Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Communication Server 1000E R7.5, Avaya Aura® Session Manager, Avaya Aura® Session Border Controller to support BT Genband Communication Server 2000 Release CVM13 SIP Trunk Service – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between BT's Genband Communication Server 2000 SIP Trunk Service and an Avaya SIP enabled Enterprise Solution. The Avaya solution consists of Avaya Aura® Session Manager, Avaya Aura® Session Border Controller and Avaya Communication Server 1000E.

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 Program at BT's Test Lab.

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between BT Genband Communication Server 2000 Hosted Voice SIP Trunk Service and an Avaya SIP enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager and Avaya Communication Server 1000E connected to the BT SIP Trunk Service via an Avaya Aura® Session Border Controller (SBC). Customers using this Avaya SIP-enabled enterprise solution with the BT 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 Session Manager, Avaya Aura® SBC and CS1000E. The enterprise site was configured to use the SIP Trunk to the Genband Communication Server 2000 (CS2K).

2.1. Interoperability Compliance Testing

The interoperability test included the following:

- 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.
- G729 annex b (silence suppression) is not supported by BT SIP Trunk Service and thus was not tested.
- G711mu is not supported by BT SIP Trunk Service and thus was not tested.
- Calls using G.729, G.711A codecs.
- 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 the BT CS2K Hosted Voice SIP Trunk with the following observations:

- Outbound fax calls from the Communication Server 1000E using codec G.729 before switching to T.38 do not work. Fax calls using the G.711 codec before switching to T.38 work successfully.
- No inbound toll free numbers were tested, however routing of inbound DID numbers and the relevant number translation was successfully tested.
- Routing to emergency numbers was tested.

2.3. Support

For technical support on BT products please contact the following website:
http://btbusiness.custhelp.com/app/contact

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an enterprise site connected to BT‘s CS2K using SIP Trunks. Located at the enterprise site are Session Manager, Avaya Aura® 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, 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.

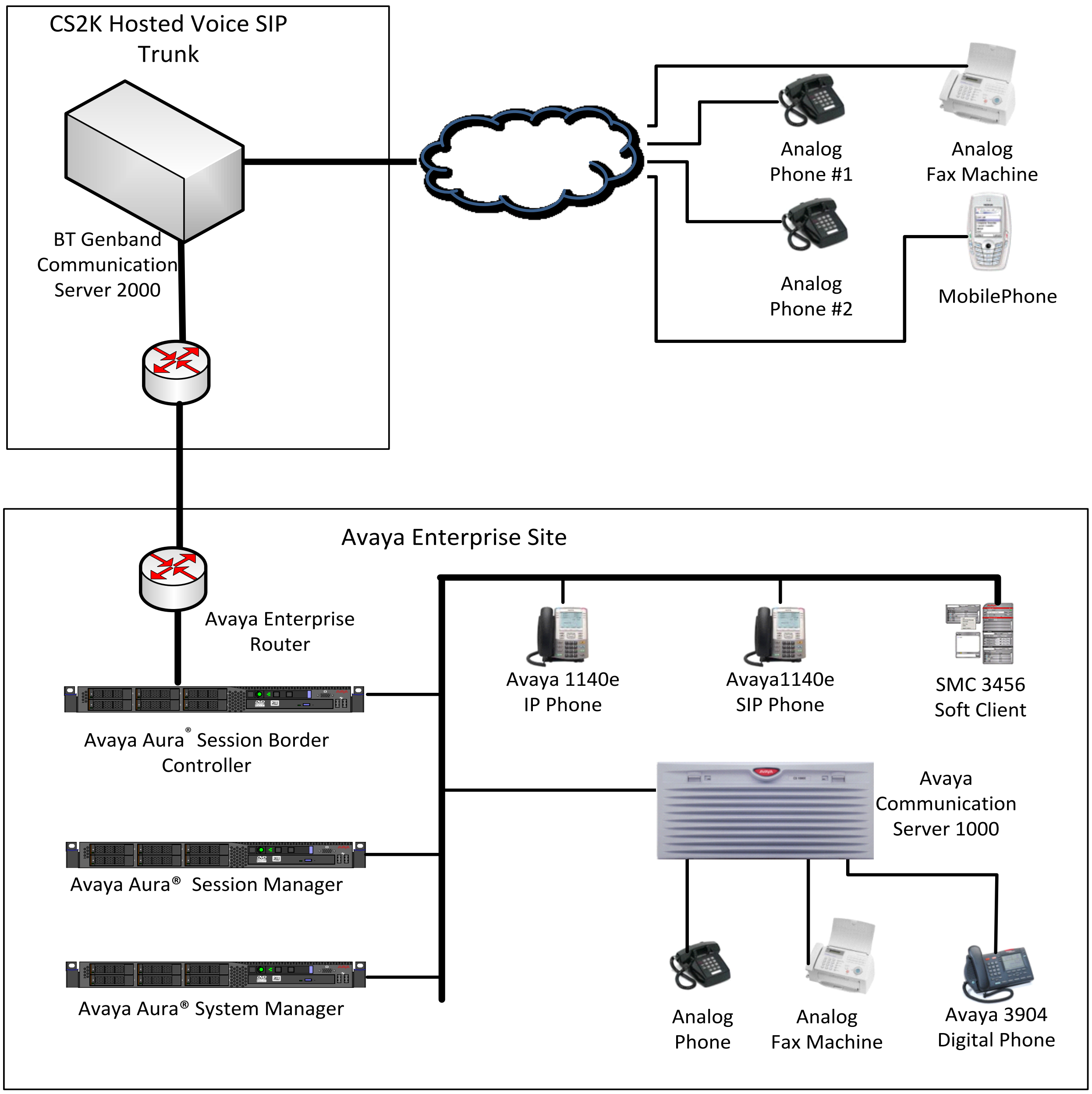


Figure 1: BT Genband Communication Server 2000 Hosted Voice SIP Trunk topology

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
Avaya S8800 server	Avaya Aura® System Manager R6.1 Load: 6.1.7.1.1260 Service Pack 3
Avaya S8800 server	Avaya Aura® Session Border Controller version 6.0.2.0.2 (E362P4)
Avaya Communication Server 1000E running on CP+PM server as co-resident configuration	Avaya Communication Server 1000E R 7.5, Version 7.50.17 Service Update: 7.50_17Nov30 Deplist: X21 07.50Q
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 AZ11+ p31161_1.mgc + p31043_1.mgc
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 Client	one-X® Communicator - cs6.1.0.10
Avaya Analogue Telephone	N/A
Avaya M3904 Digital Telephone	N/A
BT SIP Solution configuration	CVM13 - SSL/BCP 12.0.6.7 Solution version 1.0

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 the CS2K Hosted Voice SIP Trunk Service. For incoming calls, the Session Manager receives SIP messages from the SBC, through which the CS2K Hosted Voice SIP Trunk 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 the BT network. Specific

Communication Server 1000E configuration was performed using Element Manager and the system terminal interface. The general installation of the Avaya Communication Server 1000E and System Manager and Session Manager is presumed to have been previously completed and is not discussed here.

5.1. 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 the BT 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.

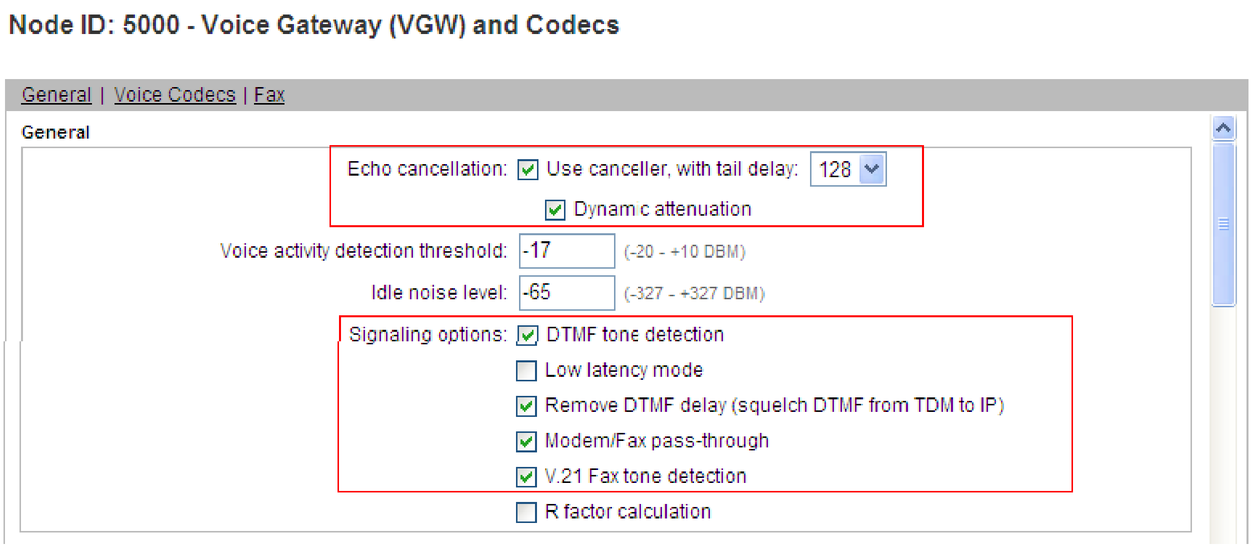
```
System type is - Communication Server 1000E/CPPM Linux
CPPM - Pentium M 1.4 GHz

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).

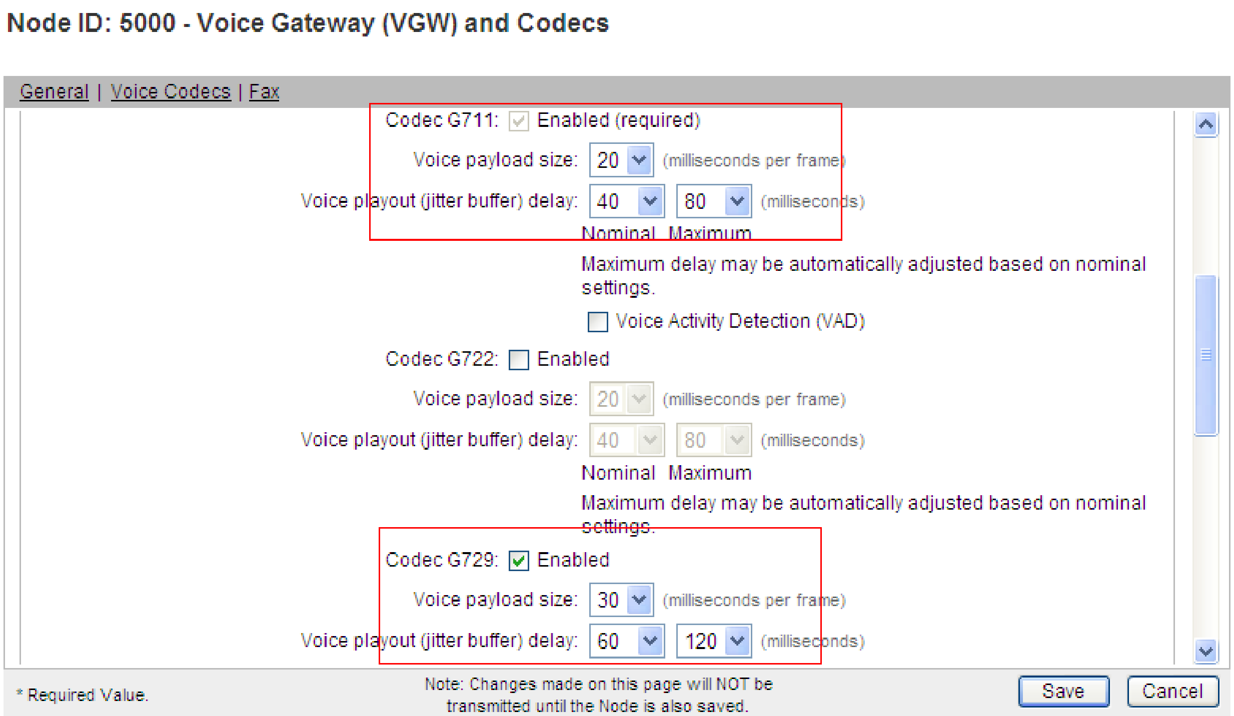
```
REQ: prt
TYPE: net
TYPE NET_DATA
CUST 0

