Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Communication Server 1000E R7.5, Avaya Aura® Session Manager R6.2, Avaya Session Border Controller for Enterprise R4.0.5 to support TDC Business Trunk - Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between TDC Business Trunk and an Avaya SIP enabled Enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager, Avaya Session Border Controller for Enterprise and Avaya Communication Server 1000E.

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

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between TDC Business Trunk and an Avaya SIP enabled Enterprise Solution. The Avaya solution consists of Avaya Aura® Session Manager, Avaya Communication Server 1000E (CS1000E) connected to TDC Business Trunk via an Avaya Session Border Controller for Enterprise (Avaya SBCE). Customers using this Avaya SIP-enabled Enterprise Solution with TDC Business Trunk 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 SBCE and Communication Server 1000E. The enterprise site was configured to use the SIP Trunk to TDC Business Trunk. This configuration (shown in Figure 1) was used to exercise the features and functionality listed in Section 2.1.

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

2.1. Interoperability Compliance Testing

The interoperability test included the following:

- Incoming PSTN calls were made to Unistim, SIP, Digital and Analog telephones and one-X® Communicator softphones at the enterprise
- Incoming calls to the enterprise site from the PSTN routed to the DDI numbers assigned by TDC
- Outgoing calls from the enterprise to the PSTN were made from Unistim, SIP, Digital and Analog telephones and one-X® Communicator softphones
- Outgoing calls from the enterprise site completed via TDC to PSTN destinations
- Calls using the G.711A, G.711MU and G.729A codecs supported by TDC (G.729A was never selected when G.711 was present in the SDP)
- Fax calls to/from a group 3 fax machine to a PSTN connected fax machine using the T.38 mode
- DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls
- 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

- Off-net call forwarding and mobility (extension to mobile)

2.2. Test Results

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

- No inbound toll free numbers were tested, however routing of inbound DID numbers and the relevant number translation was successfully tested.
- No Emergency Services numbers tested as test calls to these numbers should be pre-arranged with the Operator.
- SIP OPTIONS messages from the network contained a user in the URI which the Session Manager attempted to analyse. A “404 Not Found” message was returned.
- When an unassigned PSTN number was dialled, the network responded with a “500 Server Internal Error”. A more commonly used and informative response is “404 Not Found”.
- Codec Testing was limited as the network always selects G.711A/MU if available which is always the case on CS1000E.
- When testing blind call transfer to the PSTN, no ring-back was heard on the calling phone. Provisional reliable responses weren’t used on leg 2 of the call, in which case CS1000E does not send UPDATE messages. Without UPDATE, the backwards speech path is not established meaning the caller does not hear ring-back.
- One-X Communicator uses Payload Type 120 for DTMF and when this was sent in the re-INVITE when the call was put on hold, the network cleared the call. A script is required on the Avaya SBCE as a workaround.
- Calls to the mobile extension require two numbers in the To header, these are the Angöringsnummer (ANG) and the Calling Party Number. This could only be achieved with a script on the Avaya SBCE. For details of the mobile extension service, refer to the documentation for TDC Business Trunk

2.3. Support

For technical support on TDC products please contact the following website:
http://www.tdc.se

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an enterprise site connected to the TDC Business Trunk Service. Located at the enterprise site are Session Manager, Avaya SBCE and 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.

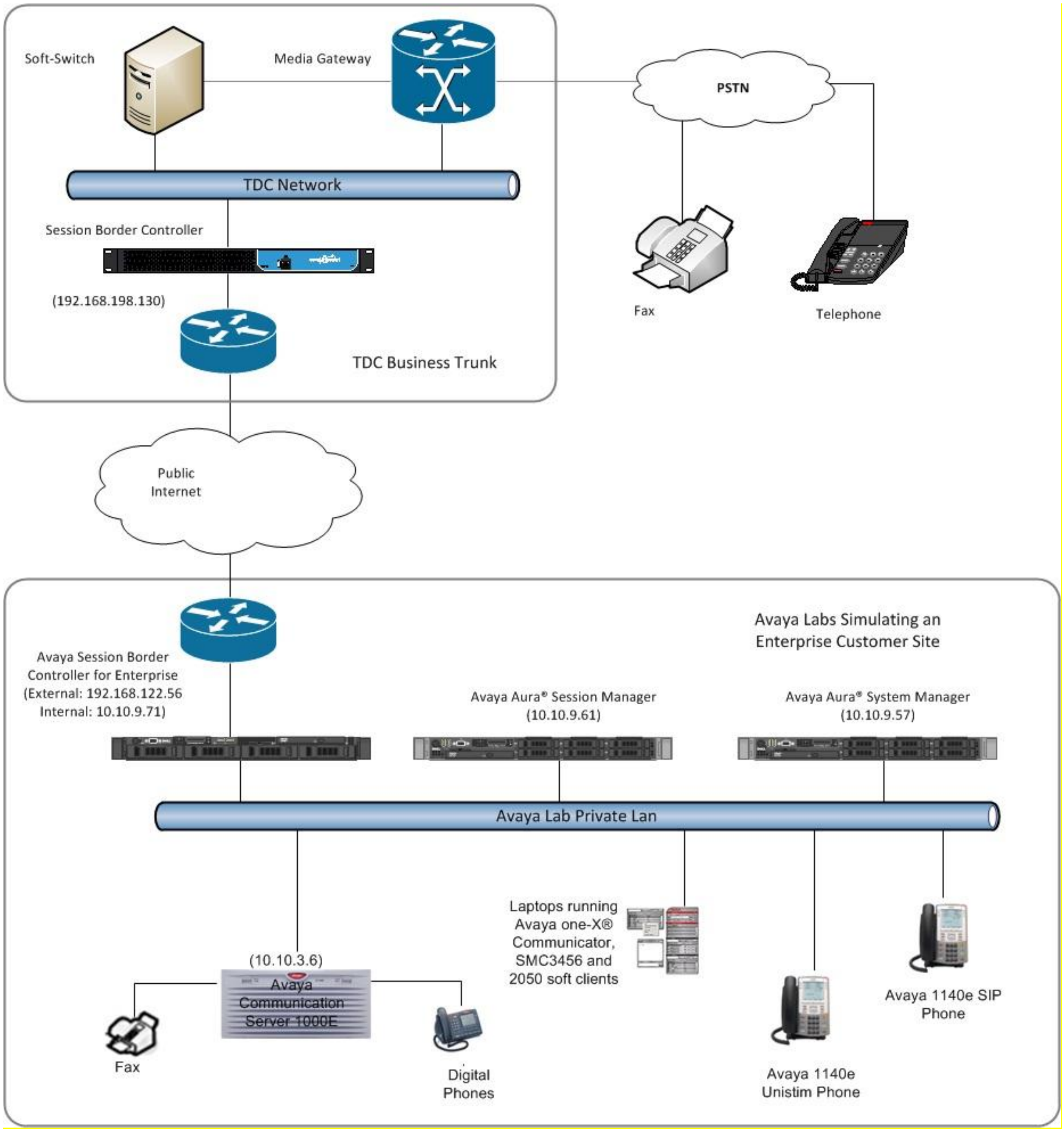


Figure 1: TDC SIP Trunk Topology

4. Equipment and Software Validated

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

Equipment/Software	Release/Version
Avaya	
Avaya Aura® Session Manager running on Avaya S8800 Server	R6.2 Build 6.2.0.0.620110
Avaya Aura® System Manager running on Avaya S8800 Server	R6.2 (System Platform 6.2.0.0.27, Template 6.2.12.0)
Avaya Communication Server 1000E running on CP+PM server as co-resident configuration	R7.5, Version 7.50.17 Service Update: 7.50_17Jan11 Deplist: X21 07.50Q
Avaya Session Border Controller for Enterprise on Dell R210 V2 server	Build: 4.0.5.Q09
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 AB03
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 53715
Avaya one-X® Communicator	Version cs6.1.0.10
Avaya Analogue Telephone	N/A
Avaya M3904 Digital Telephone	N/A
TDC	
Acme Packet SD3820	6.1
Ericsson IMS	11B
Broadsoft Broadworks	R17
Cisco PGW2200	9.8

5. Configure Avaya Aura® Communication Manager 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 Signalling associated with TDC Business Trunk. For incoming calls, the Session Manager receives SIP messages from the Avaya SBCE through which TDC's 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 signalling is routed to the Session Manager. The Session Manager directs the outbound SIP messages to the Avaya SBCE and on to TDC'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. Log in to the Avaya Communication Server 1000E

Log in using SSH to the ELAN IP address of the Call Server using a user with correct privileges. Once logged in type **csconsole**, 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 TDC's network, and any other SIP trunks needed. See the following screenshot for a typical System Limits printout. The value of **SIP ACCESS PORTS** defines the maximum number of SIP trunks for the Communication Server 1000E.

