section.

- **SIP Link Monitoring** Select **Use Session Manager Configuration**

Click **Commit** to save the definition of the new SIP Entity. The following screenshot shows the SIP Entity defined for Communication Server 1000E in the sample configuration.

The screenshot shows the 'SIP Entity Details' configuration page for a SIP Entity named 'CS1K'. The left navigation pane is expanded to 'Routing' > 'SIP Entities'. The main content area is titled 'SIP Entity Details' and 'General'. The configuration fields are as follows:

- Name:** CS1K
- FQDN or IP Address:** 10.10.8.3
- Type:** Other
- Notes:** (empty)
- Adaptation:** (empty)
- Location:** SipLab8
- Time Zone:** Etc/GMT

Below these fields, there are checkboxes for 'Override Port & Transport with DNS SRV' (unchecked) and 'SIP Timer B/F (in seconds):' (4). There is also a 'Credential name:' field (empty) and a 'Call Detail Recording:' dropdown (set to 'none').

At the bottom, the 'SIP Link Monitoring' section is expanded, showing 'SIP Link Monitoring:' set to 'Use Session Manager Configuration'.

A 'Commit' button is visible in the top right corner.

The following screenshot shows the SIP Entity defined for SBC in the sample configuration, note the adaption created in **Section 6.3** is associated with this entity link.

The screenshot displays the 'SIP Entity Details' configuration page. On the left is a navigation menu with options: Routing, Domains, Locations, Adaptations, SIP Entities (highlighted with a red box), Entity Links, Time Ranges, Routing Policies, Dial Patterns, Regular Expressions, and Defaults. The main content area is titled 'SIP Entity Details' and has a 'General' tab selected. A red rectangular box highlights the configuration fields for the entity 'AASBC'. These fields include: Name (AASBC), FQDN or IP Address (10.10.8.62), Type (Gateway), Notes (empty), Adaptation (ChangeURI), Location (SipLab8), Time Zone (Europe/Dublin), Override Port & Transport with DNS SRV (unchecked), SIP Timer B/F (in seconds) (4), Credential name (empty), and Call Detail Recording (none). Below the red box, the 'SIP Link Monitoring' section is partially visible.

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

SIP Entity Details

General

\* Name: AASBC

\* FQDN or IP Address: 10.10.8.62

Type: Gateway

Notes:

Adaptation: ChangeURI

Location: SipLab8

Time Zone: Europe/Dublin

Override Port & Transport with DNS SRV: ☐

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

Credential name:

Call Detail Recording: none

SIP Link Monitoring

A SIP Entity link must also be defined for your Session Manager but that is not shown in this document.

## 6.5. Define Entity links

The SIP trunk between the Session Manager and the Communication Server 1000E is described by an Entity link. The same is needed between the Session Manager and SBC. Expand **Elements** → **Routing** and select **Entity Links** from the left navigation menu. Click **New** (not shown).

Enter the following values.

- **Name** Enter an identifier for the link to each telephony system
- **SIP Entity 1** Select SIP Entity defined for **Session Manager**
- **SIP Entity 2** Select the SIP Entity defined for Avaya Communication Server 1000E/SBC in **Section 6.3** i.e. **CS1K**
- **Protocol** After selecting both SIP Entities, select **TCP** as the required protocol
- **Port** Verify **Port** for both SIP entities is the default listen port. For the sample configuration, default listen port is **5060**
- **Trusted** Enter a tick in the box
- **Notes** Enter a brief description [Optional]

Click **Commit** to save **Entity Link** definition. The following screen shows the entity link defined for the SIP trunk between Session Manager and Communication Server 1000E.

The screenshot shows the 'Entity Links' configuration page. The left navigation menu has 'Entity Links' highlighted. The main area displays a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Trusted, and Notes. The entry is for 'CS1K', with SIP Entity 1 set to 'Session Manager', Protocol to 'TCP', Port to '5060', SIP Entity 2 set to 'CS1K', Port to '5060', and 'Trusted' checked. The Notes field contains 'toCS1K'.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* CS1K	* Session Manager	TCP	* 5060	* CS1K	* 5060	<input checked="" type="checkbox"/>	toCS1K

The following screen shows the entity link defined for the SIP trunk between Session Manager and SBC.

The screenshot shows the 'Entity Links' configuration page. The left navigation menu has 'Entity Links' highlighted. The main area displays a table with one item. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Trusted, and Notes. The entry is for 'toAASBC', with SIP Entity 1 set to 'Session Manager', Protocol to 'TCP', Port to '5060', SIP Entity 2 set to 'AASBC', Port to '5060', and 'Trusted' checked. The Notes field contains 'toAASBC'. Below the table, there is a red asterisk and the text 'Input Required'.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* toAASBC	* Session Manager	TCP	* 5060	* AASBC	* 5060	<input checked="" type="checkbox"/>	toAASBC

\* Input Required

## 6.6. Define Routing Policy

Routing policies describe the conditions under which calls will be routed to CS1K from either SIP endpoint registered to Session Manager or from other telephony system. It also describes the routing policies for which calls will be routed to the SBC and therefore to BTW/HIPCOM's SIP network. To add a routing policy, expand **Elements** → **Routing** and select **Routing Policies**. Click **New** (not shown). In the **General** section, enter the following values.

- **Name** Enter an identifier to define the routing policy
- **Disabled** Leave unchecked
- **Notes** Enter a brief description [Optional]

In the **SIP Entity as Destination** section, click **Select**. The **SIP Entity List** page opens (not shown). For routing policy to the Communication Server 1000E, select the SIP Entity associated with Communication Server 1000E defined in **Section 6.4** and click **Select**. The selected SIP Entity displays on the **Routing Policy Details** page. Use default values for remaining fields. Click **Commit** to save Routing Policy definition.

**Note:** The routing policy defined in this section is an example and was used in the sample configuration. Other routing policies may be appropriate for different customer networks.

The following screenshot shows the Routing Policy for CS1K:

Routing Policy Details

**General**

\* Name:

Disabled: ☐

Notes:

**SIP Entity as Destination**

Name	FQDN or IP Address	Type	Notes
CS1K	10.10.8.3	Other	



For routing policy to the SBC – BTW/HIPCOM SIP Trunk, select the SIP Entity associated with SBC defined in **Section 6.4** and click **Select**. The selected SIP Entity displays on the **Routing Policy Details** page. Use default values for remaining fields. Click **Commit** to save Routing Policy definition. The following screenshot shows the Routing Policy for SBC – BTW/HIPCOM SIP trunk.