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

5.2. Configure Codec's for Voice and FAX operation

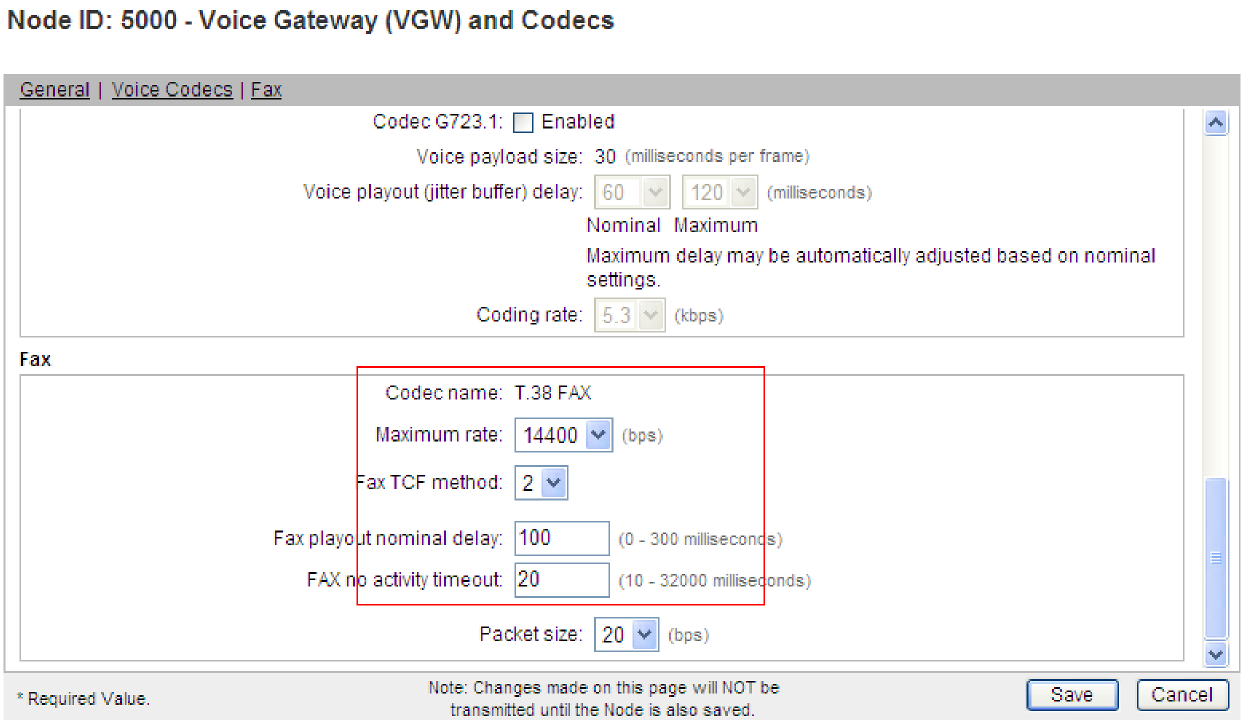
The CS2K Hosted Voice SIP Trunk service supports G.711A and G.729A voice codecs and T.38 FAX transmissions. Using the Communication Server 1000E element manager sidebar, navigate to the **IP Network → IP Telephony Nodes → Node Details → VGW and Codecs** property page and configure the Communication Server 1000E General codec settings as in the next screenshot. The values highlighted are required for correct operation.



Next, scroll down and configure the G.711 and G.729 codec settings. Voice payload size is 20 milliseconds for G.711 and 30 milliseconds for G.729 . The relevant settings are highlighted in the following screenshot.

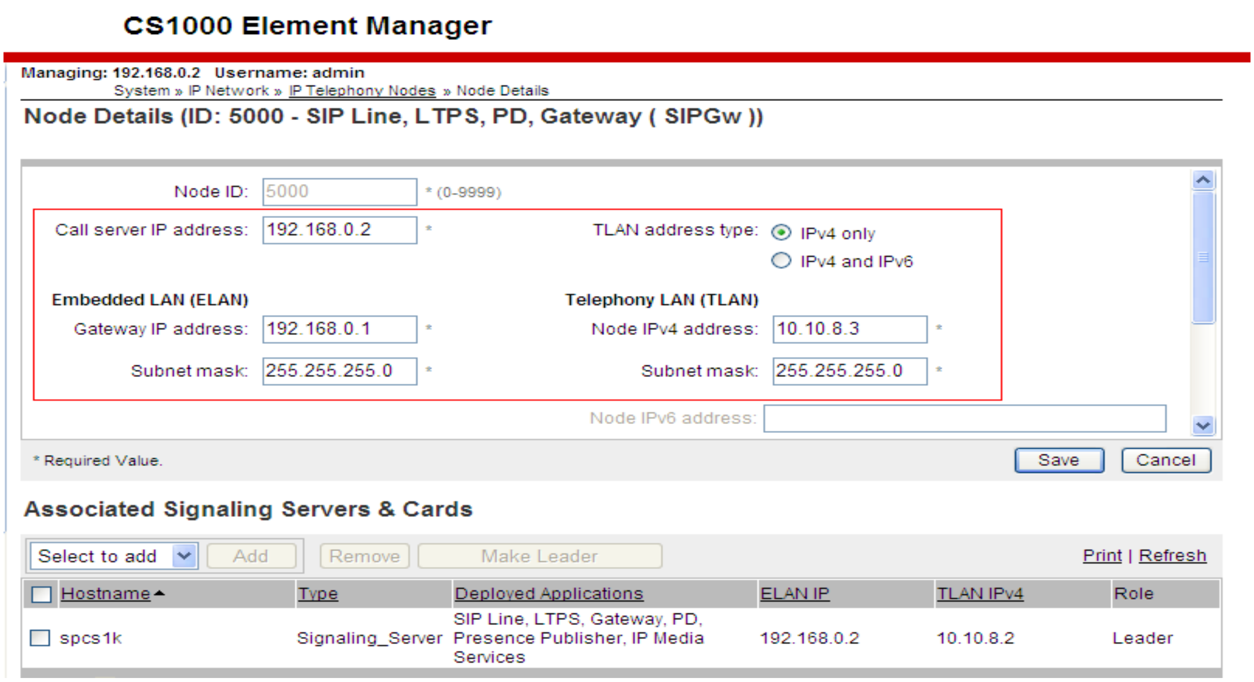


Finally, configure the Fax settings as in the highlighted section of the next screenshot.



5.3. Virtual Trunk Gateway Configuration

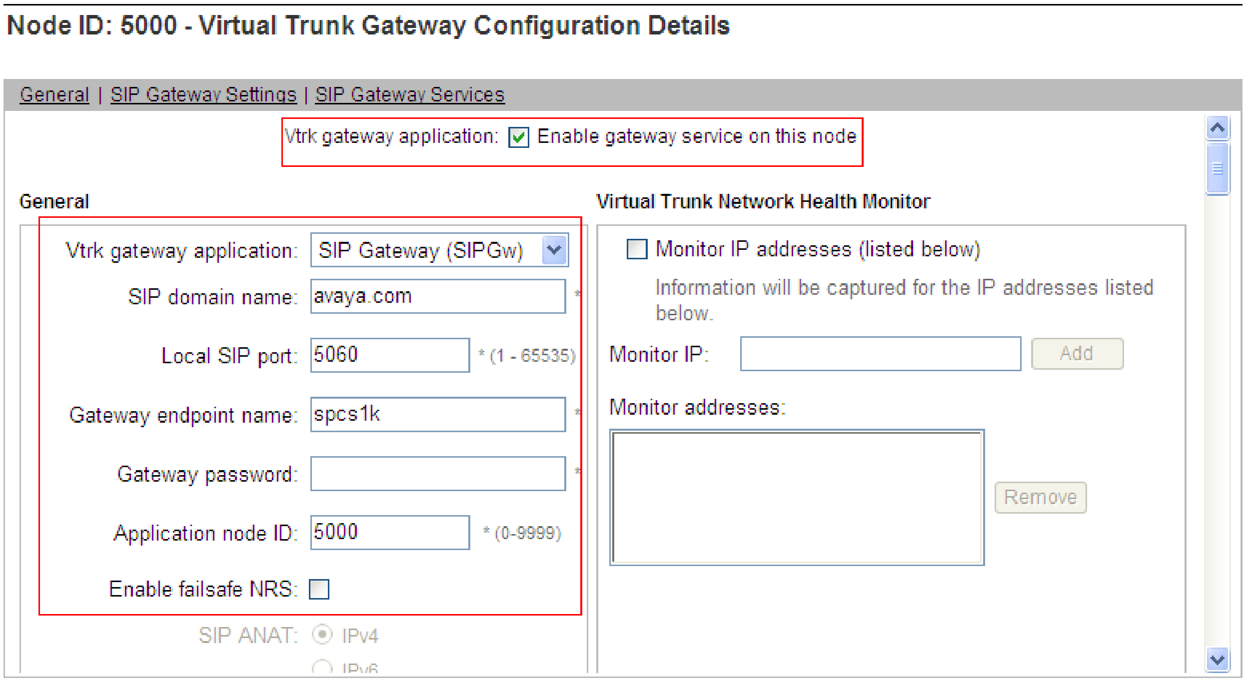
Use Communication Server 1000E Element Manager to configure the system node properties. Navigate to the **System → IP Network → IP Telephony Nodes → Node Details** and verify the highlighted section is completed with the correct IP addresses and subnet masks of the Node. At this stage the call server 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 is added in Session Manager for the CS1000E it is the Node ip that is used (please see **Section 6.4** – Define SIP Entities for more details).

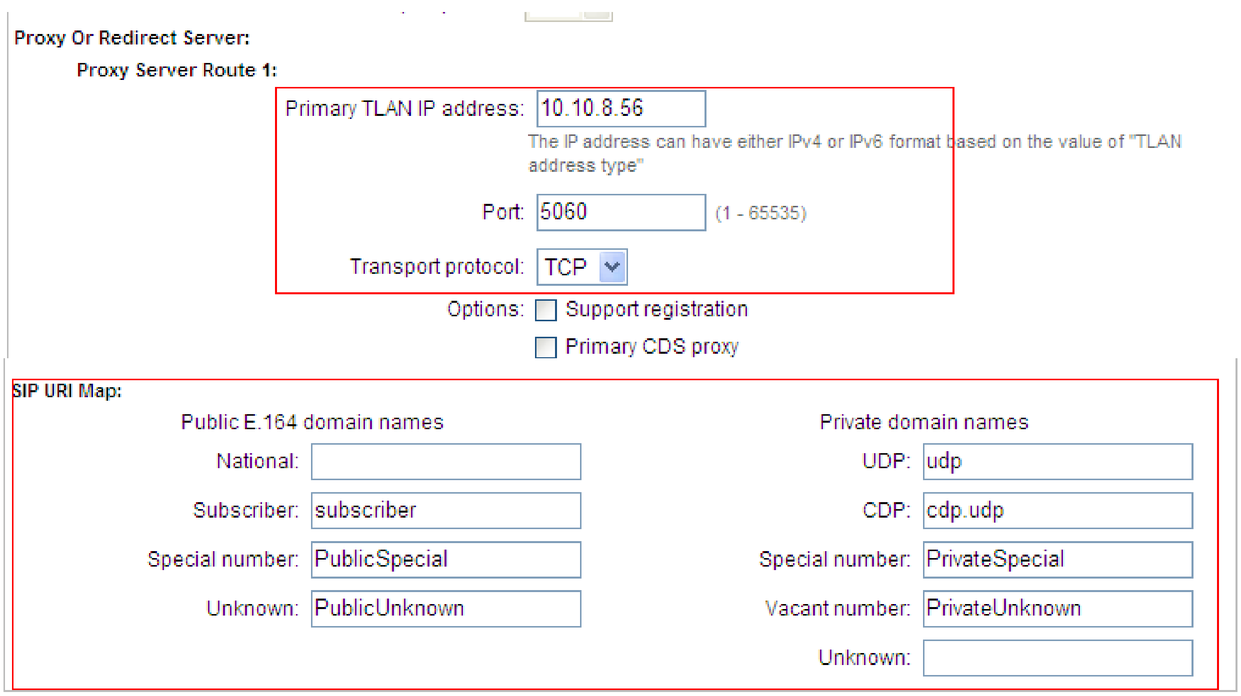


The next two screenshots show the SIP Virtual Trunk Gateway configuration. Navigate to **System → IP Network → IP Telephony Nodes → Node Details → Gateway (SIPGW) Virtual Trunk Configuration Details** and fill in the highlighted areas with the relevant settings.

- **Vtrk gateway application:** Provides option to select Gateway applications. The three supported modes are SIP Gateway (SIPGw), H. 323Gw, and SIPGw and H.323Gw
- **SIP domain name:** The SIP Domain Name is the SIP Service Domain. The SIP Domain Name configured in the Signaling Server properties must match the Service Domain name configured in 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.

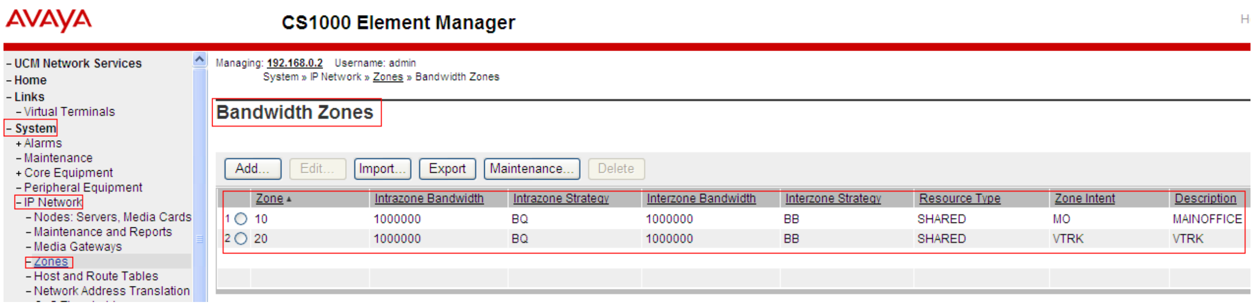
- **Application node id:** This is a unique value that can be alphanumeric and is for the new Node that is being created, in this case 5000
- **Proxy or Redirect Server:** Primary TLAN ip address is the SM100 ip address of the Session Manager. The transport protocol used for SIP, in this case is TCP
- **SIP URI Map:** National and Unknown have no values assigned.