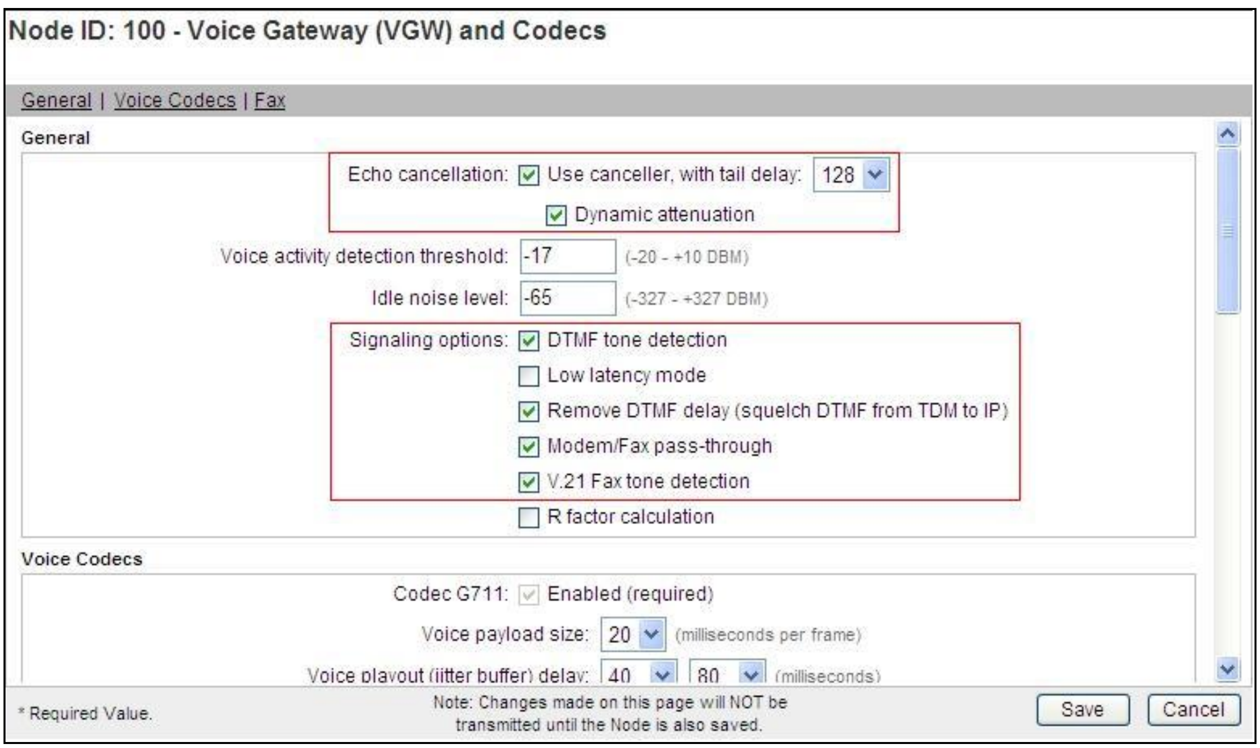
```
System type is - Communication Server 1000E/CPPM Linux
CPPM - Pentium M 1.4 GHz

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

TRADITIONAL TELEPHONES 32767    LEFT 32766    USED     1
DECT USERS             32767    LEFT 32767    USED     0
IP USERS               32767    LEFT 32744    USED    23
BASIC IP USERS         32767    LEFT 32766    USED     1
TEMPORARY IP USERS     32767    LEFT 32767    USED     0
DECT VISITOR USER      10000    LEFT 10000    USED     0
ACD AGENTS             32767    LEFT 32752    USED    15
MOBILE EXTENSIONS      32767    LEFT 32767    USED     0
TELEPHONY SERVICES     32767    LEFT 32767    USED     0
CONVERGED MOBILE USERS 32767    LEFT 32767    USED     0
NORTEL SIP LINES       32767    LEFT 32765    USED     2
THIRD PARTY SIP LINES  32767    LEFT 32761    USED     6
SIP CONVERGED DESKTOPS 32767    LEFT 32767    USED     0
SIP CTI TR87           32767    LEFT 32767    USED     0
SIP ACCESS PORTS        2000    LEFT 1970     USED    30
```

Load **overlay 21**, and confirm the Communication Server 1000E is setup to use **ISDN** trunks (see below).