Routing Policy Details Commit

**General**

\* Name:

Disabled: ☐

Notes:

**SIP Entity as Destination**

Name	FQDN or IP Address	Type	Notes
AASBC	10.10.8.62	Gateway	

## 6.7. Define Dial Pattern

Dial patterns are used to route calls to appropriate SIP Entities. In the sample configuration, since the DDI range given for the testing all numbers that start with **44203** will be routed to the Communication Server 1000E for terminating to test sets. Alternately calls that are originated on the Communication Server 1000E that start with digits **00353** will be routed to the SBC and then on to BTW/HIPCOM's SIP network, there is a dialing pattern added for this as well. To define a dial pattern, expand **Elements** → **Routing** and select **Dial Patterns** (not shown). Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Pattern** Enter dial pattern for calls to Avaya Communication Server 1000E
- **Min** Enter the minimum number digits that must be dialed
- **Max** Enter the maximum number digits that may be dialed
- **SIP Domain** Select the SIP Domain from drop-down menu or select **All** if Session Manager should accept incoming calls from all SIP domains
- **Notes** Enter a brief description [Optional]

In the **Originating Locations and Routing Policies** section, click **Add**. The **Originating Locations and Routing Policy List** page opens (not shown).

- **Originating Locations** Select **ALL**
- **Routing Policies** Select the Routing Policy defined for Communication Server 1000E in **Section 6.6**

Click **Select** to save these changes and return to **Dial Pattern Details** page. Click **Commit** to save. The following screen shows the Dial Pattern defined for sample configuration. The following screenshot shows the Routing Policy for Communication Server 1000E.

The screenshot displays two configuration pages from a network management interface. The top page, 'Dial Pattern Details', shows the 'General' tab with fields for Pattern (44203), Min (5), Max (12), SIP Domain (-ALL-), and Notes. The bottom page, 'Originating Locations and Routing Policies', shows a table with one item: Any Locations, toCS1K, Rank 0, Routing Policy Disabled, and Routing Policy Destination CS1K.

**Dial Pattern Details**

General

\* Pattern: 44203

\* Min: 5

\* Max: 12

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	toCS1K	0	<input type="checkbox"/>	CS1K	

Repeat the above steps to add the dial Pattern to the SBC, select the routing policy defined for the SBC in **Section 6.5**. The following screenshot shows the Routing Policy for SBC – BTW/HIPCOM’s SIP network.

**Dial Pattern Details** Commit

**General**

\* Pattern:

\* Min:

\* Max:

Emergency Call: ☐

SIP Domain:

Notes:

**Originating Locations and Routing Policies**

Add Remove

1 Item Refresh Filter:

<input type="checkbox"/>	Originating Location Name <small>1 ▲</small>	Originating Location Notes	Routing Policy Name	Rank <small>2 ▲</small>	Routing Policy Disabled	Routing Policy Destination	Routing P Notes
<input type="checkbox"/>	SipLab8		toAASBC	0	<input type="checkbox"/>	AASBC	

Select: All None

## 7. Configure Avaya Aura® Session Border Controller

This section provides the procedures for configuring SBC to receive and route calls over the SIP trunk between CS1K and BTW/HIPCOM SIP Trunks. These instructions assume other administration activities have already been completed such as the default configuration. This section will cover the configuration that was put in place specifically for BTW/HIPCOM. For more information regarding the configuration of the SBC, please refer to the sample SBC configuration file in **Appendix B**. In **Appendix B**, note that public IP addresses have been taken out for security purposes.

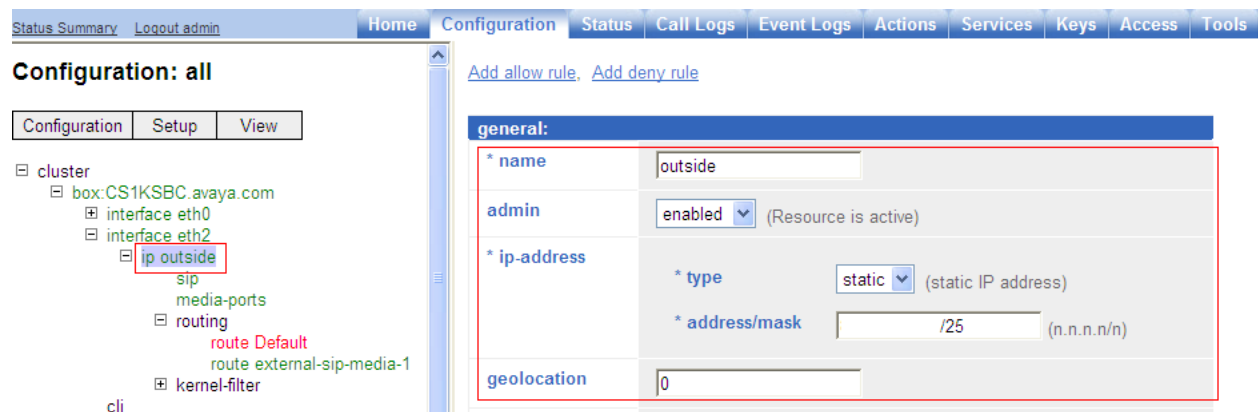
### 7.1. Access Avaya Aura® Session Border Controller

Access the SBC using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the private IP address configured.



### 7.2. Configuring Outside Interface

An ip address was given to the outside interface that is on the public internet. The ip address is blanked out in the screenshot below for security purposes. Click on the **Configuration** tab and browse to **cluster** → **interface eth2** → **ip outside**.



## 7.2.1. Configure SIP

For the outside interface a transport protocol needs to be configured. In the compliance testing UDP was used as the transport method for the SIP messaging. Click on the **Configuration** tab and browse to **cluster → interface eth2 → ip outside → sip → Add udp-port**

- **Port** Port number to be used for SIP messaging, default is **5060**

**Configuration: all**

Configuration Setup View

cluster

- box:cs1ksbc.avaya.com
  - interface eth0
  - interface eth2
    - ip outside
      - sip

**Create cluster/box 1/interface eth2/ip outside/sip/udp-port 5060 - Step 1 of 1: Edit**

Please provide some basic information for udp-port 5060. Then press "Create".

\* port 5060 (at minimum 1,default=5060)

Create Reset Cancel

The newly created UDP port is shown below.