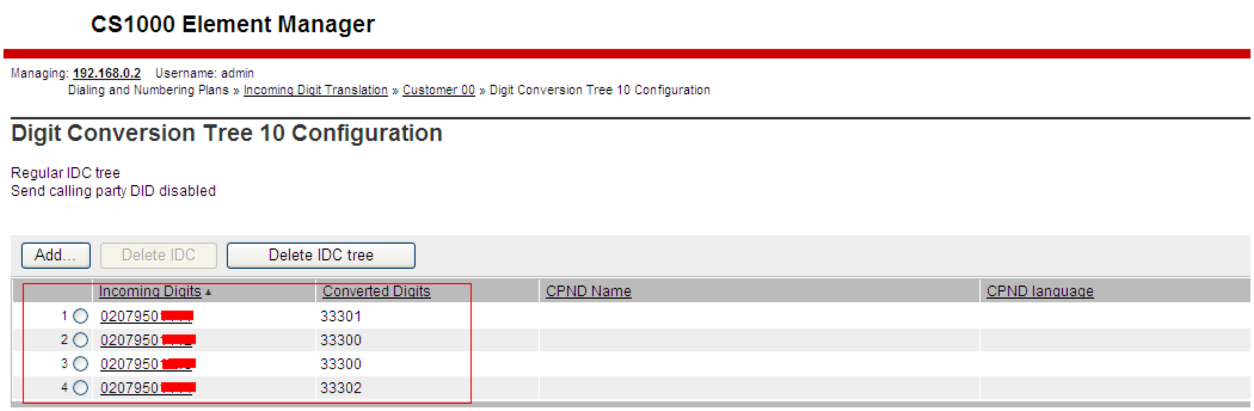
5.4. Configure Bandwidth Zones

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.



5.5. 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.



5.6. Configure SIP Trunks

Communication Server 1000E virtual trunks will be used for all inbound and outbound PSTN calls to the BT 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.

```
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 5000
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  YES
DCNO 10
NDNO 10 *
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 Route List Block (RLB) in overlay 86. Load overlay 86 at the system terminal and type **new**. The following example shows the values used. The value for **ROUT** is the same as previously entered in overlay 16. The **RLI** value is unique to each RLB.

```
Overlay 86
CUST 0
FEAT rlb
RLI  24
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  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 **RLI 24** SDRR NONE ITEI NONE	SPN 90 FLEN 7 ITOH NO CLTP NONE **RLI 24** SDRR NONE ITEI NONE	SPN 2 FLEN 7 ITOH NO CLTP NONE **RLI 24** SDRR NONE ITEI NONE	SPN 15 FLEN 3 ITOH NO CLTP NONE **RLI 24** SDRR NONE ITEI NONE

5.7. 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 RCBD
     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 OCBD 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 33300 0     MARP
        CPND
          CPND_LANG ROMAN
            NAME IP1140
            XPLN 10
            DISPLAY_FMT FIRST,LAST
     01 MCR 33300 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 RCBD
     ICDA CDMA LLCN MCTD CLBD AUTU
     GPUD DPUD DNDA CFXA ARHD FITD CNTD CLTD ASCD
     CPFA CPTA ABDA CFHD FICD NAID BUZZ AGRD MOAD
     UDI RCC HBTD AHA IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
     DRDD EXR0
     USMD USRD ULAD 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 33301 0     MARP
        CPND
          CPND_LANG ROMAN
            NAME Digital Set
            XPLN 10
            DISPLAY_FMT FIRST,LAST
     01 MCR 33301 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   33302
AST  NO
IAPG 0
HUNT
TGAR 0
LDN  NO
NCOS 0
SGRP 0
RNPG 0
XLST
SCI  0
SCPW
SFLT NO
CAC_MFC 0
CLS  UNR DTN FBD XFD WTA THFD FND HTD ONS
     LPR XRD AGRD CWD SWD MWD RMMD SMWD LPD XHD SLKD CCSD LND TVD
     CFTD SFD MRD C6D CNID CLBD AUTU
     ICDD CDMD LLCN EHTD MCTD
     GPUD DPUD CFXD ARHD OVDD AGTD CLTD LDTD ASCD SDND
     MBXD CPFA CPTA UDI RCC HBTD IRGD  DDGA NAMA MIND
     NRWD NRCD NROD SPKD CRD PRSD MCRD
     EXR0 SHL SMSD ABDD CFHD DNDY DNO3
     CWND USMD USRD CCBD BNRD OCBD 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
```

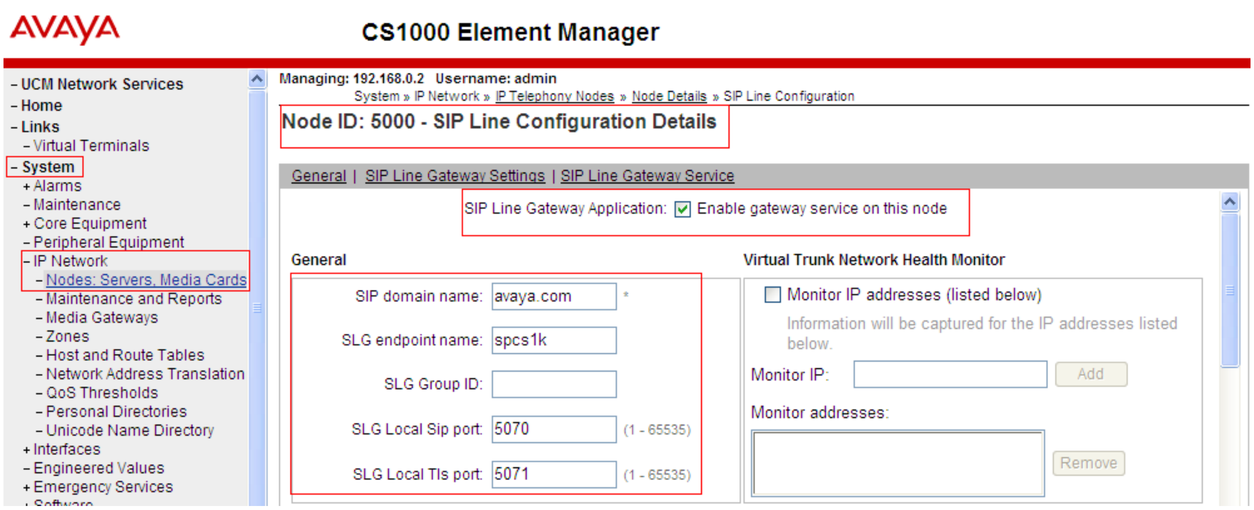
5.8. Configure the SIP Line Gateway Service

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 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.



5.9. Configure SIP Line Telephones

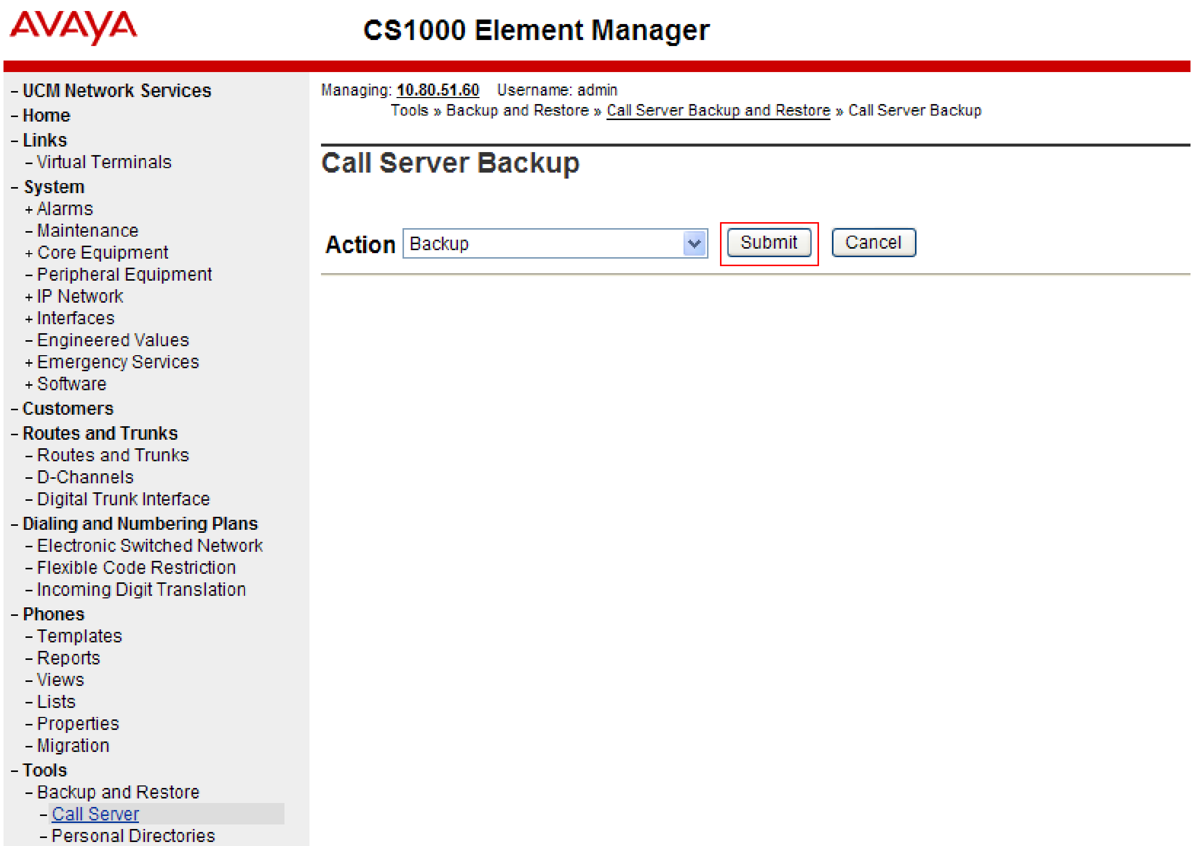
When SIP Line service configuration is completed, use the Communication Server 1000E system terminal and overlay 20 to add a Universal Extension (UEXT). See the following example of a SIP Line extension. The value for **UXTY** must be **SIPL**. This example is for an Avaya SIP telephone, so the value 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 **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 33003
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 33303
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 RCBD
     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---
```