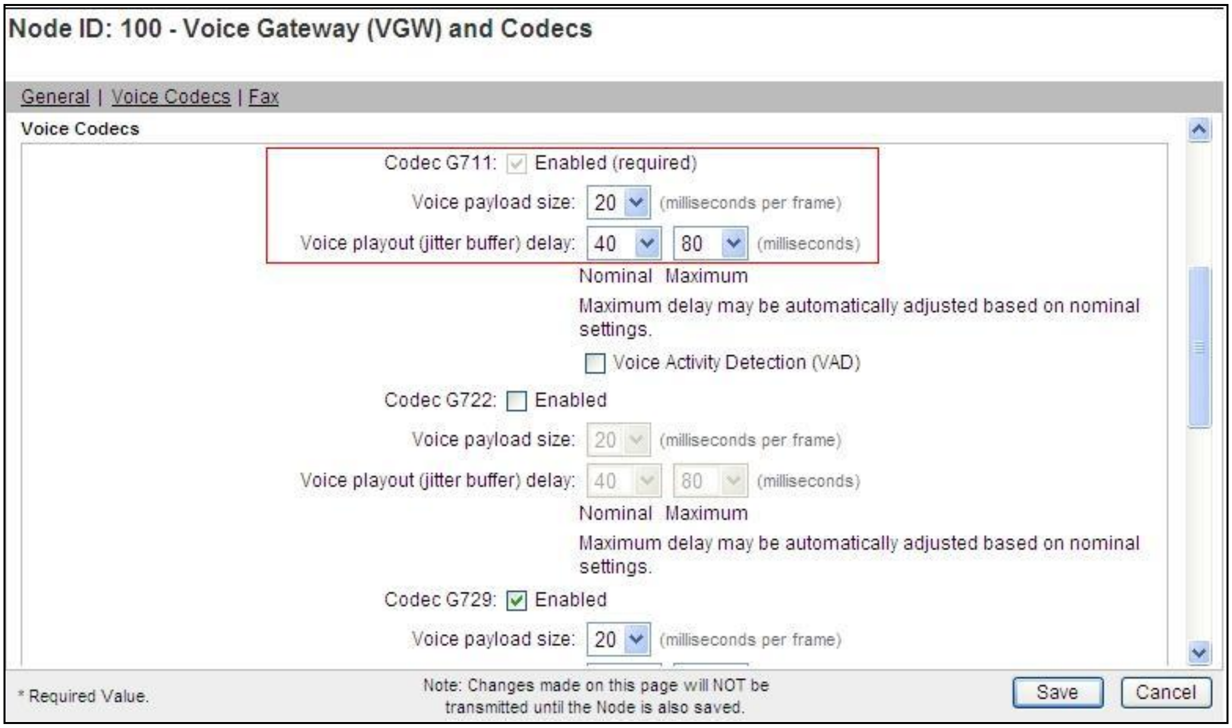
```
REQ: prt
TYPE: net
TYPE NET_DATA
CUST 0

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

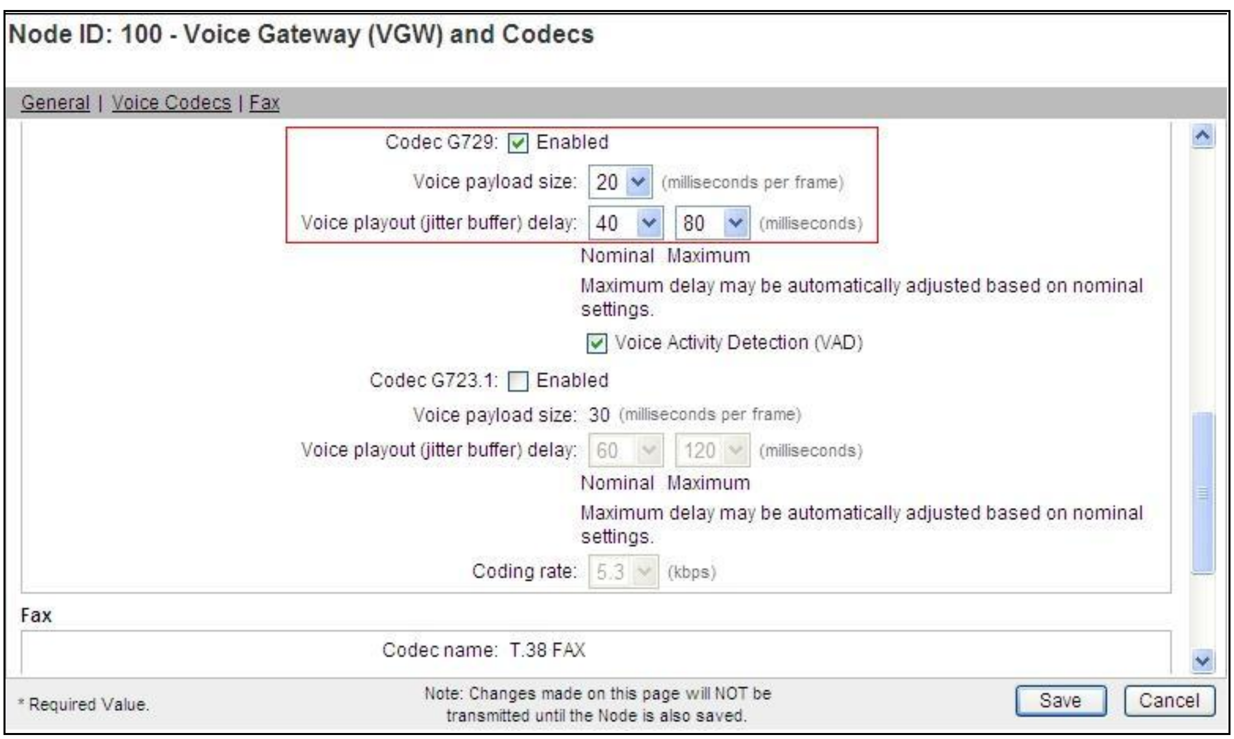
TDC's SIP Trunk service supports G.711A, G.711MU and G.729A voice codecs and T.38 FAX transmissions. Use the Communication Server 1000E element manager to configure the Voice and Fax properties. Navigate to the **IP Network → IP Telephony Nodes → Node Details → VGW Gateway (VGW) and Codecs** (not shown) property page and configure the Communication Server 1000E General codec settings as in the next screenshot.



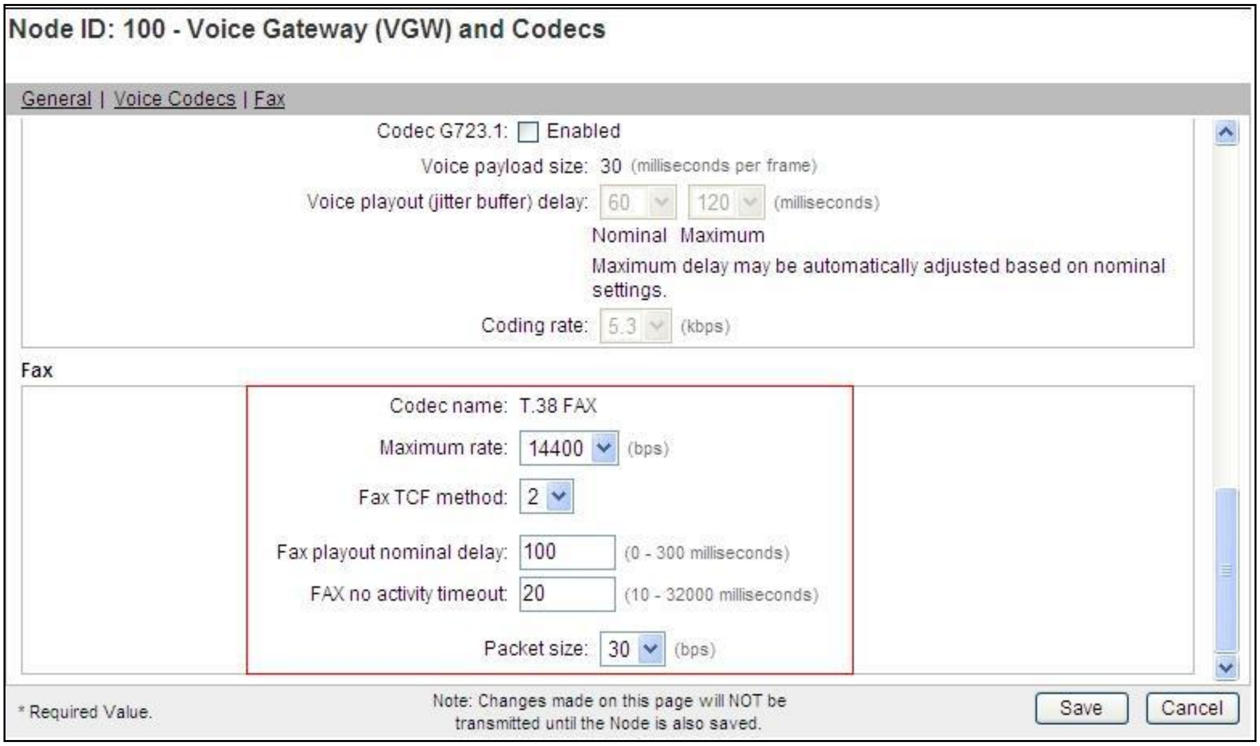
Next, scroll down and configure the **Codec G.711**. The relevant settings are highlighted in the following screenshot.



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

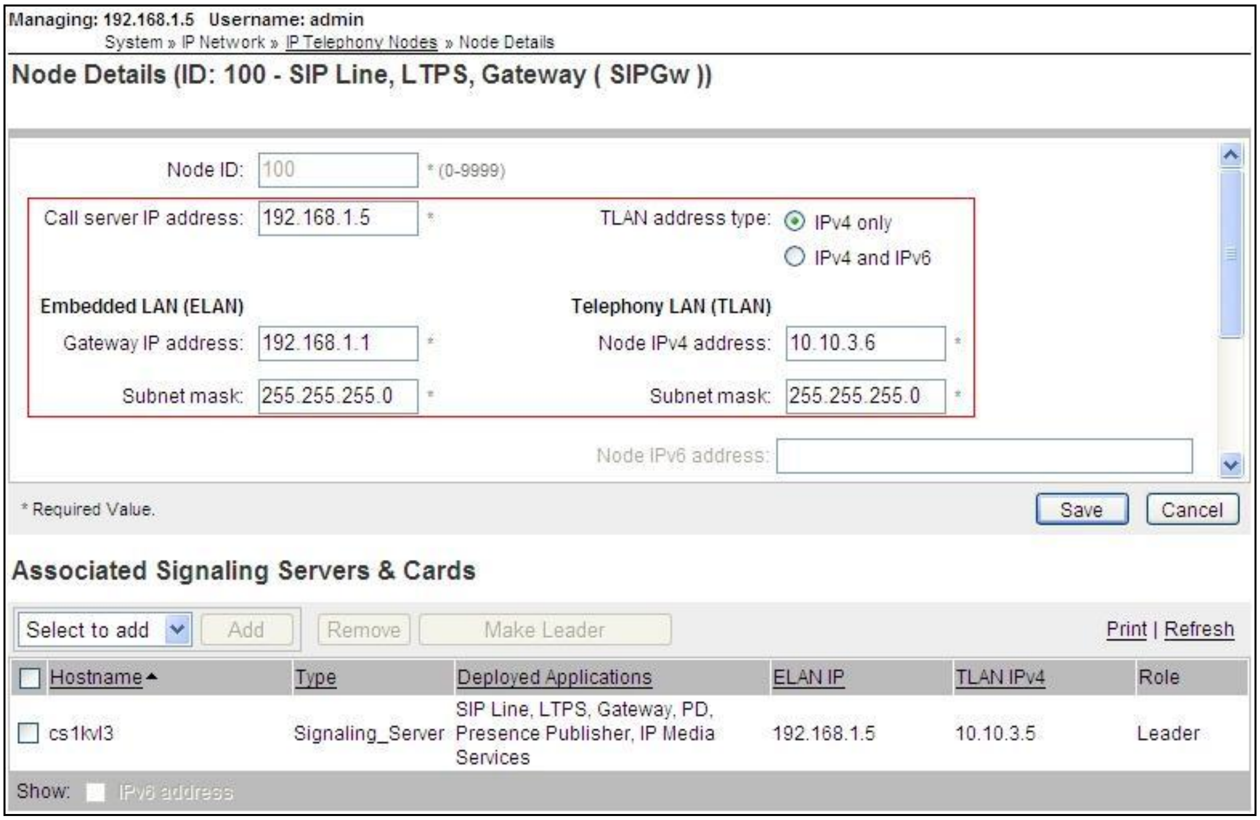


Finally, configure the **Fax** settings as in the highlighted section of the next screenshot.



5.4. Virtual Trunk Gateway Configuration

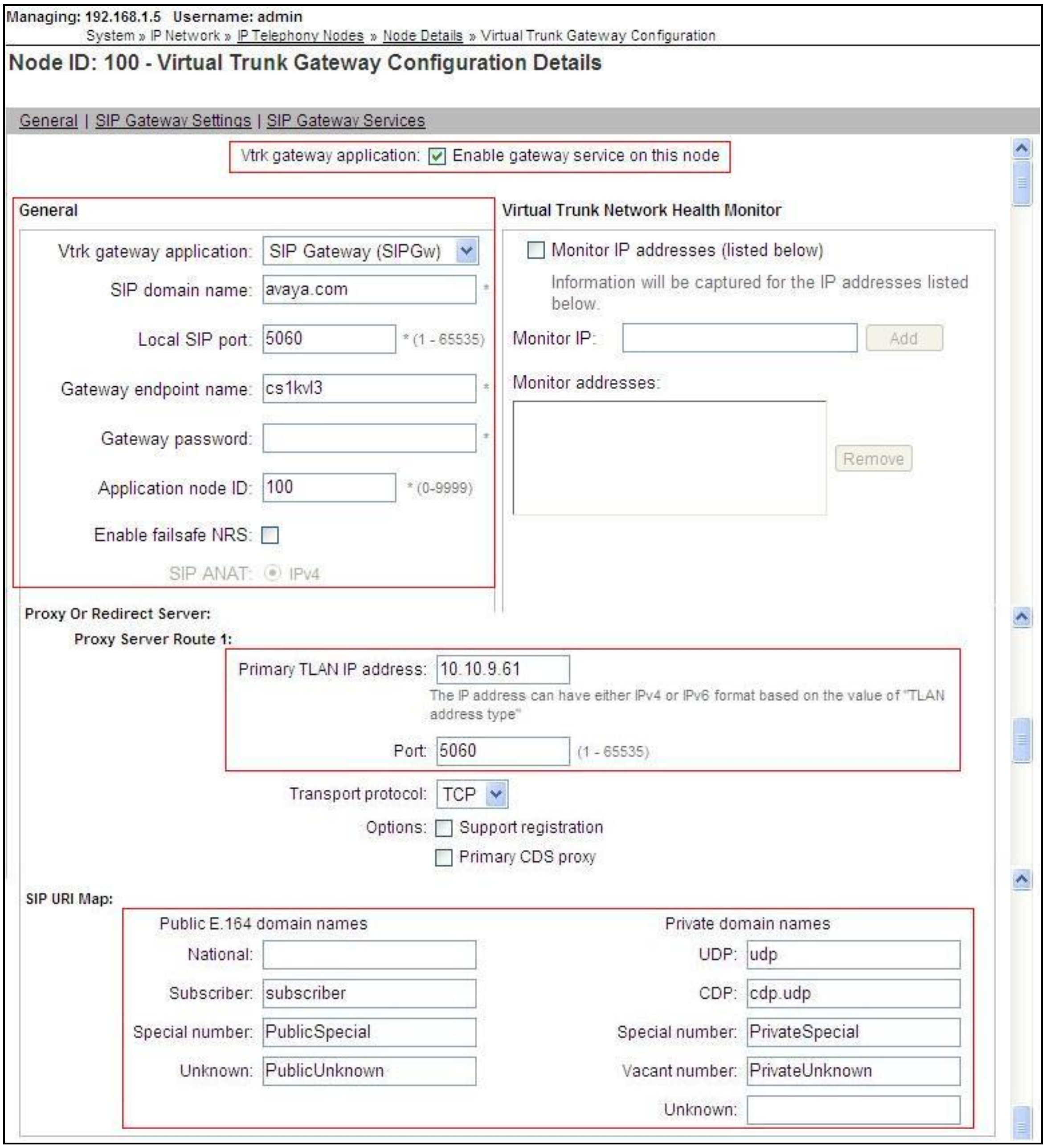
Use Communication Server 1000E Element Manager to configure the system node properties. Navigate to the **System → IP Networks → IP Telephony Nodes → Node Details** and verify the highlighted section is completed with the correct IP addresses and subnet masks of the Node. At this stage the call server 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 Communication Server 1000E, it is the Node IP that is used (please see **Section 6.5** – Define SIP Entities for more details).



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

- **Vtrk gateway application**: Provides option to select Gateway applications. The three supported modes are **SIP Gateway (SIPGw)**, **H.323Gw**, and **SIPGw and H.323Gw**. **SIPGw** was used in the test configuration
- **SIP domain name**: The SIP domain name configured in this section must match the SIP domain name configured in the Session Manager **Section 6.2**, in this case **avaya.com**
- **Local SIP port**: The Local SIP Port is the port to which the gateway listens. The default value is **5060**

- **Gateway endpoint name**: This field cannot be left blank so a value is needed here. This field is used when a Network Routing Server is used for registration of the endpoint. In this network a Session Manager is used so any value can be put in here and will not be used
- **Application node ID**: This is a unique value that can be alphanumeric and is for the new Node that is being created, in this case **100**
- **Proxy or Redirect Server**: Primary TLAN IP address is the Security Module 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



5.5. Configure Bandwidth Zones

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

5.6. Configure SIP Trunks

Communication Server 1000E virtual trunks will be used for all inbound and outbound PSTN calls to TDC's SIP Trunk Service. Six 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 Digit Manipulation Data Block (**DGT**); configure using the Communication Server 1000E system terminal and overlay 86
- Configure a Route List Block (**RLB**); configure using the Communication Server 1000E system terminal and overlay 86
- Configure Co-ordinated Dialling Plan(s) (**CDP**); configure using the Communication Server 1000E system terminal and overlay 87

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 1
  CTYP DCIP
  DES  VIR TRK
  USR  ISLD
  ISLM 4000
  SSRC 3700
  OTBF 32
  NASA YES
  IFC  SL1
  CNEG 1
  RLS  ID  4
  RCAP ND2
  MBGA NO
  H323
    OVLR NO
    OVLS NO
```