**Configuration: all**

Configuration Setup View

cluster

- box:CS1KSBC.avaya.com
  - interface eth0
  - interface eth2
    - ip outside
      - sip

**Configure cluster/box:CS1KSBC.avaya.com/interface eth2/ip outside/sip** Help Index

Set Reset Back Delete

admin enabled (Resource is active)

nat-translation disabled (Resource is inactive)

nat-add-received-from disabled (Resource is inactive)

nat-add-X-Remote-Info enabled (Resource is active)

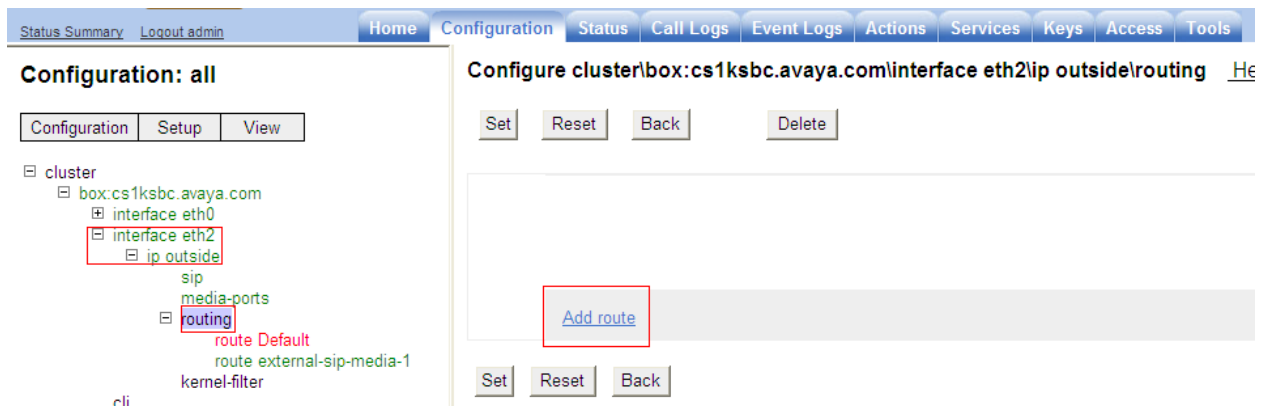
load-balance-head-end false

udp-port

	udp-port	from-server	to-server	transport	remote-port	certificate
Edit Delete	udp-port 5060	Edit	Edit	any	0	Edit

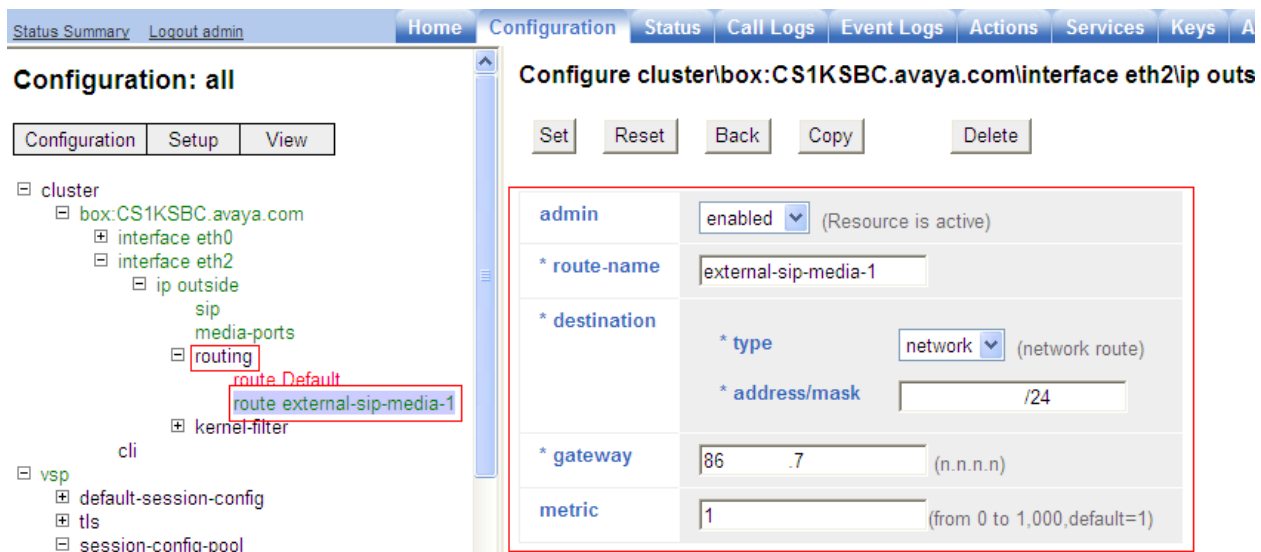
## 7.2.2. Configure Routing

For the outside interface routing needs to be configured to advise the SIP traffic how to route out to BTW/HIPCOM's network from the outside interface of the SBC. The ip address is blanked out in the screenshot below for security purposes. Click on the **Configuration** tab and browse to **cluster → interface eth2 → ip outside → routing → add route**.



The following values need to be added for the new route that is being created:

- **admin** Enables or disables this route configuration
- **route name** Enter a name for the route
- **destination type** Use network as the network route
- **destination address/mask** The destination address is the subnet used by the service provider and mask
- **gateway** Sets the gateway or next hop IP address for the packet
- **metric** Associates a cost for the route, default is 1



## 7.3. Configuring VSP

### 7.3.1. Configure Session-Config-Pool Entry ToTelco

In the **to-uri-specification** a valid host was added for BTW/HIPCOM. Expand **vsp** → **session-config pool** → **entry ToTelco** → **to-uri-specification**. For the testing domain **uk.ic.static.hipcom.co.uk** was used as shown below.

**Notes:** The domain name used by BTW/HIPCOM will change depending on access method, please consult BTW/HIPCOM to confirm what this will be.

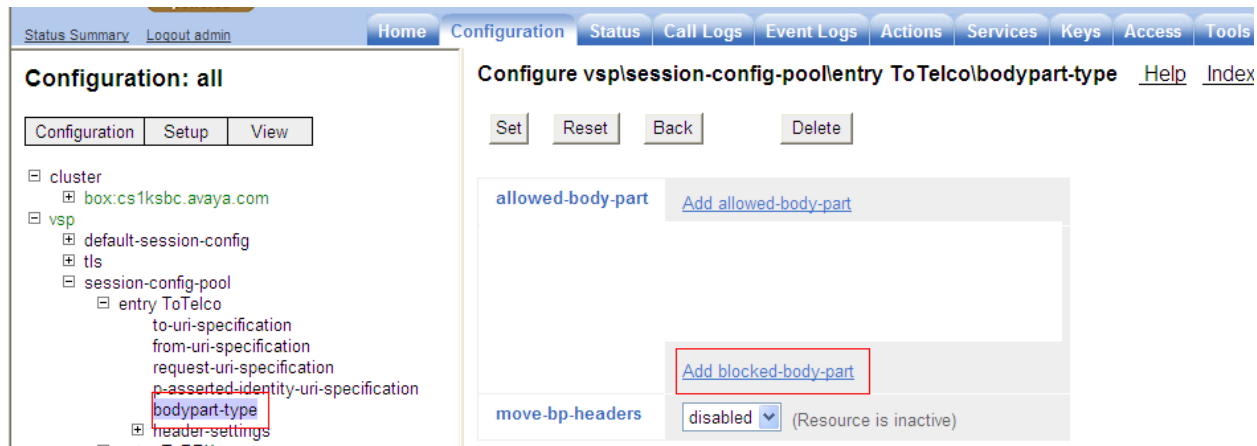
The screenshot shows the Avaya Aura Configuration interface. On the left, a tree view shows the navigation path: **cluster** → **box:cs1ksbc.avaya.com** → **vsp** → **default-session-config** → **tls** → **session-config-pool** → **entry ToTelco** → **to-uri-specification**. The main area displays the configuration form for 'Configure vspsession-config-poolentry ToTelco to-uri-specification'. The form includes fields for **user**, **host**, **port**, **display**, and **transport**. The **host** field is set to 'uk.ic.static.hipcom.co.uk'. The **transport** field is set to 'to-uri'. A red box highlights the form fields.