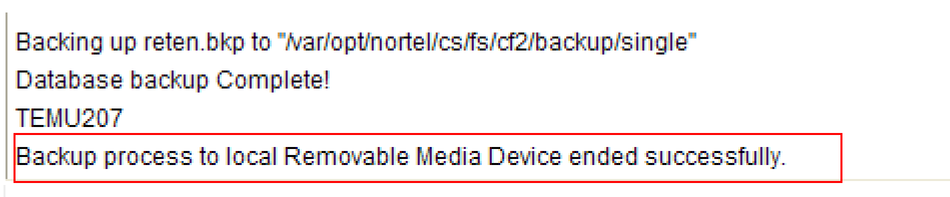
```
---continued from previous page---

     UDI RCC HBTD AHA IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
     DRDD EXR0
     USMD USRD ULAD CCBD RTDD RBDD RBHD PGND OCBD 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 33303 0     MARP
        CPND
          CPND_LANG ROMAN
            NAME Sigma 1140
            XPLN 11
            DISPLAY_FMT FIRST,LAST*
     01 HOT U 7833303 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.



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.



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 Communication Server 1000E
- Configure the Adaptation Module designed for Communication Server 1000E R7.5
- Define SIP Entity corresponding to Avaya Communication Server 1000E and Avaya Aura® SBC
- Define an Entity Link describing the SIP trunks between the Communication Server 1000E and Session Manager and also between the Avaya Aura® SBC and Session Manager.
- Define Routing Policies, which control call routing between the SIP Entities.
- Define Dial Patterns, which govern to which SIP Entity a call is routed.

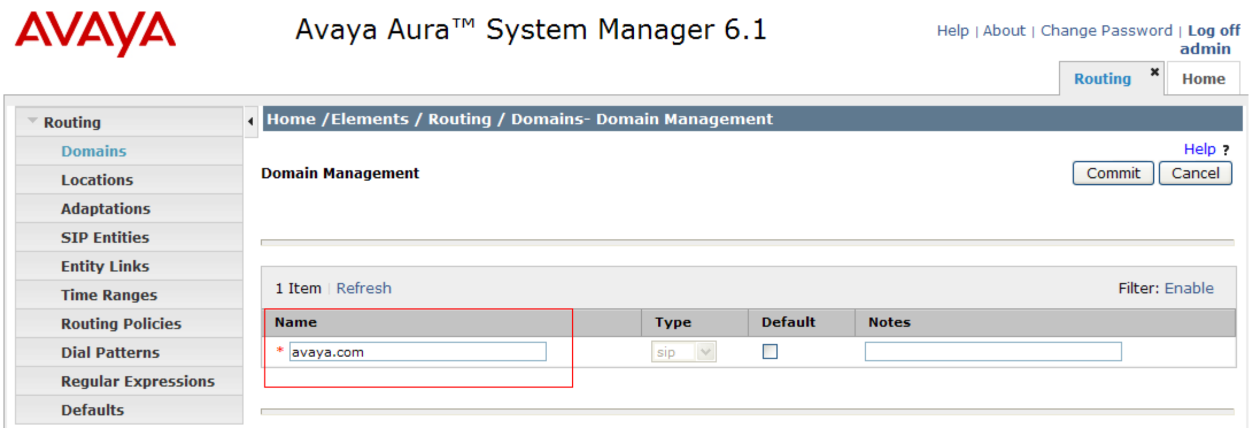
Configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL "**http://<ip-address>/SMGR**", where **<ip-address>** is the IP address of System Manager. Log in with the appropriate credentials. Some administration screens have been abbreviated for clarity.

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 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 / Domains- Domain Management
Help ?
Domain Management
Commit
Cancel
1 Item | Refresh
Filter: Enable
Name
Type
Default
Notes
* avaya.com
sip

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**.**

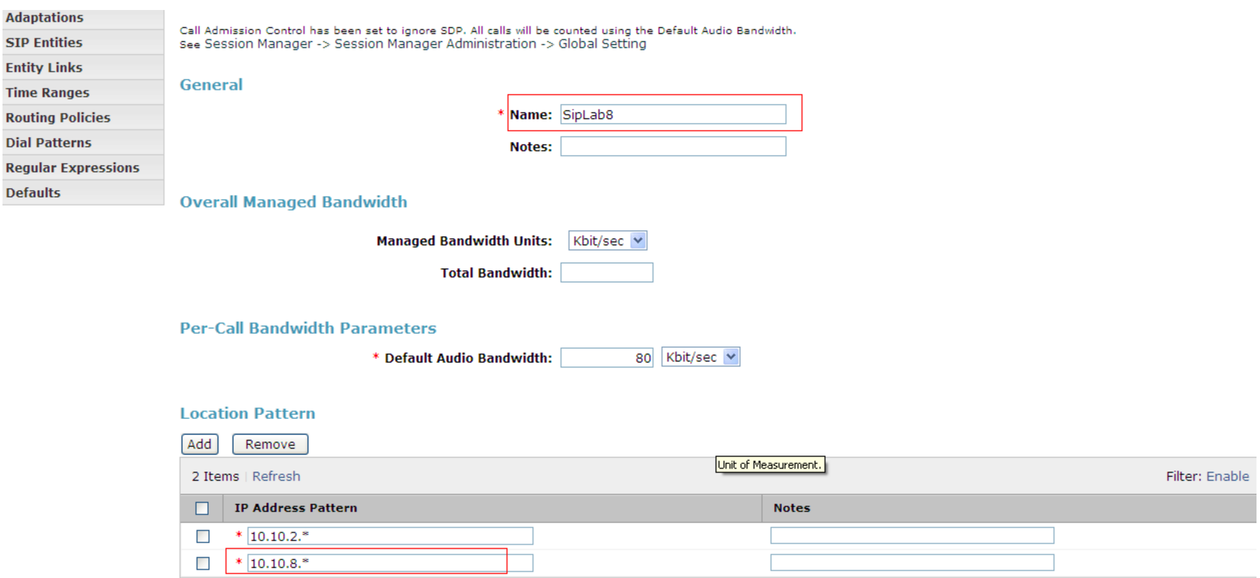
- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description. [Optional]

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.



6.3. Configure Adaptation Module

To enable calls between stations on Communication Server 1000E and SIP endpoints registered to the CS2K, Session Manager should be configured to use an Adaptation Module designed for Communication Server 1000E to convert SIP headers in messages sent by the CS2K and vice versa. Expand **Elements → Routing** and select **Adaptations** from the left navigational menu. Click **New (**not shown**).** In the **General** section, enter the following values and use default values for remaining fields**.**

- **Adaptation Name:** Enter an identifier for the Adaptation Module
- **Module Name:** Select **CS1000Adapter** from drop-down menu

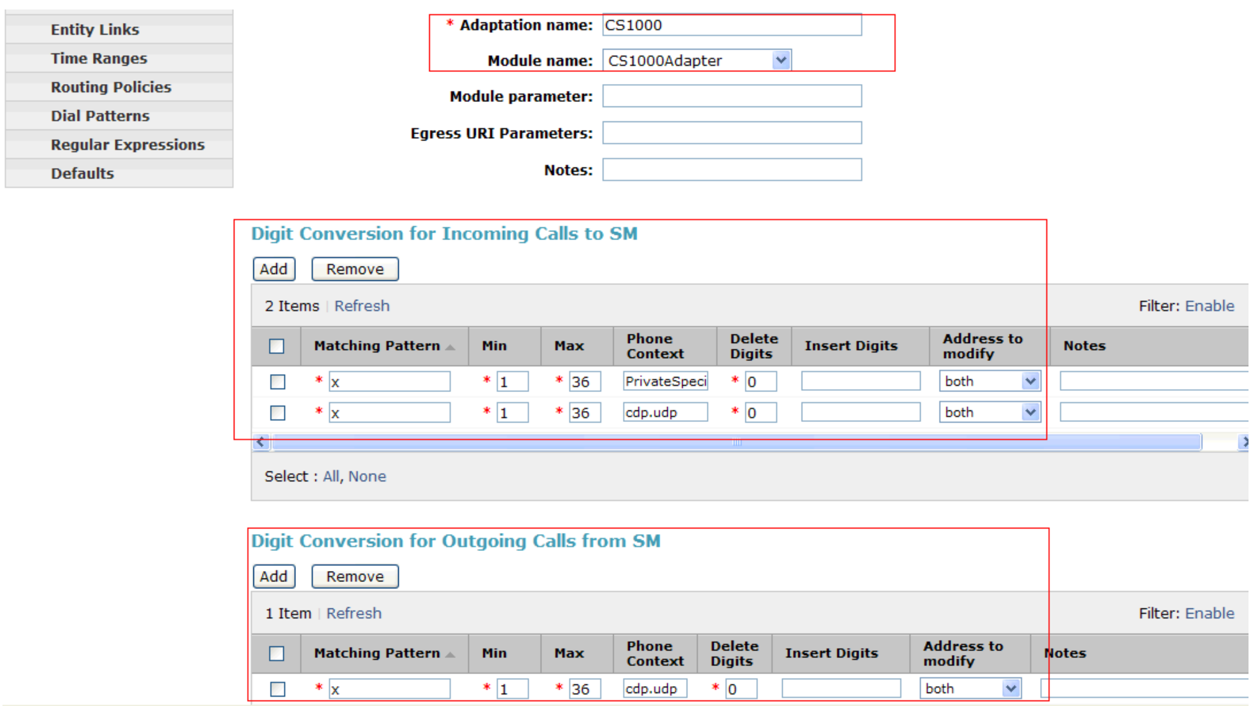
In the **Digit Conversion for Incoming Calls to SM** section, click **Add** and enter the following values.

- **Matching Pattern** Enter dialed prefix for calls to SIP endpoints registered to Session Manager. In the sample configuration, **X** was used, meaning everything
- **Min** Enter minimum number of digits that must be dialed
- **Max** Enter maximum number of digits that may be dialed. In the sample configuration 36 was used
- **Phone Context** Enter value of **Private CDP domain name** defined in section **5.3**
- **Delete Digits** Enter **0**, unless digits should be removed from dialed number before call is routed by Session Manager
- **Address to modify** Select **both**

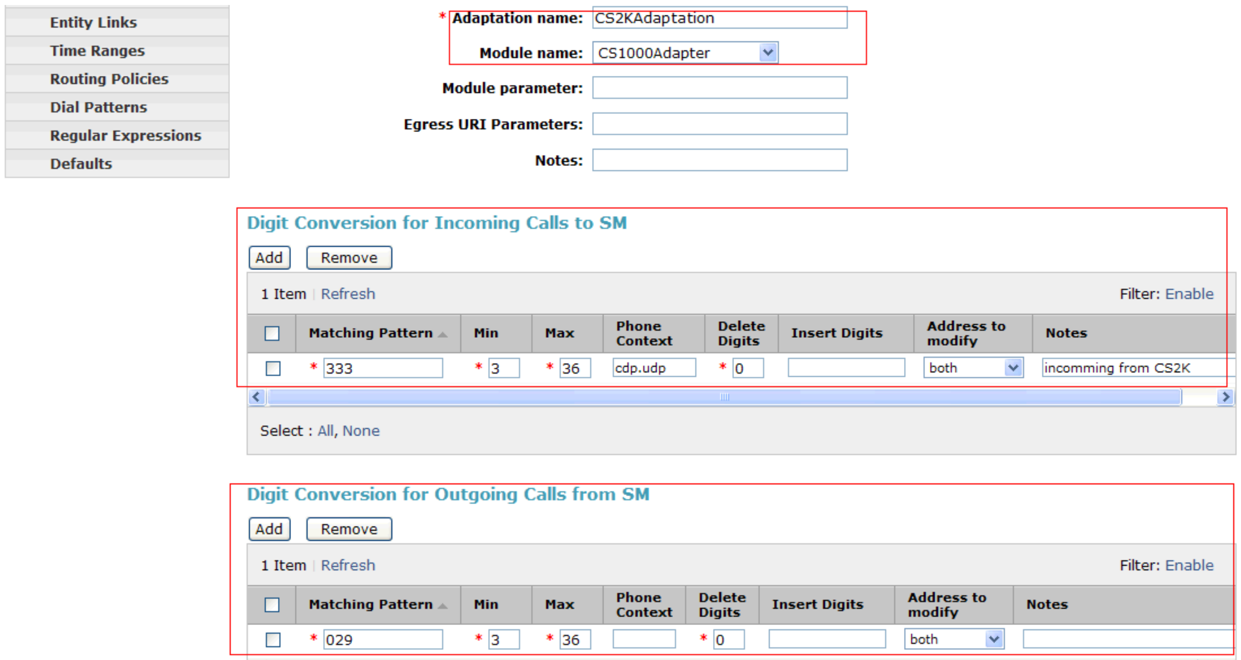
In the **Digit Conversion for Outgoing Calls to SM** section, click **Add** and enter the following values.

- **Matching Pattern** Enter dialed prefix for calls to SIP endpoints registered to Session Manager. In the sample configuration, **X** was used, meaning everything
- **Min** Enter minimum number of digits that must be dialed
- **Max** Enter maximum number of digits that may be dialed. In the sample configuration 36 was used
- **Phone Context** Enter value of **Private CDP domain name** defined in section **5.3**
- **Delete Digits** Enter **0**, unless digits should be removed from dialed number before call is routed by Session Manager
- **Address to modify** Select **both**

Click **Commit.** The Adaptation Module defined for sample configuration is shown below.



Below is the screenshot for the adaptation added for the CS2K. This adaptation will be assigned to the SBC SIP Entity.



6.4. Define SIP Entities

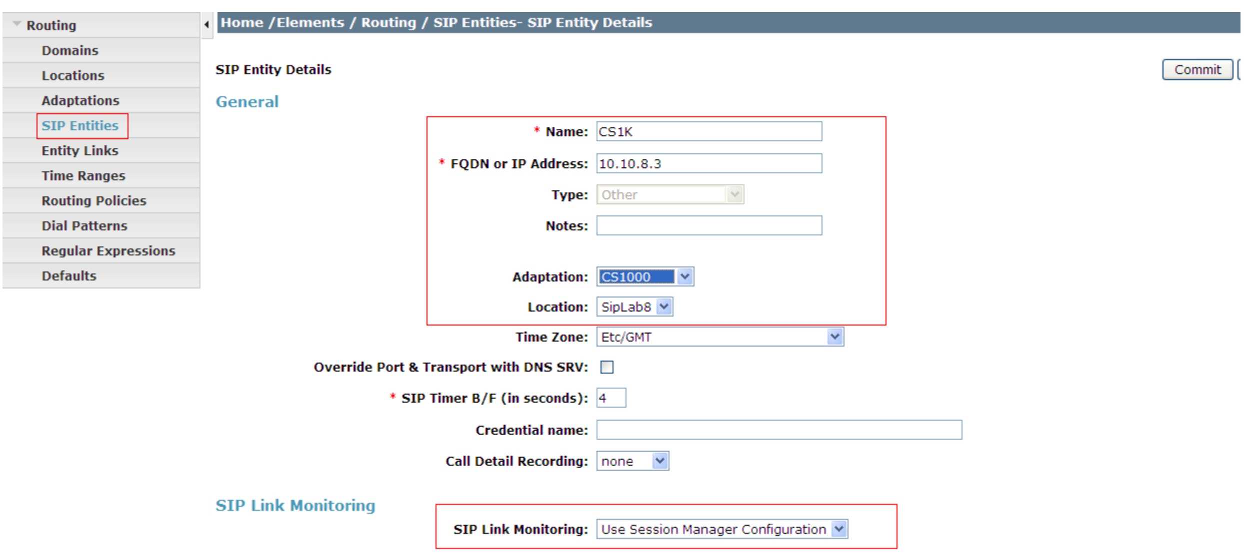