Next, configure the SIP trunk Route Data Block (**RDB**) using the Communication Server 1000E system terminal and overlay 16. Load **Overlay 16**, enter **RDB** at the prompt, press return and commence configuration. The value for **DCH** is the same as previously entered in overlay 17. The value for **NODE** should match the node value in **Section 5.4**. The value for **ZONE** should match that used in **Section 5.5** for **VTRK**. The remaining highlighted values are important for correct SIP trunk operation.

```
Overlay 16
TYPE: RDB
CUST 00
ROUT 1
TYPE RDB
CUST 00
ROUT 1
DES  VIR_TRK
TKTP TIE
NPID_TBL_NUM   0
ESN  NO
RPA  NO
CNVT NO
SAT  NO
RCLS EXT
VTRK YES
ZONE 00001
PCID SIP
CRID NO
NODE 100
DTRK NO
ISDN YES
    MODE ISLD
    DCH  1
    IFC  SL1
    PNI  00000
    NCNA YES
    NCRD YES
    TRO  NO
    FALT NO
    CTYP UKWN
    INAC NO
    ISAR NO
    DAPC NO
MBXR NO
MBXOT NPA
MBXT 0
PTYP ATT
CNDP UKWN
AUTO NO
DNIS NO
DCDR NO
ICOG IAO
SRCH LIN
TRMB YES
STEP
```

```
ACOD 1111
TCPP NO
PII NO
AUXP NO
TARG
CLEN 1
BILN NO
OABS
INST
IDC  YES
DCNO 0
NDNO 0 *
DEXT NO
DNAM NO
SIGO STD
STYP SDAT
MFC  NO
ICIS YES
OGIS YES
TIMR ICF  1920
     OGF  1920
     EOD  13952
     LCT  256
     DSI  34944
     NRD  10112
     DDL  70
     ODT  4096
     RGV  640
     GTO  896
     GTI  896
     SFB  3
     PRPS  800
     NBS  2048
     NBL  4096
     IENB  5
     TFD  0
     VSS  0
     VGD  6
     EESD  1024
SST  5 0
DTD  NO
SCDT NO
2 DT NO
NEDC ORG
FEDC ORG
```

```
CPDC NO
DLTN NO
HOLD 02 02 40
SEIZ 02 02
SVFL 02 02
DRNG NO
CDR  NO
NATL YES
SSL
CFWR NO
IDOP NO
VRAT NO
MUS  YES
MRT  21
PANS YES
RACD NO
MANO NO
FRL  0 0
FRL  1 0
FRL  2 0
FRL  3 0
FRL  4 0
FRL  5 0
FRL  6 0
FRL  7 0
OHQ  NO
OHQT 00
CBQ  NO
AUTH NO
TTBL 0
ATAN NO
OHTD NO
PLEV 2
OPR  NO
ALRM NO
ART  0
PECL NO
DCTI 0
TIDY 1600 100
ATRR NO
TRRL NO
SGRP 0
ARDN NO
CTBL 0
AACR NO
```