In the **from-uri-specification** a valid host was added for BTW/HIPCOM. Expand **vsp** → **session-config pool** → **entry ToTelco** → **to-from-specification**. For the testing domain **uk.ic.static.hipcom.co.uk** as seen below.

The screenshot shows the Avaya Aura Configuration interface. On the left, a tree view shows the navigation path: **cluster** → **box:cs1ksbc.avaya.com** → **vsp** → **default-session-config** → **tls** → **session-config-pool** → **entry ToTelco** → **from-uri-specification**. The main area displays the configuration form for 'Configure vspsession-config-poolentry ToTelco from-uri-specification'. The form includes fields for **user**, **host**, **port**, and **display**. The **host** field is set to 'uk.ic.static.hipcom.co.uk'. The **port** field is set to 'from-uri'. A red box highlights the form fields.

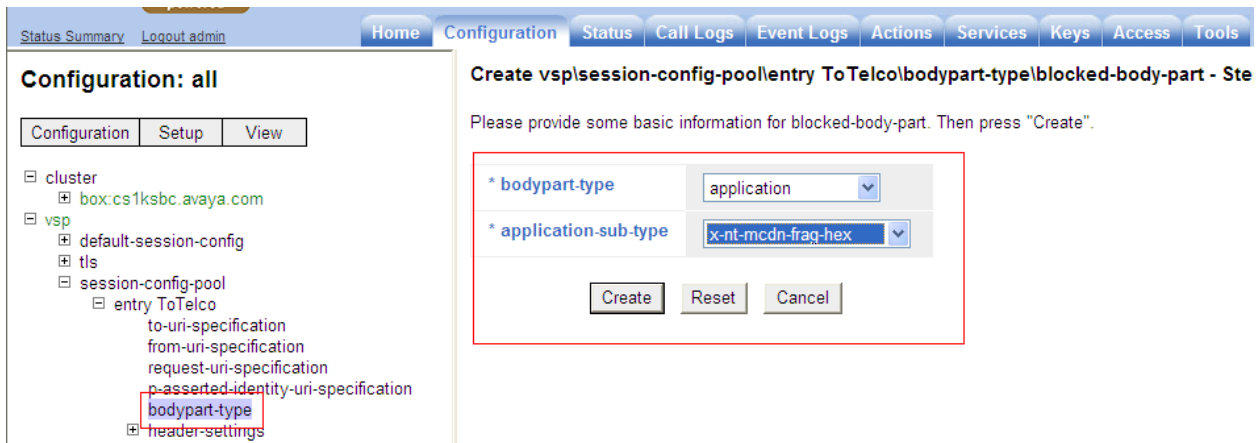
Repeat the same process to the change the host value in the request and p-asserted-identity headers to **uk.ic.static.hipcom.co.uk**, this is not shown.

Two new blocked body parts were also added. This sets the body part types to prohibit during the session. Any body sections that contain this type are removed from the message before forwarding. Expand **vsp** → **session-config pool** → **entry ToTelco** → **bodypart-type** → **Add blocked-body-part**.



The following values need to be added for the blocked-body-part.

- **bodypart-type** set this to **application**
- **application-sub-type** set this to **x-nt-mcdn-frag-hex**





The same process outlined above needs to be added for blocked body part **x-nt-epid-frag-hex**. In the below screenshot both blocked body parts are shown.

**Configuration: all**

Configuration Setup View

- cluster
  - box:CS1KSBC.avaya.com
- vsp**
  - default-session-config
  - tls
  - session-config-pool**
    - entry ToTelco**
      - to-uri-specification
      - from-uri-specification
      - request-uri-specification
      - p-asserted-identity-uri-specification
      - bodypart-type**
      - header-settings

**Configure vsp|session-config-pool|entry ToTelco|bodypart-type**

Set Reset Back Delete

allowed-body-part [Add allowed-body-part](#)

blocked-body-part		bodypart-type
▼	<a href="#">Edit</a> <a href="#">Delete</a>	application x-nt-mcdn-frag-hex
▲	<a href="#">Edit</a> <a href="#">Delete</a>	application x-nt-epid-frag-hex

[Add blocked-body-part](#)

move-bp-headers disabled (Resource is inactive)

### 7.3.2. Creating a new reg-ex-header

A reg-ex header was also added to change the host portion in the History-Info header so that it had a value of **uk.ic.static.hipcom.co.uk**. To define a new reg-ex-header click on **header settings** → **add reg-ex-header** and a new screen will appear as shown below.

- number:** Enter a unique number for the reg-ex-header
- destination:** Enter the header that is going to be manipulated, in this case **History-Info**

Then click on **Create**.

**Configuration**

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

**Configuration: all**

Configuration Setup View

- cluster
  - box:cs1ksbc.avaya.com
- vsp**
  - default-session-config
  - tls
  - session-config-pool**
    - entry ToTelco**
      - to-uri-specification
      - from-uri-specification
      - request-uri-specification
      - p-asserted-identity-uri-specification
      - bodypart-type
      - header-settings**

**Create vsp|session-config-pool|entry ToTelco|header-settings|reg-ex-header 0 - Step 1**

Please provide some basic information for reg-ex-header 0. Then press "Create".

\* number

\* destination enter  or select from <Not configured>

Create Reset Cancel

A new window will appear. In the create field click on **configure**. A new window appears as shown below with the following fields.