A SIP Entity must be added for Communication Server 1000E and also for the Avaya Aura® SBC. Expand **Elements → Routing** and select **SIP Entities** from the left navigation menu. Two new SIP Entities will need to be added as noted above. Click **New** (not shown). In the **General** section, enter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

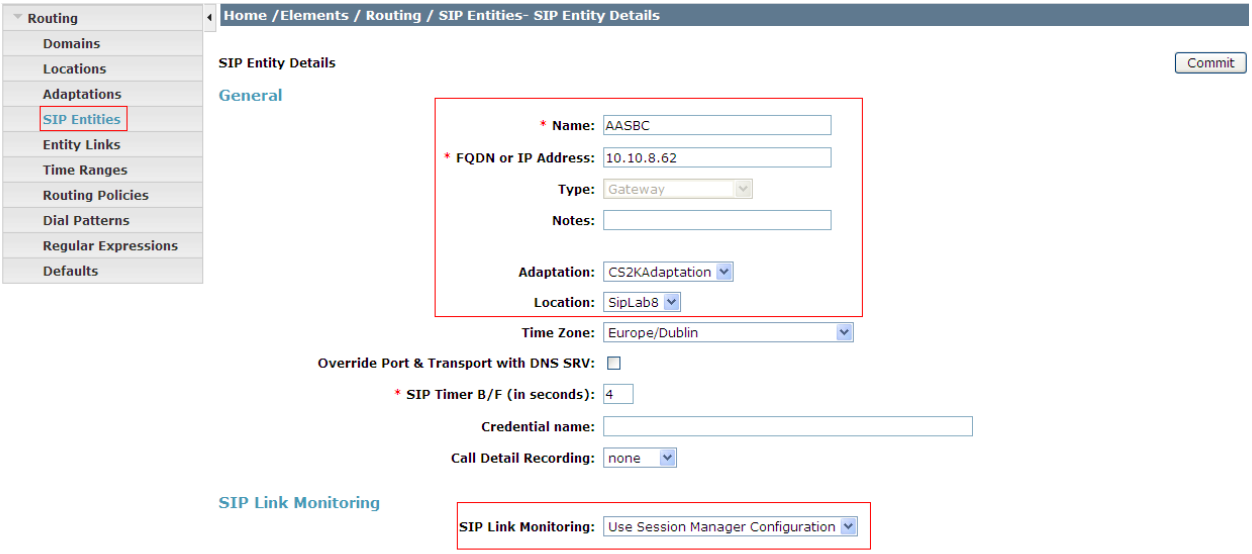
In the **SIP Link Monitoring** section:

- **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 following screenshot shows the SIP Entity defined for SBC in the sample configuration. Note that the **Adaptation** named “CS2KAdaptation” is used on this Entity link as shown below.



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
- **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 Avaya Communication Server 1000E.

Entity Links Commit Cancel

1 Item | Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* CS1K	* Session Manager	TCP	* 5060	* CS1K	* 5060	☑	toCS1K

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

Entity Links Commit Cancel

1 Item | Refresh Filter: Enable

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* toAASBC	* Session Manager	TCP	* 5060	* AASBC	* 5060	☑	toAASBC

6.6. Define Routing Policy

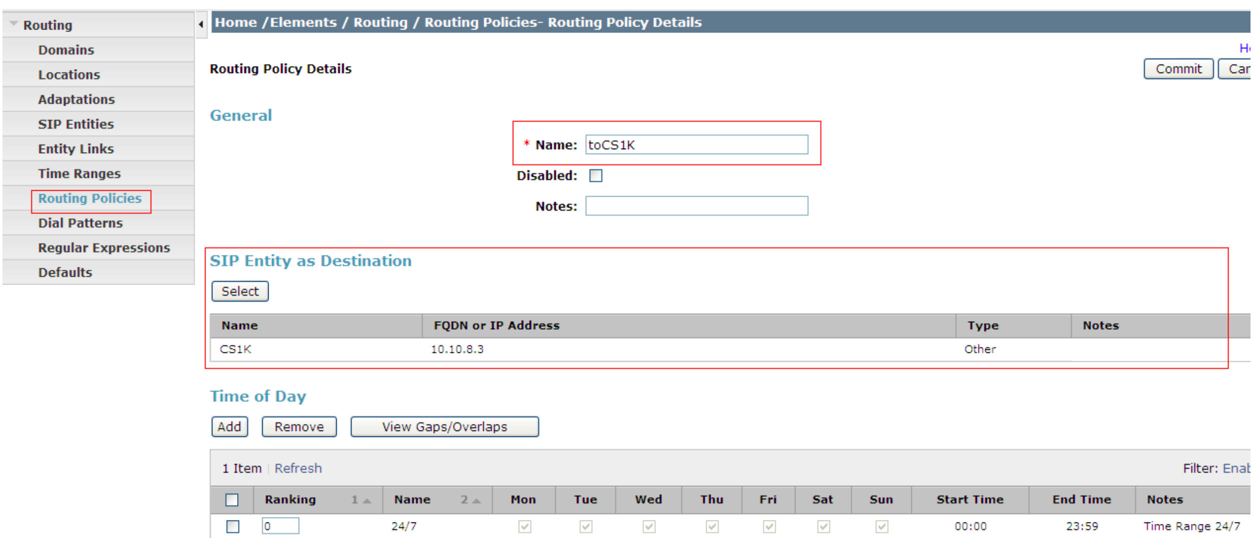
Routing policies describe the conditions under which calls will be routed to the CS1000E from either SIP endpoint registered to Session Manager or from other telephony system. It also describes the routing polices for which calls will be routed to the SBC and therefore to the Genband CS2K. To add a routing 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]

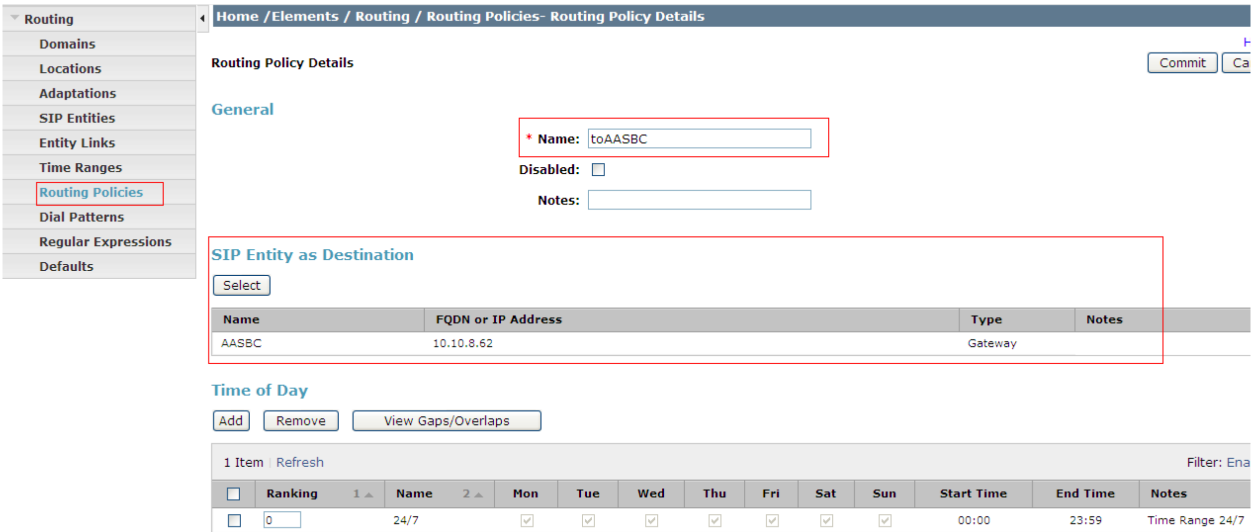
In the **SIP Entity as Destination** section, click **Select.** The **SIP Entity List** page opens (not shown). For routing policy to the Avaya Communication Server 1000E, select the SIP Entity associated with Communication Server 1000E defined in **Section 6.4** and click **Select.** The selected SIP 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 CS1000E:



For routing policy to the SBC – Genband CS2K, select the SIP Entity associated with the 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 the SBC – Genband CS2K:



6.7. Define Dial Pattern

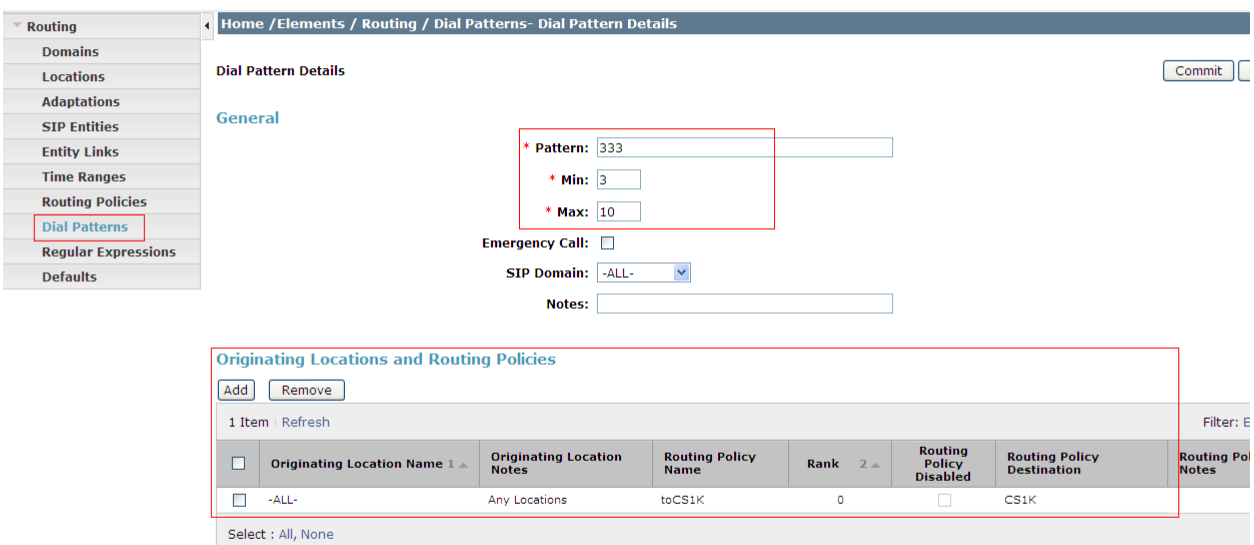
Dial patterns are used to route calls to appropriate SIP Entities. In the sample configuration, since stations on Communication Server 1000E were assigned extensions starting with **333**, calls starting with digits **333** will be routed to CS1000E. Alternately calls to the Genband CS2K start with digits **02920** so 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 to 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]

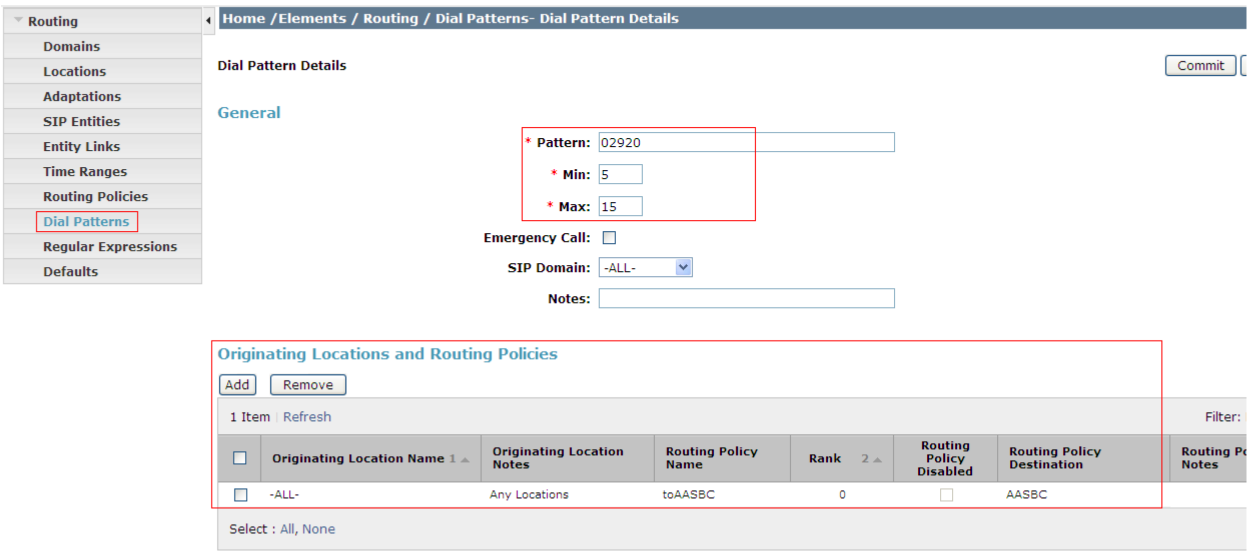
In the **Originating Locations and Routing Policies** section, click **Add.** The **Originating Locations and Routing Policy List** page opens (not shown).

- **Originating Locations** table Select **All**
- **Routing Policies** table 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 for CS 1000E:



Repeat the above steps to add the dial Pattern to the SBC, select the routing policy defined for the SBC in **Section 6.6**. The following screenshot shows the Routing Policy for SBC – Genband CS2K:



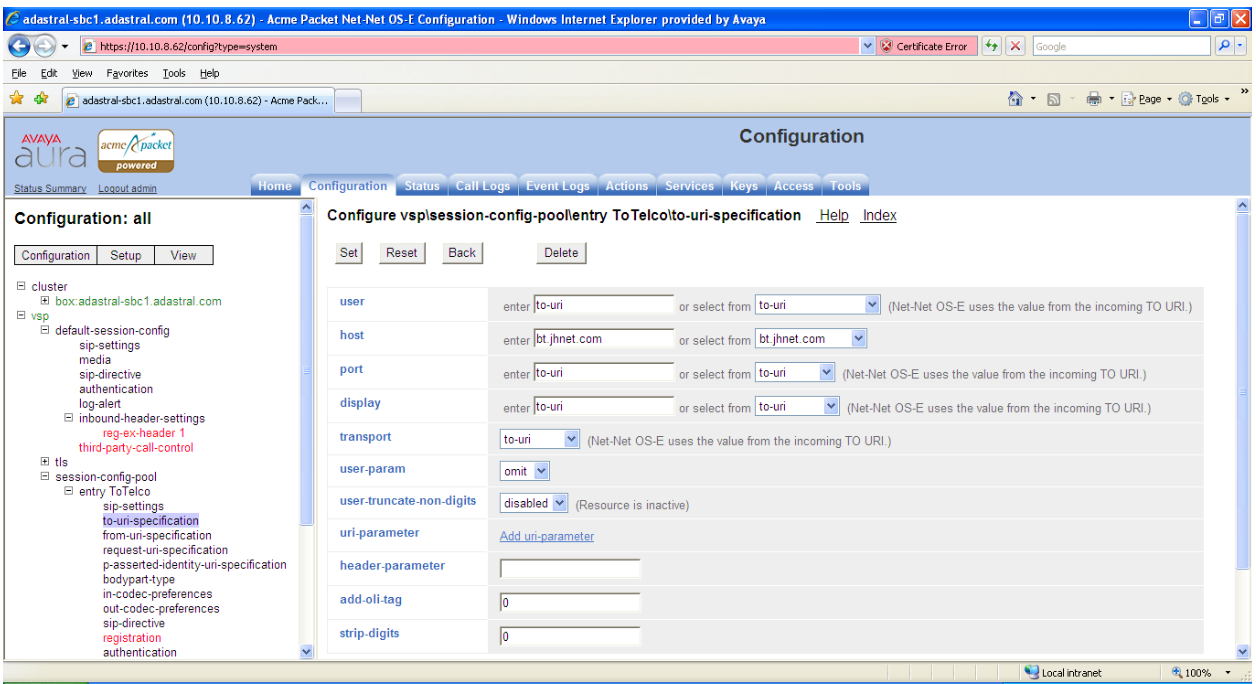
7. Configure Avaya Aura® Session Border Controller

This section provides the procedures for configuring the Avaya Aura® SBC to receive and route calls over the SIP trunk between the CS1000E and the Genband CS2K. 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 the CS2K. 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 IP addresses have been taken out for security purposes.

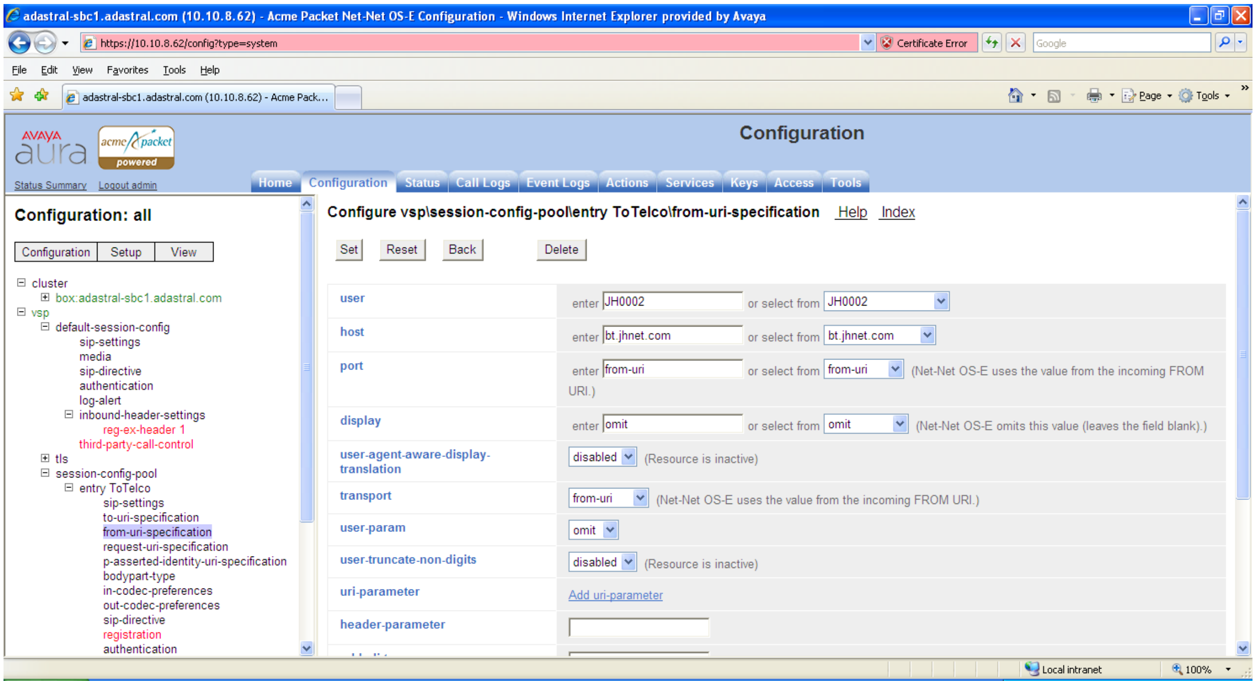
7.1. VSP configuration

7.1.1. Configure Session-Config-Pool Entry ToTelco

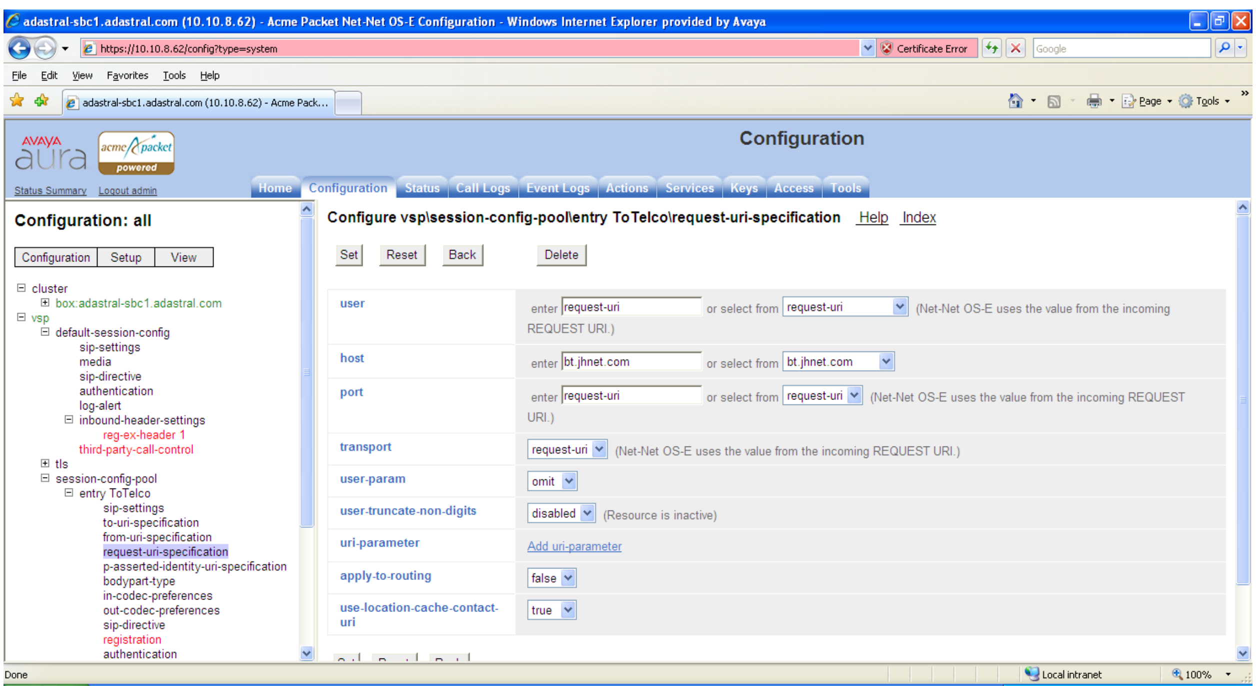
In the **to-uri-specification** a valid host was added, as shown below. Expand **vsp → session-config pool → entry ToTelco → to-uri-specification**.



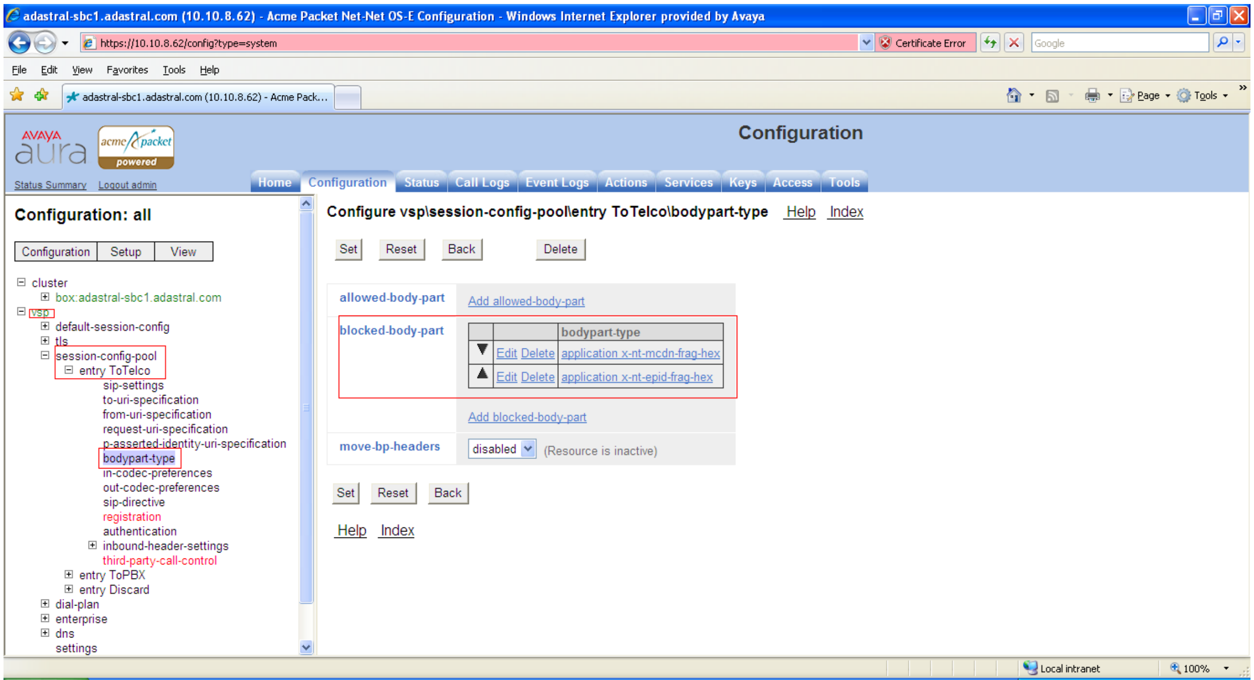
In the **from-uri-specification** a valid user was added, as shown below. Expand **vsp → session-config pool → entry ToTelco → from-uri-specification**.



In the **request-uri-specification** the same host that was added above needs to be added here. Expand **vsp → session-config pool → entry ToTelco → request-uri-specification**.

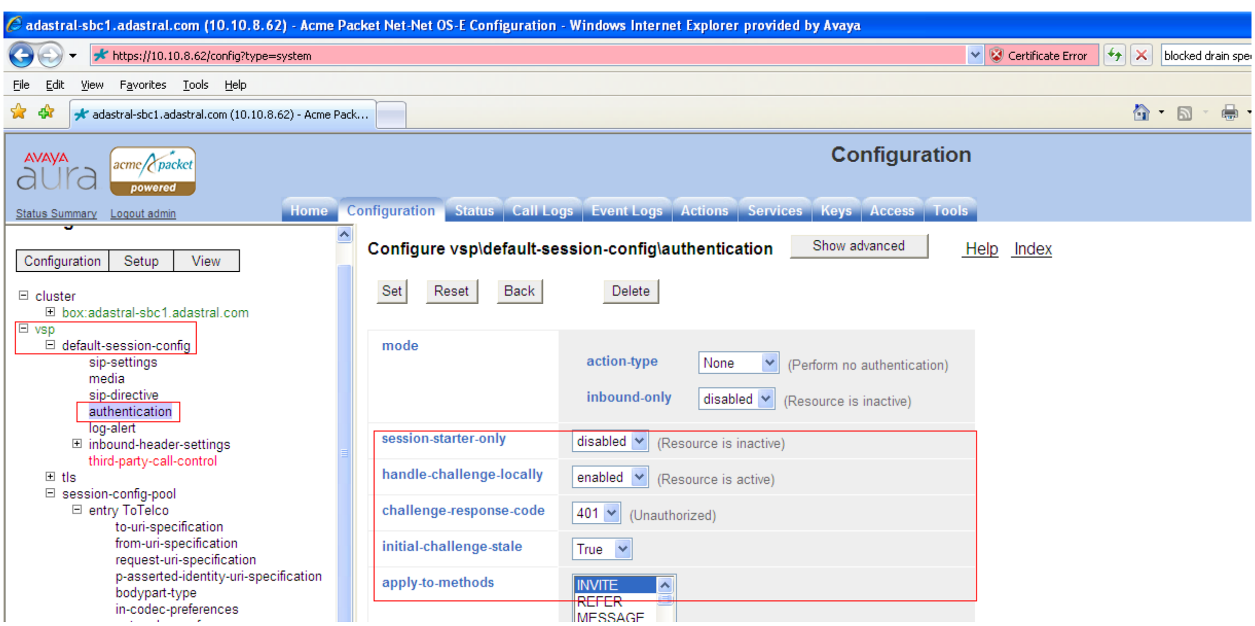