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

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

```
Overlay 86
CUST 0
FEAT dgt
DMI  10
DEL  0
ISPN NO
CTYP NPA
```

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

```
Overlay 86
CUST 0
FEAT rlb
RLI  10
ELC  NO
ENTR 0
LTER NO
ROUT 1
TOD  0 ON  1 ON  2 ON  3 ON
     4 ON  5 ON  6 ON  7 ON
VNS  NO
SCNV NO
CNV  NO
EXP  NO
FRL  0
DMI  10
CTBL 0
ISDM 0
FCI  0
FSNI 0
BNE  NO
DORG NO
SBOC NRR
PROU 1
IDBB DBD
IOHQ NO
OHQ  NO
CBQ  NO

ISET 0
NALT 5
MFRL 0
OVLL 0
```

Next, configure Co-ordinated Dialling Plan(s) (CDP) which users will dial to reach PSTN numbers. Use the Communication Server 1000E system terminal and **Overlay 87**. The following are some example CDP entries used. The highlighted **RLI** value previously configured in overlay 86 is used as the Route List Index (**RLI**); this is the default PSTN route to the SIP Trunk service.

TSC 00353 FLEN 0 RRPA NO **RLI 10** CCBA NO	TSC 18 FLEN 0 RRPA NO **RLI 10** CCBA NO	TSC 800 FLEN 0 RRPA NO **RLI 10** CCBA NO	TSC 08 FLEN 0 RRPA NO **RLI 10** CCBA NO

5.7. 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 5.5** for **MO**

Overlay 20 IP Telephone configuration

```
DES  1140
TN   100 0 01 0  VIRTUAL
TYPE 1140
CDEN 8D
CTYP XDLC
CUST 0
NUID
NHTN
CFG_ZONE 00002
CUR_ZONE 00002
ERL  0
ECL  0
FDN  0
TGAR 0
LDN  NO
NCOS 0
SGRP 0
RNPG 1
SCI  0
SSU
LNRS 16
XLST
SCPW
SFLT NO
CAC_MFC 0
CLS  UNR FBA WTA LPR PUA MTD FNA HTA TDD HFA CRPD
     MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
     POD SLKD 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
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
```

---continued on next page----

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

DGRP
MLWU_LANG 0
MLNG ENG
DNDR 0
KEY  00 MCR 5000 0     MARP
        CPND
          CPND_LANG ROMAN
            NAME IP1140
            XPLN 10
            DISPLAY_FMT FIRST,LAST
     01 MCR 5000 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   04 0 02 00  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 5008 0     MARP
        CPND
          CPND_LANG ROMAN
            NAME Digital Set
            XPLN 10
            DISPLAY FMT FIRST,LAST
     01 MCR 5008 0
        CPND
          CPND_LANG ROMAN
            NAME Digital Set
            XPLN 10
            DISPLAY_FMT FIRST,LAST
     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 CLT
     28 RLT
     29
     30
     31
```

Analogue telephones are also configured using **Overlay 20**, the following example shows an analog port configured for Plain Old 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   04 0 03 00
TYPE 500
CDEN 4D
CUST 0
MRT
ERL 00000
WRLS NO
DN   5015
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
```

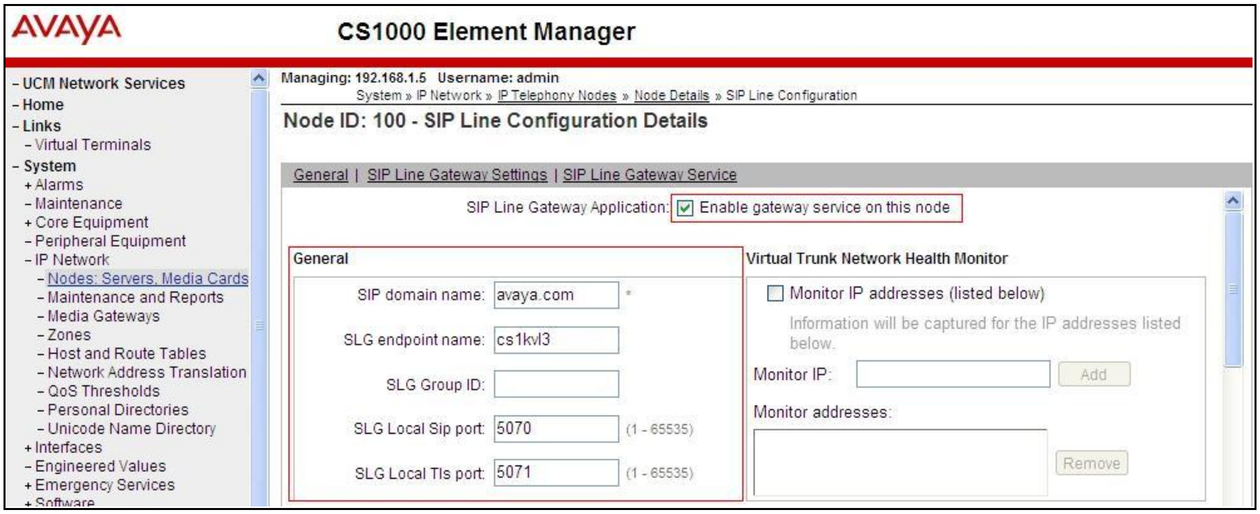
5.8. Configure the SIP Line Gateway Service