- **source** Enter the header that is going to be manipulated, in this case **History-Info**
- **expression** The expression to match in the manipulation, avaya.com - **(.\*)avaya.com(.\*)**
- **replacement** The expression to replace in the manipulation, uk.ic.static.hipcom.co.uk - **\1uk.ic.static.hipcom.co.uk\2**

The following screen shows the actual reg-ex-header that was configured for BTW/HIPCOM.

Configuration										
Configure vspsession-config-poolentry ToTelcoheader-settings										
<a href="#">Set</a> <a href="#">Reset</a> <a href="#">Back</a> <a href="#">Delete</a>										
<a href="#">allowed-header</a> <a href="#">Edit allowed-header</a>										
<a href="#">blocked-header</a> <a href="#">Edit blocked-header</a>										
<a href="#">altered-header</a> <a href="#">Add altered-header</a>										
reg-ex-header										
	reg-ex-header	admin	destination	create	append	apply-to-methods	apply-to-responses	apply-to-dialog	session-persis	
<a href="#">Edit</a>	<a href="#">Delete</a>	reg-ex-header 350	enabled	History-Info	History-Info (.*avaya.com(.*)\1uk.ic.static.hipcom.co.uk\2		INVITE	no	both	disable

### 7.3.3. Configure Session-Config-Pool Entry ToPBX

In the **to-uri-specification** a new **host** was added **avaya.com**. This is the SIP domain used in the enterprise and is configured in Section 6.1. Expand **vsp** → **session-config pool** → **entry ToPBX** → **to-uri-specification**. Enter **avaya.com** in the **host** field and click on **Set**.

Configuration: all

Configuration Setup View

cluster

box:CS1KSBC.avaya.com

vsp

default-session-config

tls

session-config-pool

entry ToTelco

to-uri-specification

from-uri-specification

request-uri-specification

p-asserted-identity-uri-specification

bodypart-type

header-settings

entry ToPBX

to-uri-specification

request-uri-specification

Configure vsp|session-config-pool|entry ToPBX|to-uri-specification Help Index

Set Reset Back Delete

user enter to-uri or select from to-uri (Net-Net OS-E uses t)

host enter avaya.com or select from avaya.com

port enter to-uri or select from to-uri (Net-Net OS-E uses t)

display enter to-uri or select from to-uri (Net-Net OS-E uses t)

transport to-uri (Net-Net OS-E uses the value from the incoming TO URI.)

user-param omit

user-truncate-non-digits disabled (Resource is inactive)

In the **request-uri-specification** a new **host** was added **avaya.com**. This is the SIP domain used in the enterprise and is configured in Section 6.1. Expand **vsp** → **session-config pool** → **entry ToPBX** → **request-uri-specification**. Enter **avaya.com** in the **host** field and click on **Set**.

Configuration: all

Configuration Setup View

cluster

box:CS1KSBC.avaya.com

vsp

default-session-config

tls

session-config-pool

entry ToTelco

to-uri-specification

from-uri-specification

request-uri-specification

p-asserted-identity-uri-specification

bodypart-type

header-settings

entry ToPBX

to-uri-specification

request-uri-specification

Configure vsp|session-config-pool|entry ToPBX|request-uri-specification Help Index

Set Reset Back Delete

user enter request-uri or select from request-uri (Net-Net OS-E uses t REQUEST URI.)

host enter avaya.com or select from avaya.com

port enter request-uri or select from request-uri (Net-Net OS-E uses the URI.)

transport request-uri (Net-Net OS-E uses the value from the incoming REQUEST URI.)

user-param omit

user-truncate-non-digits disabled (Resource is inactive)

### 7.3.4. Configuring Enterprise

In the **sip-gateway-Telco** the **domain** name used is **avaya.com**. A newly added server was created for BTW/HIPCOM's SBC; information needed here is the ip address, port and transport protocol. Click on the **Configuration** tab and browse to **vsp** → **enterprise** → **servers** → **sip-gateway Telco** → **server-pool**. Click the **Add server** link.



A new window will appear as shown below

- **server name** Enter the name of the server pool configuration instance that you want to create or modify
- **admin** Enable or disable this server, default is enabled
- **host** Specifies ip address of the service provider's SBC
- **transport** Specifies the protocol used by the server
- **port** Specifies the port used by the server for SIP traffic

All other values in other fields are set as default.

The screenshot displays the Avaya SBC configuration interface. The top navigation bar includes tabs for Status Summary, Logout admin, Home, Configuration, Status, Call Logs, Event Logs, Actions, Services, Keys, Access, and Tools. The main window is titled 'Configuration: all' and shows a tree view on the left with the following structure:

- cluster
  - box:cs1ksbc.avaya.com
- vsp
  - default-session-config
  - tls
  - session-config-pool
    - entry ToTelco
    - entry ToPBX
      - to-uri-specification
      - request-uri-specification
    - entry Discard
  - dial-plan
  - enterprise
    - servers
      - sip-gateway PBX
      - sip-gateway Telco
        - vsp\session-config-pool\entry ToTelco
        - server-pool
  - dns

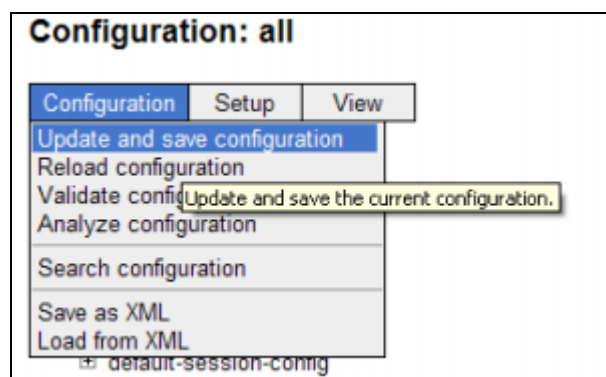
The right pane shows the configuration for 'Configure vsplenterprise\servers\sip-gateway Telco\server-poolserver Telco1'. The 'General' tab is active, showing the following fields:

- \* server-name: Telco1
- admin: enabled (Resource is active)
- \* host: 10.10.10.5 (host name or n.n.n.n)
- transport: transport UDP (User Datagram Protocol)
- port: 5060 (at minimum 1, default=5060)

The 'Policy' tab is also visible, showing 'outbound-normalization' and 'Add outbound-normalization'.

## 7.4. 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. BT Wholesale/HIPCOM Service Provider Configuration

The configuration of BTW/HIPCOM's equipment used to support the SIP trunk service is outside of the scope for these application notes and will not be covered. To obtain further information on BTW/HIPCOM's equipment and system configuration please contact an authorised BTW/HIPCOM representative.