In **the session-config pool** two **blocked-body-parts** were added. Expand the **session-config pool → entry ToTelco →bodypart-type**. The following screenshot shows the two **blocked body-parts.**

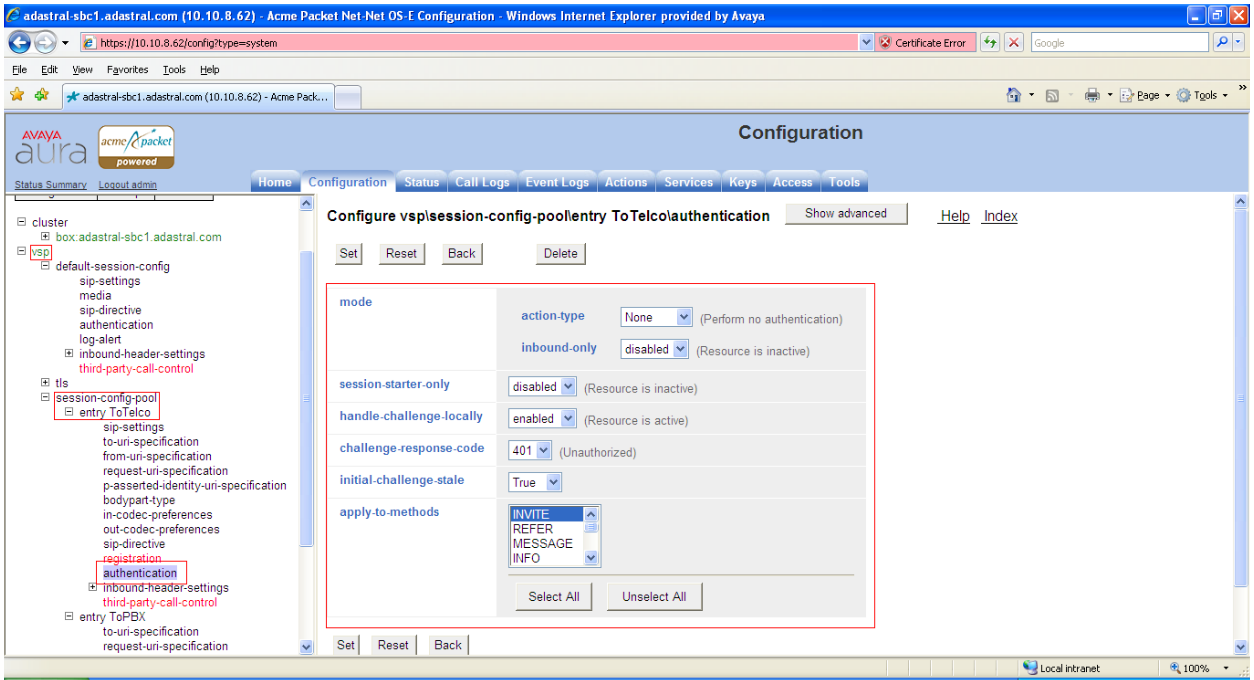


7.1.2. Authentication configuration

Authentication is enabled on an INVITE. Navigate to the **default-session confg → authentication.** Apply the authentication to the **INVITE** method as seen below:



Authentication is enabled on an INVITE in the **ToTelco** configuration. Expand the **session-config pool → entry to Telco** and select **authentication.** Apply the authentication to the INVITE method as seen below.



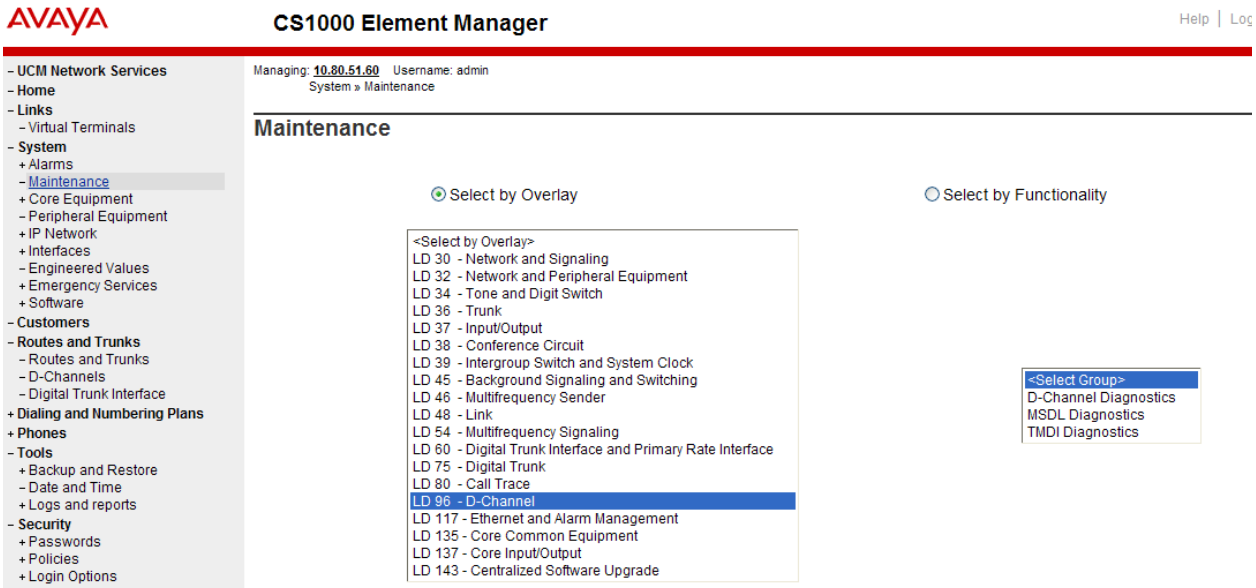
8. Service Provider Configuration

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

9. Verification

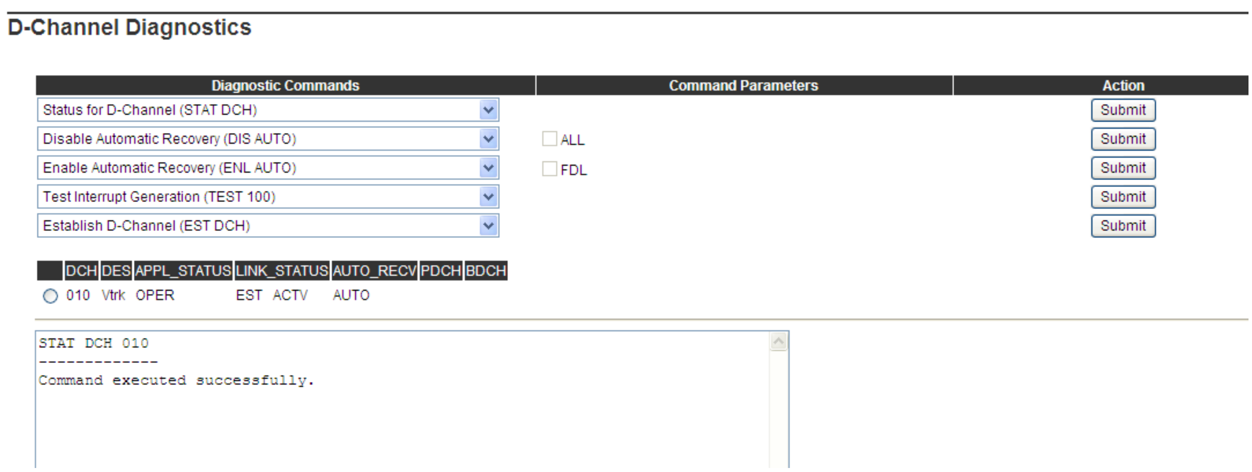
9.1. Verify Avaya Communication Server 1000E Operational Status

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.



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**

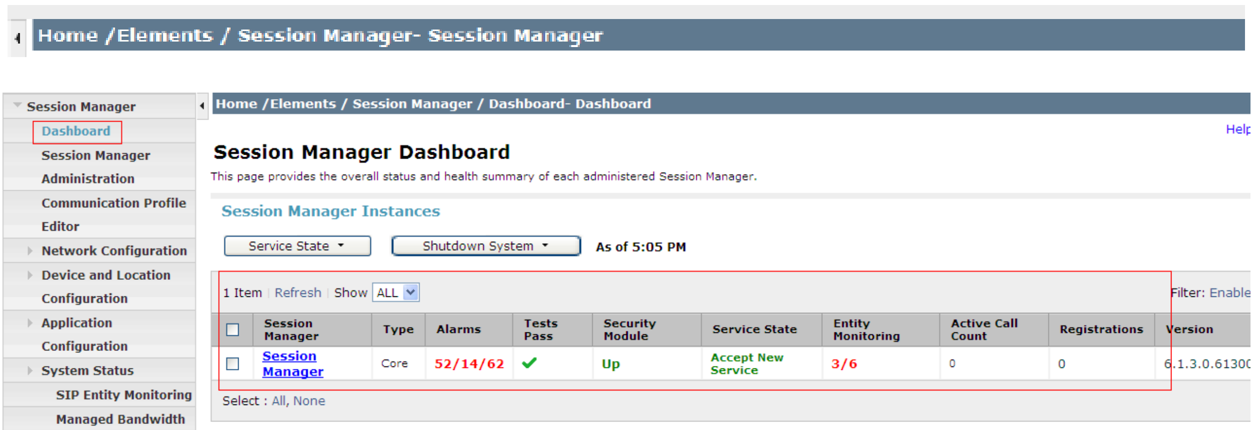


9.2. Verify Avaya Aura® Session Manager Operational Status

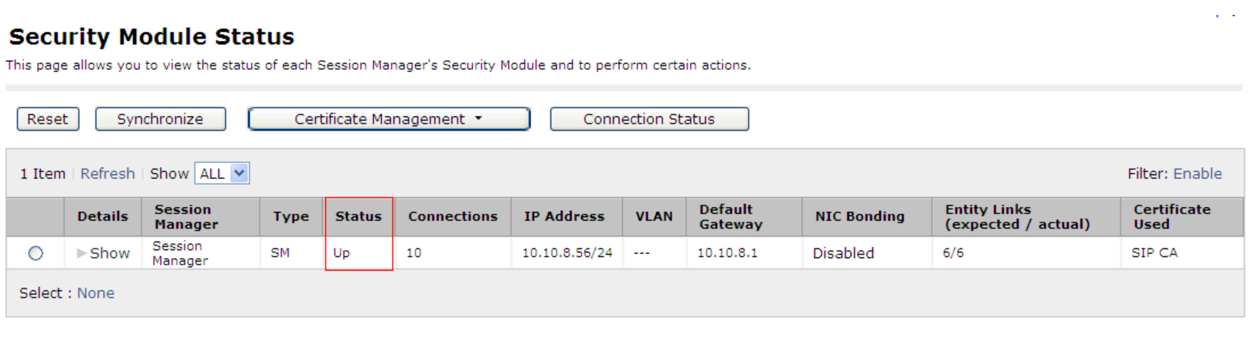
9.2.1. Verify Avaya Aura® Session Manager is Operational

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** Up
- **Service State** Accept New Service

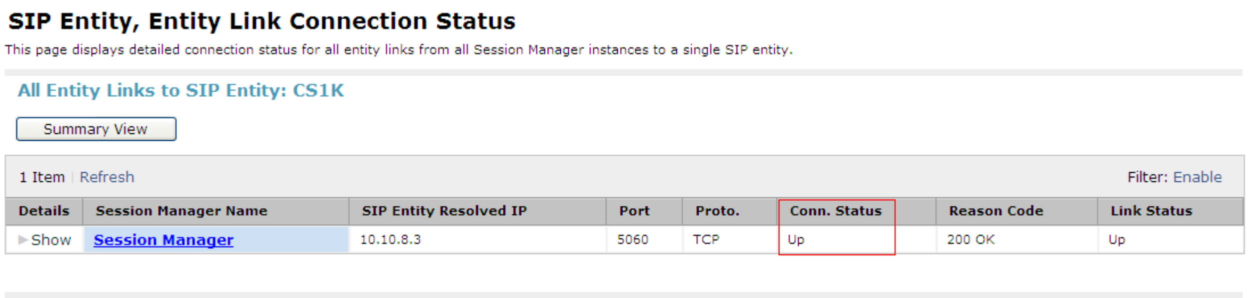


Navigate to **Elements → Session Manager → System Status → Security Module Status** (not shown) to view more detailed status information on the status of Security Module for the specific Session Manager. Verify the **Status** column displays **Up** as shown below.



9.3.1 Verify SIP Entity Link Status

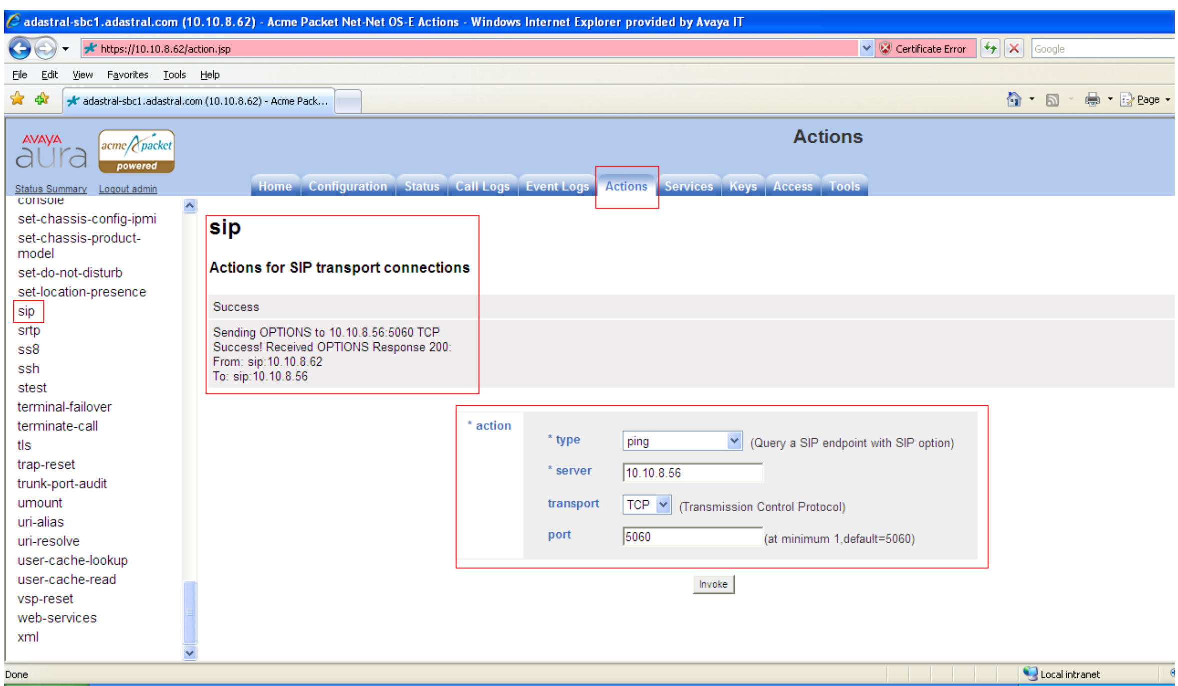
Navigate to **Elements → Session Manager → System Status → SIP Entity Monitoring** (not shown) to view more detailed status information for one of the SIP Entity Links. Select the SIP Entity for Communication Server 1000E from the **All Monitored SIP Entities** table (not shown) to open the **SIP Entity, 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.



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 BT's Genband CS2K using SIP Trunks. The CS2K Hosted Voice SIP Trunk Service is a SIP-based Voice over IP solution providing businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks.

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: 2011-05-05 13:27:07 (est))

IN-SERVICE PEPS
PAT# CR #          PATCH REF #     NAME      DATE        FILENAME       SPECINS
000  wi00842409    ISS1:1OF1       p30621_1  25/05/2011  p30621_1.cpl   NO
001  wi00835294    ISS1:1OF1       p30565_1  25/05/2011  p30565_1.cpl   NO
002  wi00841980    ISS1:1OF1       p30618_1  25/05/2011  p30618_1.cpl   NO
003  wi00852389    ISS1:1OF1       p30641_1  25/05/2011  p30641_1.cpl   NO
004  wi00832626    ISS2:1OF1       p30560_2  25/05/2011  p30560_2.cpl   NO
005  wi00836981    ISS1:1OF1       p30613_1  25/05/2011  p30613_1.cpl   NO
006  wi00837618    ISS1:1OF1       p30594_1  25/05/2011  p30594_1.cpl   NO
007  wi00839134    ISS1:1OF1       p30698_1  25/05/2011  p30698_1.cpl   YES
008  wi00832106    ISS1:1OF1       p30550_1  25/05/2011  p30550_1.cpl   NO
009  wi00837461    ISS1:1OF1       p30597_1  25/05/2011  p30597_1.cpl   NO
010  WI00843571    ISS1:1OF1       p30627_1  25/05/2011  p30627_1.cpl   NO
011  wi00843623    ISS1:1OF1       p30731_1  25/05/2011  p30731_1.cpl   YES
012  wi00852365    ISS1:1OF1       p30707_1  25/05/2011  p30707_1.cpl   NO
013  wi00860722    ISS1:1OF1       p30784_1  25/05/2011  p30784_1.cpl   YES
014  wi00856702    ISS1:1OF1       p30573_1  25/05/2011  p30573_1.cpl   NO
015  wi00871739    ISS1:1OF1       p30856_1  25/05/2011  p30856_1.cpl   NO
016  wi00857566    ISS1:1OF1       p30766_1  25/05/2011  p30766_1.cpl   NO
017  wi00850521    ISS1:1OF1       p30709_1  25/05/2011  p30709_1.cpl   YES
018  wi00688505    ISS1:1OF1       p30595_1  25/05/2011  p30595_1.cpl   NO
019  wi00839821    ISS1:1OF1       p30619_1  25/05/2011  p30619_1.cpl   NO
020  wi00839255    ISS1:1OF1       p30591_1  25/05/2011  p30591_1.cpl   NO
021  wi00838073    ISS1:1OF1       p30588_1  25/05/2011  p30588_1.cpl   NO
MDP>LAST SUCCESSFUL MDP REFRESH :2011-05-05 19:03:54(Local Time)
MDP>USING DEPLIST ZIP FILE DOWNLOADED :2011-05-05 13:58:27(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]
   ftrpkg                       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, the IP Addresses have been masked for security purposes.