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 11
  NMME NO
```

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

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



5.9. Configure SIP Line Telephones

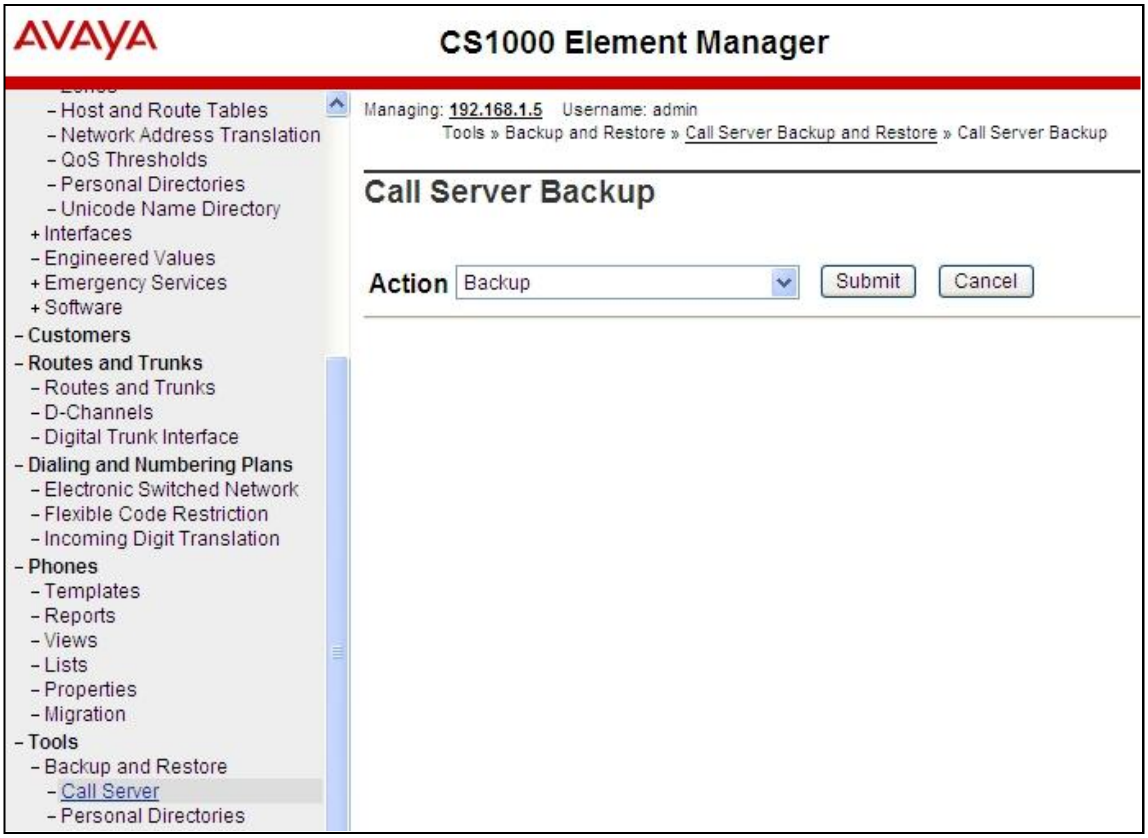
When SIP Line service configuration is completed, use the Communication Server 1000E system terminal and **Overlay 20** to add a Universal Extension (UEXT). See the following example of a SIP Line extension. The value for **UXTY** must be **SIPL**. This example is for an Avaya SIP telephone, so the value 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 **VTRK** in **Section 5.5**. A unique telephone number is entered for value **KEY 00**. The value for **KEY 01** is comprised of the **UAPR** value and the telephone number used in **KEY 00**.

```
Overlay 20 – SIP Telephone Configuration
DES  SIPD
TN   100 0 01 10  VIRTUAL
TYPE UEXT
CDEN 8D
CTYP XDLC
CUST 0
UXTY SIPL
MCCL YES
SIPN 1
SIP3 0
FMCL 0
TLSV 0
SIPU 5003
NDID 100
SUPR NO
SUBR DFLT MWI RGA CWI MSB
UXID
NUID 100
NHTN 100 0 01 10
CFG_ZONE 00002
CUR_ZONE 00002
ERL  0
ECL  0
VSIT NO
FDN
TGAR 0
LDN  NO
NCOS 0
SGRP 0
RNPG 0
SCI  0
SSU
XLST
SCPW 1234
SFLT NO
CAC_MFC 0
CLS  UNR FBD WTA LPR MTD FNA HTA TDD HFD CRPD
     MWD LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
     POD SLKD CCSD SWD LND CNDA
     CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED 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 SCR 5003 0     MARP
        CPND
          CPND_LANG ROMAN
            NAME Sigma 1140
            XPLN 11
            DISPLAY_FMT FIRST,LAST*
     01 HOT U 115003 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** 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.

Configuration of Communication Server 1000E is complete.

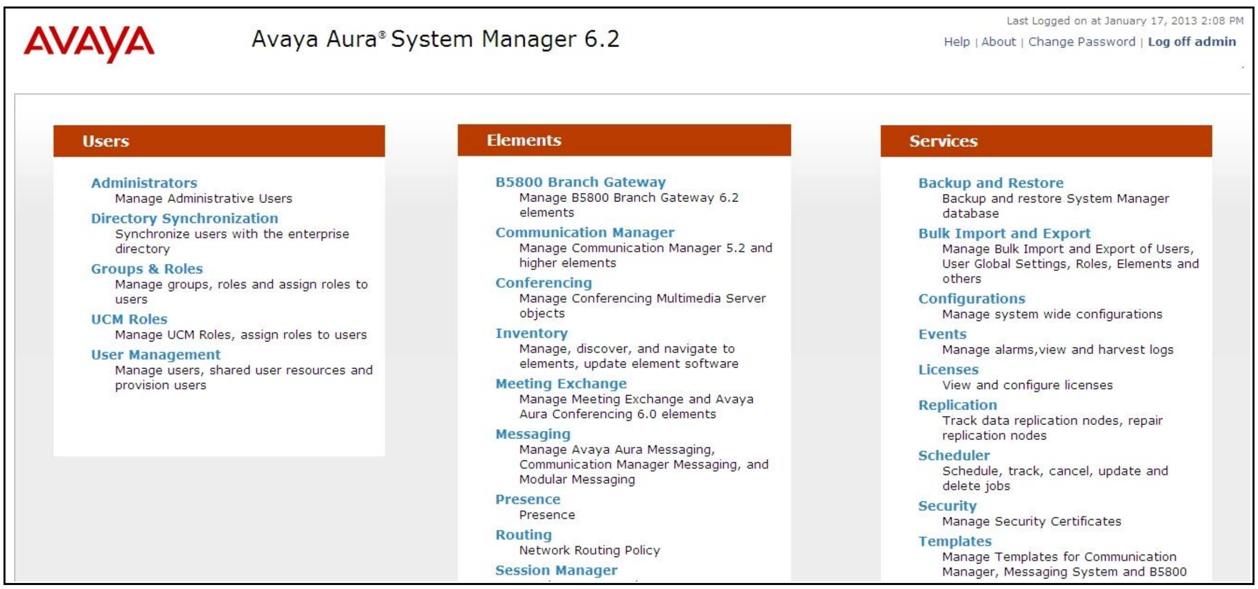
6. Configuring Avaya Aura® Session Manager