## 9. Verification

### 9.1. 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
<b>LD 96 - D-Channel</b>
LD 117 - Ethernet and Alarm Management
LD 135 - Core Common Equipment
LD 137 - Core Input/Output
LD 143 - Centralized Software Upgrade

<Select Group>
<b>D-Channel Diagnostics</b>
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
<input type="radio"/> 010	Vtrk	OPER	EST ACTV	AUTO		

```

STAT DCH 010
-----
Command executed successfully.
  
```

## 9.2. Verify Avaya Aura® Session Manager Operational Status

### 9.2.1. 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

### 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 9:22 AM

1 Item Refresh Show ALL
Filter: Enable

	Session Manager	Type	Alarms	Tests Pass	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Version
<input type="checkbox"/>	Session Manager	Core	50/14/39	✓	Up	Accept New Service	0/5	0	0	6.1.0.0.610023

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.

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	Session Manager	SM	Up	14	10.10.8.56/24	---	10.10.8.1	Disabled	5/5	SIP CA

Select : None

## 9.2.2. 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 Communication Server 1000E 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: CS1000 Rel7.5** 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: CS1K

Summary View

1 Item Refresh

Filter: Enabled

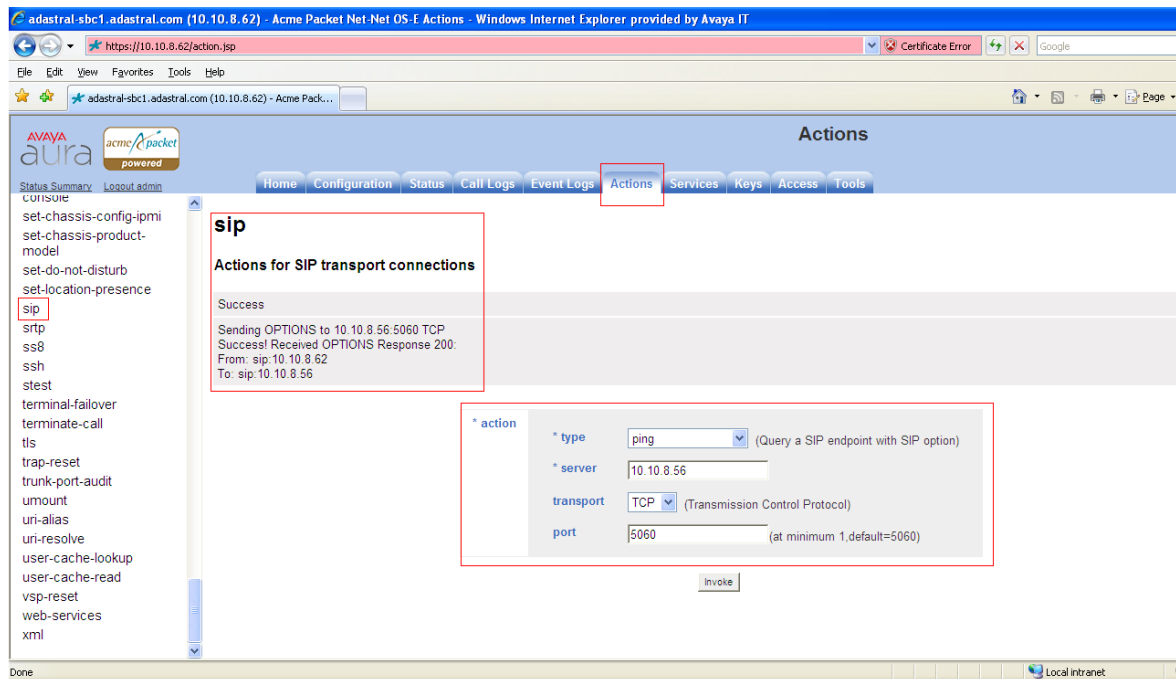
Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
► Show	Session Manager	10.10.8.3	5060	TCP	Up	200 OK	Up

Verify the SIP link is up between the Session Manager and the SBC by going through the same process as outlined above but selecting the SIP Entity for the SBC in the **All Monitored SIP Entities** table (not shown).



### 9.3. Verify Avaya Aura® Session Border Controller Operational Status

Navigate to **Actions** → select **SIP (left hand menu)** → action type select **PING** and enter the server you want to verify, in the screenshot below it is with the Session Manager (SM100) interface. The SBC sends an option message and a 200 OK is sent back.



## 10. Conclusion

These Application Notes describe the configuration necessary to connect the Avaya Communication Server 1000E, Avaya Aura® Session Manager and Avaya Aura® Session Border Controller to BTW/HIPCOM's SIP Service. The observation noted during this testing is detailed in **Section 2.2**.

## 11. Additional References

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

- [1] Avaya Aura® Session Manager Overview, Doc ID 03-603323, available at <http://support.avaya.com>.
- [2] Installing and Configuring Avaya Aura® Session Manager, available at <http://support.avaya.com>.
- [3] Avaya Aura® Session Manager Case Studies, available at <http://support.avaya.com>
- [4] Maintaining and Troubleshooting Avaya Aura® Session Manager, Doc ID 03-603325, available at <http://support.avaya.com>.
- [5] Administering Avaya Aura® Session Manager, Doc ID 03-603324, available at <http://support.avaya.com>

- [6] IP Peer Networking Installation and Commissioning, Release 7.5, Document Number NN43001-313, available at <http://support.avaya.com>
- [7] Unified Communications Management Common Services Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-116, available at <http://support.avaya.com>
- [8] Network Routing Service Fundamentals, Release 7.5, Document Number NN43001-130, Issue 03.02, available at <http://support.avaya.com>
- [9] 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>
- [10] Signaling Server and IP Line Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-125, available at <http://support.avaya.com>

# Appendix A

## Avaya Communication Server 1000E Software

### Communication Server 1000E call server patches and plug ins

08/04/11 10:25:28  
TID: 008808096

VERSION 4021

System type is - Communication Server 1000E/CP PM

CP PM - Pentium M 1.4 GHz

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

RELEASE 7  
ISSUE 50 Q +  
IDLE\_SET\_DISPLAY Avaya 7.5  
DepList 1: core Issue: 02(created: 2010-11-30 15:12:45 (est))

MDP>LAST SUCCESSFUL MDP REFRESH :2010-12-06 15:33:54(Local Time)  
MDP>USING DEPLIST ZIP FILE DOWNLOADED :2010-12-01 08:31:36(est)  
SYSTEM HAS NO USER SELECTED PEPS IN-SERVICE

LOADWARE VERSION: PSWV 100  
INSTALLED LOADWARE PEPS : 0  
ENABLED PLUGINS : 0

### Communication Server 1000E call server deplists

VERSION 4121  
RELEASE 7  
ISSUE 50 Q +  
DepList 1: core Issue: 01 (created: 2011-05-24 10:13:35 (est)) ALTERED