```
#
#  Copyright (c) 2004-2011  Acme Packet Inc.
#  All Rights Reserved.
#
#  File: /cxc/cxc.cfg
#  Date: 16:41:14 Mon 2011-08-01
#
config cluster
 config box 1
  set hostname xxxxxxxx.com
  set timezone Europe/London
  set name xxxxxxxxx.com
  set identifier 00:ca:fe:27:16:64
  config interface eth0
   config ip inside
    set ip-address static xx.xx.xx.xx/27
    config ssh
    return
    config snmp
     set trap-target xx.xx.xx.xx
     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 xx.xx.xx.xx
     return
     config route Static0
      set destination network xx.xx.xx.xx/30
      set gateway xx.xx.xx.xx
     return
     config route Static1
      set admin disabled
     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/28
   config sip
    set udp-port 5060 "" "" any 0
   return
   config icmp
   return
   config media-ports
   return
   config routing
    config route external-sip-media-1
     set destination network xx.xx.xx.xx/24
     set gateway xx.xx.xx.xx
    return
    config route external-sip-media2
     set destination network xx.xx.xx.xx/24
     set gateway xx.xx.xx.xx
    return
    config route Default
     set admin disabled
    return
   return
   config kernel-filter
    config allow-rule allow-sip-udp-from-peer-1
     set destination-port 5060
     set source-address/mask xx.xx.xx.xx/24
     set protocol udp
    return
    config deny-rule deny-all-sip
     set destination-port 5060
    return
   return
  return
 return
 config cli
  set prompt xxxxxxxxx.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
 config collect
 return
return