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

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

6.1. Log in to Avaya Aura® System Manager

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

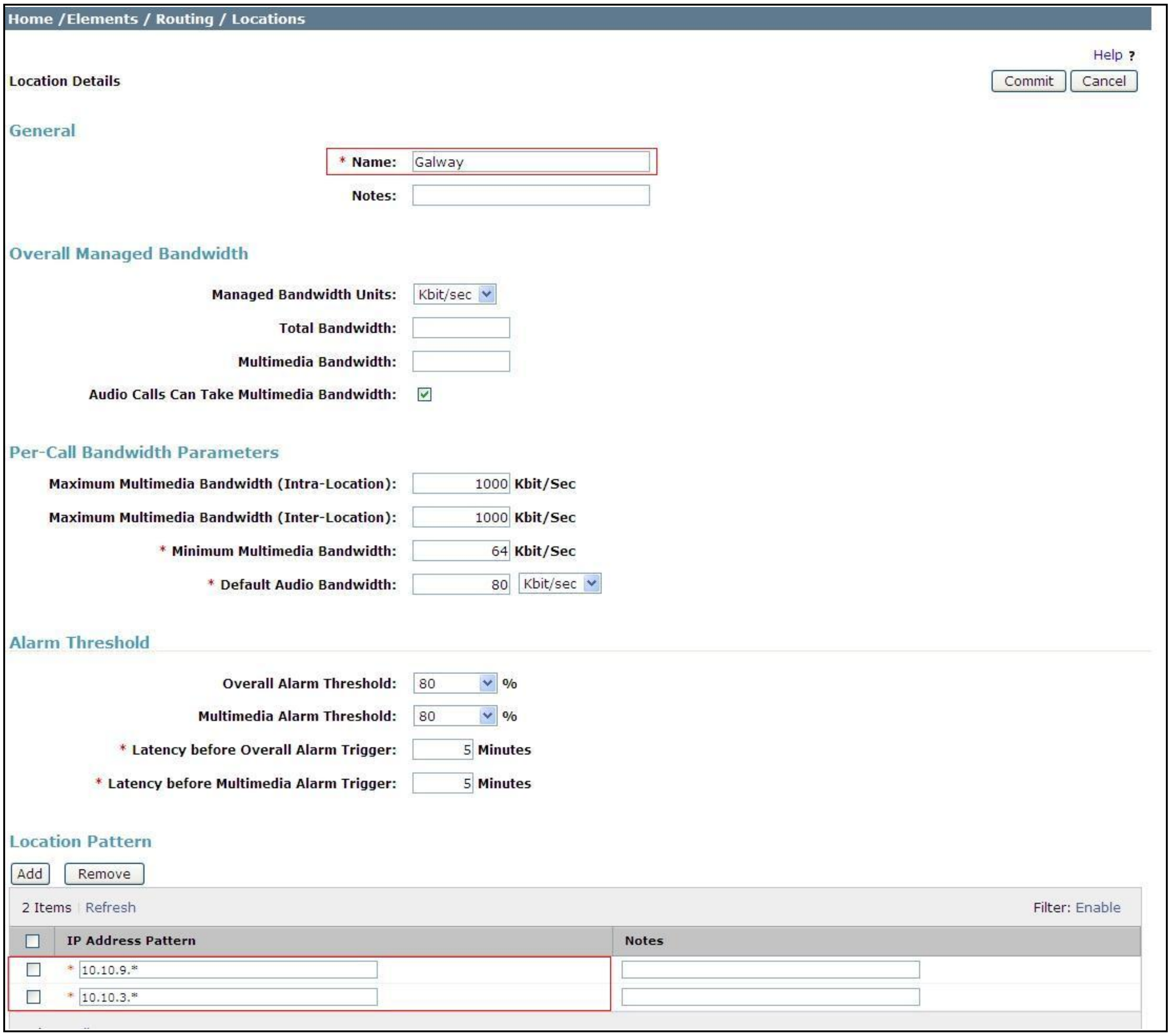


6.2. Administer SIP Domain

To add the SIP domain that will be used with Session Manager, select **Routing** from the **Home** tab menu and in the resulting tab select **Domains** from left hand menu. Click the **New** button to create a new SIP domain entry. In the **Name** field enter the domain name agreed with TDC; this will be the same as specified in the Authoritative Domain specified for the CS1000E SIP Gateway. Refer to **Section 5.4** for details. In test, **avaya.com** was used. Optionally, a description for the domain can be entered in the Notes field. Click **Commit** to save changes.

6.3. Administer Locations

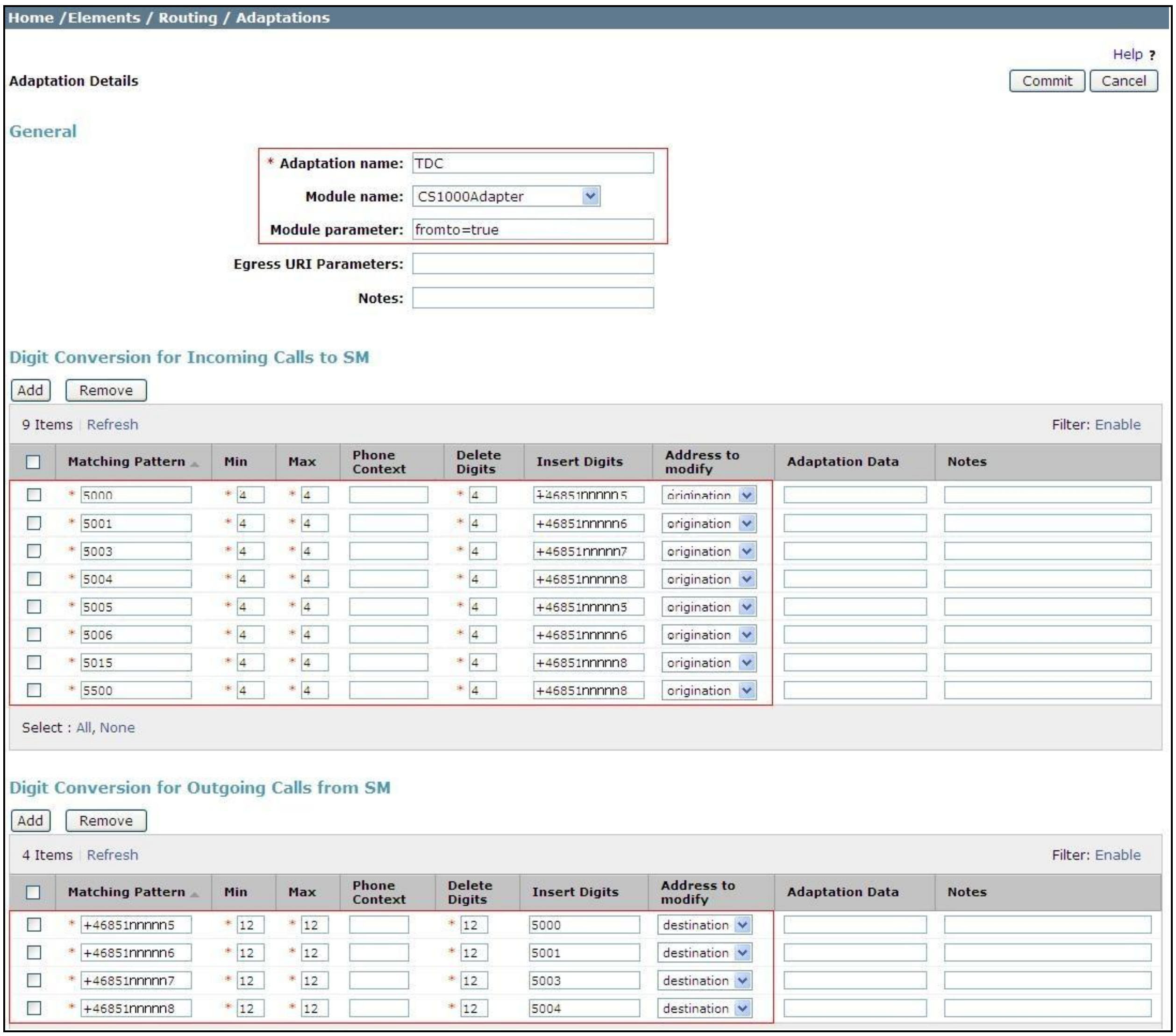
Locations can be used to identify logical and/or physical locations where SIP Entities reside, for the purposes of bandwidth management. One location is added to the sample configuration for all of the enterprise SIP entities. On the **Routing** tab select **Locations** from the left hand menu. Under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