IN-SERVICE PEPS

PAT#	CR #	PATCH REF #	NAME	DATE	FILENAME	SPECINS
012	wi00843623	ISS1:10F1	p30731_1	16/06/2011	p30731_1.cpl	YES
013	WI00843571	ISS1:10F1	p30627_1	16/06/2011	p30627_1.cpl	NO
014	wi00871739	ISS1:10F1	p30856_1	16/06/2011	p30856_1.cpl	NO
015	wi00852365	ISS1:10F1	p30707_1	16/06/2011	p30707_1.cpl	NO
016	wi00852389	ISS1:10F1	p30641_1	16/06/2011	p30641_1.cpl	NO
017	wi00839134	ISS1:10F1	p30698_1	16/06/2011	p30698_1.cpl	YES
018	wi00856702	ISS1:10F1	p30573_1	16/06/2011	p30573_1.cpl	NO
019	wi00857566	ISS1:10F1	p30766_1	16/06/2011	p30766_1.cpl	NO
020	wi00850521	ISS1:10F1	p30709_1	16/06/2011	p30709_1.cpl	YES
021	wi00860722	ISS1:10F1	p30784_1	16/06/2011	p30784_1.cpl	YES
022	wi00863876	ISS1:10F1	p30787_1	16/06/2011	p30787_1.cpl	NO
023	WI00853473	ISS1:10F1	p30625_1	16/06/2011	p30625_1.cpl	NO
024	wi00854130	ISS1:10F1	p30443_1	16/06/2011	p30443_1.cpl	NO
025	wi00875425	ISS1:10F1	p30943_1	16/06/2011	p30943_1.cpl	NO
026	wi00853658	ISS1:10F1	p30990_1	16/06/2011	p30990_1.cpl	NO
027	wi00875701	ISS1:10F1	p30942_1	16/06/2011	p30942_1.cpl	NO
028	wi00853031	ISS1:10F1	p30531_1	16/06/2011	p30531_1.cpl	NO
029	wi00877367	ISS1:10F1	p30534_1	16/06/2011	p30534_1.cpl	NO
030	wi00871969	ISS1:10F1	p30768_1	16/06/2011	p30768_1.cpl	NO
031	wi00886321	ISS1:10F1	p31009_1	16/06/2011	p31009_1.cpl	NO
032	WI00836334	ISS1:10F1	p30481_1	16/06/2011	p30481_1.cpl	NO
033	wi00836182	ISS1:10F1	p30450_1	16/06/2011	p30450_1.cpl	NO
034	wi00858335	ISS1:10F1	p30819_1	16/06/2011	p30819_1.cpl	NO
035	wi00860279	ISS1:10F1	p30789_1	16/06/2011	p30789_1.cpl	NO
036	wi00866570	ISS1:10F1	p30477_1	16/06/2011	p30477_1.cpl	NO

037	wi00854415	ISS1:10F1	p30593_1	16/06/2011	p30593_1.cpl	NO
038	WI00836292	ISS1:10F1	p30554_1	16/06/2011	p30554_1.cpl	NO
039	WI00839794	ISS1:10F1	p28647_1	16/06/2011	p28647_1.cpl	NO
040	wi00824257	ISS1:10F1	p30447_1	16/06/2011	p30447_1.cpl	NO
041	wi00827950	ISS2:10F1	p30471_2	16/06/2011	p30471_2.cpl	NO
042	wi00879814	ISS1:10F1	p30970_1	16/06/2011	p30970_1.cpl	NO
043	WI00854150	ISS1:10F1	p30468_1	16/06/2011	p30468_1.cpl	NO
044	wi00873382	ISS1:10F1	p30832_1	16/06/2011	p30832_1.cpl	NO
045	wi00853178	ISS1:10F1	p30719_1	16/06/2011	p30719_1.cpl	NO
046	wi00869695	ISS1:10F1	p30654_1	16/06/2011	p30654_1.cpl	NO
047	wi00834382	ISS1:10F1	p30548_1	16/06/2011	p30548_1.cpl	NO
048	wi00836472	ISS1:10F1	p30626_1	16/06/2011	p30626_1.cpl	NO
049	wi00854409	ISS1:10F1	p30479_1	16/06/2011	p30479_1.cpl	NO
050	WI00728461	ISS1:10F1	p30346_1	16/06/2011	p30346_1.cpl	NO

MDP>LAST SUCCESSFUL MDP REFRESH :2011-05-25 10:18:44 (Local Time)

MDP>USING DEPLIST ZIP FILE DOWNLOADED :2011-05-25 04:41:04 (est)

## Communication Server 1000E signaling server service updates

Product Release: 7.50.17.00

In system patches: 0

In System service updates: 8

PATCH#	IN_SERVICE	DATE	SPECINS	REMOVABLE	NAME
0	Yes	07/02/11	NO	YES	cs1000-baseWeb-7.50.17.01-1.i386.000
1	Yes	07/02/11	NO	YES	cs1000-linuxbase-7.50.17.04-00.i386.000
2	Yes	07/02/11	NO	YES	cs1000-sps-7.50.17-01.i386.000
3	Yes	07/02/11	NO	YES	cs1000-shared-pbx-7.50.17-01.i386.000
4	Yes	07/02/11	NO	YES	cs1000-bcc-7.50.17.03-00.i386.000
5	Yes	07/02/11	NO	YES	cs1000-Jboss-Quantum-7.50.17.01-1.i386.000
6	Yes	07/02/11	NO	YES	cs1000-vtrk-7.50.17-11.i386.000
7	Yes	07/02/11	NO	YES	cs1000-dmWeb-7.50.17.04-00.i386.001

There is no SP in loaded status.

The last applied SP: Service Pack Linux 7.50 17 20110118.ntl, It is a STANDARD SP.