config master-services
 config database
  set media enabled
 return
return

config vsp
 set admin enabled
 config default-session-config
  config sip-settings
   set strip-authint-qop enabled
  return
  config p-asserted-identity-uri-specification
   set display omit
  return
  config media
   set anchor auto
   config nat-traversal
    set symmetricRTP true
   return
   set rtp-stats enabled
  return
  config sip-directive
   set directive allow
  return
  config authentication
   set handle-challenge-locally enabled
  return
  config log-alert
  return
  config inbound-header-settings
   config reg-ex-header 1
    set admin disabled
    set destination Proxy-Authenticate
    set create Proxy-Authenticate ^(.*)qop="auth,auth-int"$ "\1qop=""auth"""
    set apply-to-responses yes 407
   return
  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 sip-settings
    set strip-authint-qop enabled
   return
   config to-uri-specification
    set host bt.jhnet.com
   return
   config from-uri-specification
    set user JH0002
    set host bt.jhnet.com
   return
   config request-uri-specification
    set host bt.jhnet.com
   return
   config p-asserted-identity-uri-specification
    set host local-ip
   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 in-codec-preferences
   return
   config out-codec-preferences
   return
   config sip-directive
    set directive allow
   return
   config registration
   return
   config authentication
    set handle-challenge-locally enabled
   return
   config inbound-header-settings
    config reg-ex-header 1
     set admin disabled
     set destination Proxy-Authenticate
     set create Proxy-Authenticate ^(.*)qop="auth,auth-int"$ "\1qop=""auth"""
     set apply-to-responses yes 407
    return
    config reg-ex-header 2
     set admin disabled
     set destination To
     set create To ^(.*);phone-context=.*@(.*)$ "\1@\2"
    return
   return
   config third-party-call-control
    set strip-require-100-rel enabled
   return
  return
  config entry ToPBX
   config to-uri-specification
    set host next-hop-domain
   return
   config request-uri-specification
    set host next-hop-domain
   return
   config header-settings
```

```
    config reg-ex-header 1
     set admin disabled
     set destination Request
     set create Request (.*);phone-context=local@(.*) "\1;phone-context=cdp.udp@\2"
     set apply-to-methods INVITE+ACK
    return
    config reg-ex-header 2
     set admin disabled
     set destination To
     set create To (.*);phone-context=local@(.*) "\1;phone-context=cdp.udp@\2"
     set apply-to-methods INVITE+ACK
    return
   return
   config third-party-call-control
   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 request-user strip-off 4
   set to-user strip-off 4
   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
  config source-route test
   set peer server "vsp\enterprise\servers\sip-gateway PBX"
   set source-match host 192.168.122.245
  return
 return
 config enterprise
  config servers
   config sip-gateway PBX
    set domain adastral.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 xx.xx.xx.xx
      set transport TCP
     return
    return
   return
   config sip-gateway Telco
    set domain bt.jhnet.com
    set failover-detection register
    set ping-interval 60
    set user JH0002
    set password-tag cs2kaccount
    set add-user-to-contact enabled
    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
   config sip-gateway testepc
```

```
    set domain xx.xx.xx.xx
    config server-pool
     config server testpc
      set host xx.xx.xx.xx
     return
    return
   return
  return
 return
 config dns
  config resolver
   config server xx.xx.xx.xx
   return
  return
 return
 config settings
  set read-header-max 8191
 return
 config codec-payload-type-bindings
  set binding any 5
  set binding g729 1
  set binding pcma 2
  set binding pcmu 3
  set binding t38 4
 return
return

config external-services
return

config preferences
 config gui-preferences
  set enum-strings DisplayURIStringSource TesteAPKT
  set enum-strings URIStringSource JH0002
  set enum-strings RequestURIStringSource bt.jhnet.com
  set enum-strings SIPSourceHeader proxy-authenticate
 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 0x000e10acb6d003fe3cc9f1371dc550e726ccbed02d76c054b1439aefa8
   set permissions access\permissions superuser
  return
  config user cust
   set password 0x002c493913eef4ce0dc26e6d6093cc65ada5922ed65d8152efce33fc94
   set permissions access\permissions read-only
  return
  config user init
   set password 0x002d65dec8ee9a07c37d33e3c47222d7c59791a2cb19d8b6c23f03d94a
   set permissions access\permissions superuser
  return
  config user craft
   set password 0x0037058cee27f2ee4c2029dd08b604223701437b1458504fcf3b39dc02
   set permissions access\permissions superuser
  return
  config user dadmin
   set password 0x00164fec25d9a9343a5f9c845355f29c97aa54bd1575af509786674523
   set permissions access\permissions read-only
  return
  config user BTPrime
   set password 0x002a553ec44709305d3c1046eed0210fafea21a4bd43de8b9a2741f52f
```

```
   set permissions access\permissions superuser
  return
 return
return

config features
return
```

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.