Has been applied by user nortel on Mon Feb 7 14:59:01 2011

## 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	
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	7.50.17	
Snmp-Daemon-TrapLib	7.50.17	
ISECSH	7.50.17	
patchWeb	7.50.17	
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	

vtrk	7.50.17	[patched]
pd	7.50.17	
sps	7.50.17	[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]
ftpkg	7.50.17	
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	

## Appendix B

# Sample Avaya Aura® Session Border Controller Configuration File

As noted in **Section 7**, in the following sample SBC configuration file, public IP Addresses have been masked for security purposes.

```
#
# Copyright (c) 2004-2011 Acme Packet Inc.
# All Rights Reserved.
#
# File: /cxc/cxc.cfg
# Date: 09:23:04 Wed 2011-08-03
#
config cluster
config box 1
  set hostname cs1ksbc.avaya.com
  set timezone Etc/GMT
  set name cs1ksbc.avaya.com
  set identifier 00:ca:fe:56:07:85
config interface eth0
  config ip inside
    set ip-address static 10.10.8.62/24
  config ssh
  return
  config snmp
    set trap-target 10.10.8.61 162
    set trap-filter generic
    set trap-filter dos
    set trap-filter sip
    set trap-filter system
  return
  config web
  return
  config web-service
    set protocol https 8443
    set authentication certificate "vsp\tls\certificate ws-cert"
  return
  config sip
    set udp-port 5060 "" "" any 0
    set tcp-port 5060 "" "" any 0
    set tls-port 5061 "" "" TLS 0 "vsp\tls\certificate aasbc.p12"
  return
  config icmp
  return
  config media-ports
  return
  config routing
    config route Default
      set gateway 10.10.8.1
    return
    config route Static0
      set destination network 192.11.13.4/30
```

```

    set gateway 10.10.8.60
    return
    config route Static2
    set admin disabled
    return
    config route Static3
    set admin disabled
    return
    config route Static4
    set admin disabled
    return
    config route Static5
    set admin disabled
    return
    config route Static6
    set admin disabled
    return
    config route Static7
    set admin disabled
    return
    return
    return
    return
    config interface eth2
    config ip outside
    set ip-address static xx.xx.xx.xx/25
    config sip
    set udp-port 5060 "" "" any 0
    set tcp-port 5060 "" "" any 0
    return
    config media-ports
    return
    config routing
    config route Default
    set admin disabled
    return
    config route external-sip-media-1
    set destination network xx.xx.xx.0/24
    set gateway xx.xx.xx.xx
    return
    return
    config kernel-filter
    return
    return
    return
    config cli
    set prompt cslksbc.avaya.com
    return
    return
    return

config services
config event-log
config file access
set filter access info
set count 3

```

```

return
config file system
    set filter system info
    set count 3
return
config file errorlog
    set filter all error
    set count 3
return
config file db
    set filter db debug
    set filter dosDatabase info
    set count 3
return
config file management
    set filter management info
    set count 3
return
config file peer
    set filter sipSvr info
    set count 3
return
config file dos
    set filter dos alert
    set filter dosSip alert
    set filter dosTransport alert
    set filter dosUrl alert
    set count 3
return
config file krnlsys
    set filter krnlsys debug
    set count 3
return
return
return

config master-services
config database
    set media enabled
return
return

config vsp
set admin enabled
config default-session-config
config media
    set anchor enabled
    set rtp-stats enabled
return
config sip-directive
    set directive allow
return
config log-alert
    set apply-to-methods-for-filtered-logs
return
config header-settings

```



```

return
config third-party-call-control
    set handle-refer-locally disabled
return
return
config tls
    config default-ca
        set ca-file /cxc/certs/sipca.pem
    return
    config certificate ws-cert
        set certificate-file /cxc/certs/ws.cert
    return
    config certificate aasbc.p12
        set certificate-file /cxc/certs/aasbc.p12
        set passphrase-tag aasbc-cert-tag
    return
return
config session-config-pool
    config entry ToTelco
        config to-uri-specification
            set host uk.ic.static.hipcom.co.uk
        return
        config from-uri-specification
            set host uk.ic.static.hipcom.co.uk
        return
        config request-uri-specification
            set host uk.ic.static.hipcom.co.uk
        return
        config p-asserted-identity-uri-specification
            set user from-uri
            set host uk.ic.static.hipcom.co.uk
        return
        config bodypart-type
            set blocked-body-part application x-nt-mcdn-frag-hex
            set blocked-body-part application x-nt-epid-frag-hex
        return
        config header-settings
            config reg-ex-header 350
            set destination History-Info
            set create History-Info (.*?)avaya.com(.*?)
"\luk.ic.static.hipcom.co.uk\2"
        return
    return
return
config entry ToPBX
    config to-uri-specification
        set host avaya.com
    return
    config request-uri-specification
        set host avaya.com
    return
return
config entry Discard
    config sip-directive
    return
return

```

```

return
config dial-plan
  config route Default
    set priority 500
    set location-match-preferred exclusive
    set session-config vsp\session-config-pool\entry Discard
  return
  config source-route FromTelco
    set peer server "vsp\enterprise\servers\sip-gateway PBX"
    set source-match server "vsp\enterprise\servers\sip-gateway Telco"
  return
  config source-route FromPBX
    set peer server "vsp\enterprise\servers\sip-gateway Telco"
    set source-match server "vsp\enterprise\servers\sip-gateway PBX"
  return
return
config enterprise
  config servers
    config sip-gateway PBX
      set domain avaya.com
      set failover-detection ping
      set outbound-session-config-pool-entry vsp\session-config-pool\entry
ToPBX
      config server-pool
        config server PBX1
          set host 10.10.7.61
          set transport TCP
        return
      return
    return
    config sip-gateway Telco
      set domain avaya.com
      set failover-detection ping
      set outbound-session-config-pool-entry vsp\session-config-pool\entry
ToTelco
      config server-pool
        config server Telco1
          set host xx.xx.xx.xx
        return
      return
    return
  return
return
config dns
  config resolver
    config server 10.10.7.100
  return
return
config settings
  set read-header-max 8191
return
return

config external-services
return

```

```

config preferences
  config gui-preferences
    set enum-strings RequestURISource uk.ic.static.hipcom.co.uk
    set enum-strings GeneralURISource uk.ic.static.hipcom.co.uk
    set enum-strings SIPSourceHeader History-Info
    set enum-strings RequestURISource avaya.com
  return
return

config access
  config permissions superuser
    set cli advanced
  return
  config permissions read-only
    set config view
    set actions disabled
  return
  config users
    config user admin
      set password 0x00c3da084a51ad08836ccad49283a1babca7bb621d17ce3b5ff788fd94
      set permissions access\permissions superuser
    return
    config user cust
      set password 0x003eb1074c8d3d30b83e1a77de17d2ea682827c07690a9bab5af1823d5
      set permissions access\permissions read-only
    return
    config user init
      set password 0x00108cd8c2081746d3bc7b7a0a0600f43178a84eb6342452c47b8f6bbd
      set permissions access\permissions superuser
    return
    config user craft
      set password 0x006273d242a7d36dd742e5917d626593833ab915aede6611f4f383e324
      set permissions access\permissions superuser
    return
    config user dadmin
      set password 0x004f373649700feb0ae40cb9d23587eeb0675e6c063a7d4ce5ea20ba77
      set permissions access\permissions read-only
    return
  return
return

config features
return

```

---

**©2011 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](mailto:devconnect@avaya.com).