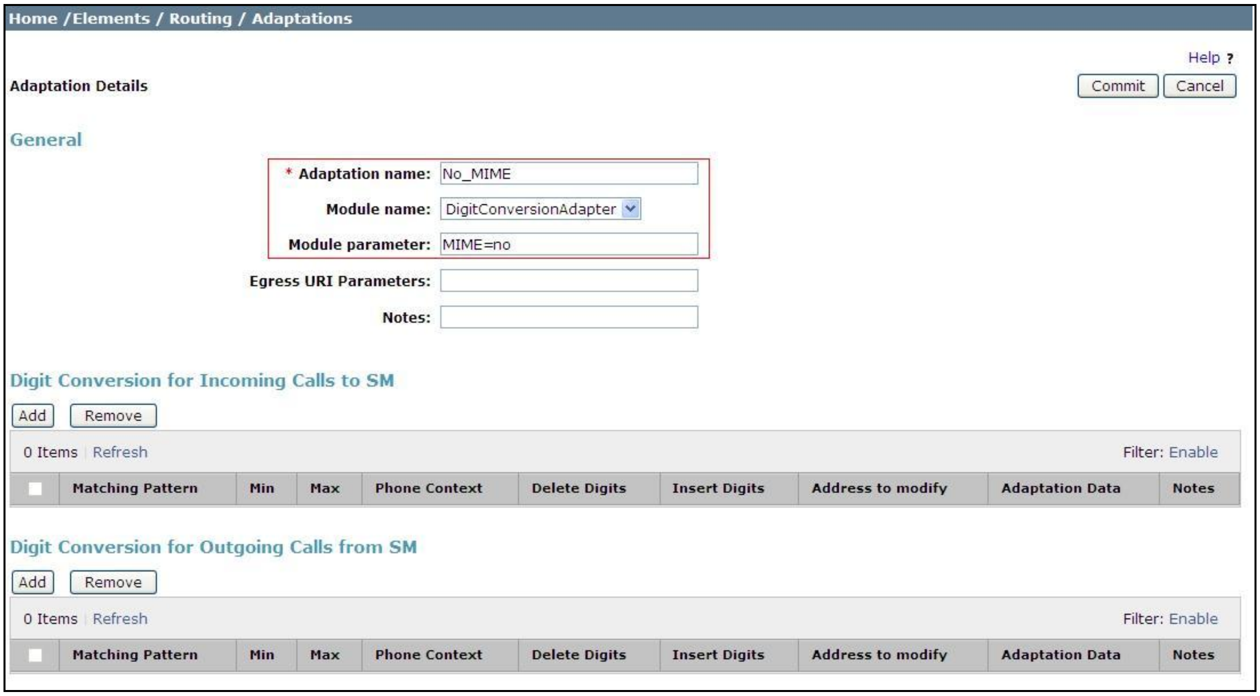
6.4. Administer Adaptations

Adaptations can be used to modify the called and calling party numbers to meet the requirements of the service. The called party number present in the SIP INVITE Request URI is modified by the **Digit Conversion** in the Adaptation. Additionally, the called and calling party numbers can be modified using **Digit Conversion** when **fromto=true** is entered in the **Module Parameters**.

The example shown uses **Digit Conversion for Incoming Calls to SM** to convert the calling number from the 4 digit extension to E.164; this applies to calls from the CS1000E to the Session Manager. It also uses **Digit Conversion for Outgoing Calls from SM** to convert the called number from E.164 to the 4 digit extension; this applies to calls from the Session Manager to the CS1000E. The module **CS1000Adaptor** is used, significant digits of the test DDI range have been obscured.



The next example shown uses "**MIME=no**" to strip MIME message bodies on egress from Session Manager to the Avaya SBCE.



6.5. Administer SIP Entities

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

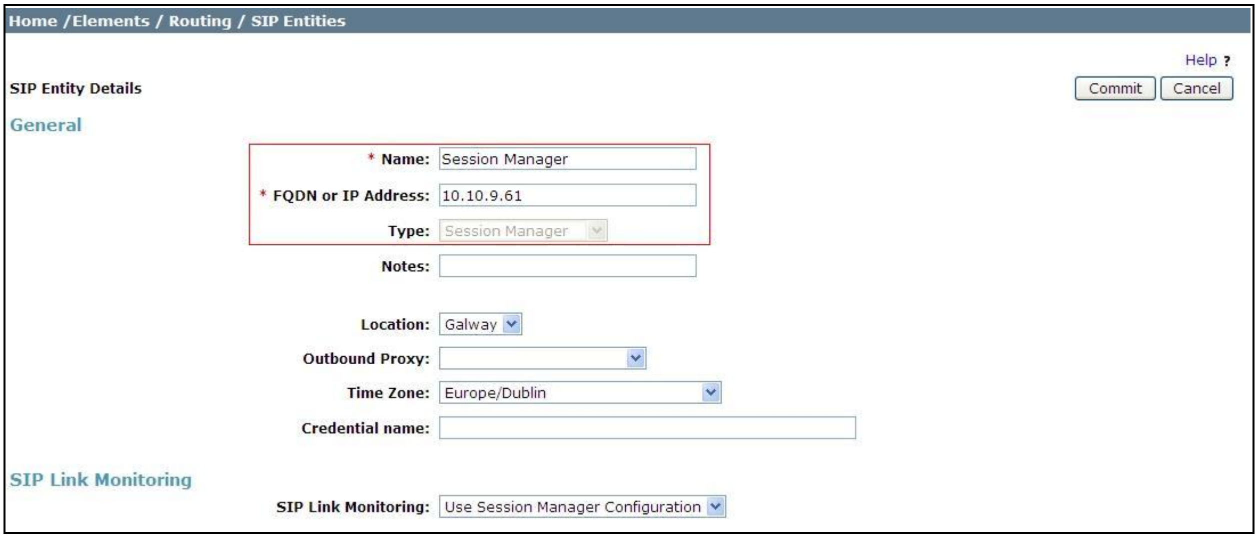
- In the **Name** field enter an informative name
- In the **FQDN or IP Address** field enter the IP address of Session Manager or the signalling interface on the connecting system
- In the **Type** field use **Session Manager** for a Session Manager SIP entity, **Other** for a CS1000E SIP entity and **SIP Trunk** for the Avaya SBCE SIP entity
- In the **Location** field select the appropriate location from the drop down menu
- In the **Time Zone** field enter the time zone for the SIP Entity

In this configuration there are three SIP Entities:

- Avaya Aura® Session Manager SIP Entity
- Avaya CS1000E SIP Entity
- Avaya Session Border Controller for Enterprise (Avaya SBCE) SIP Entity

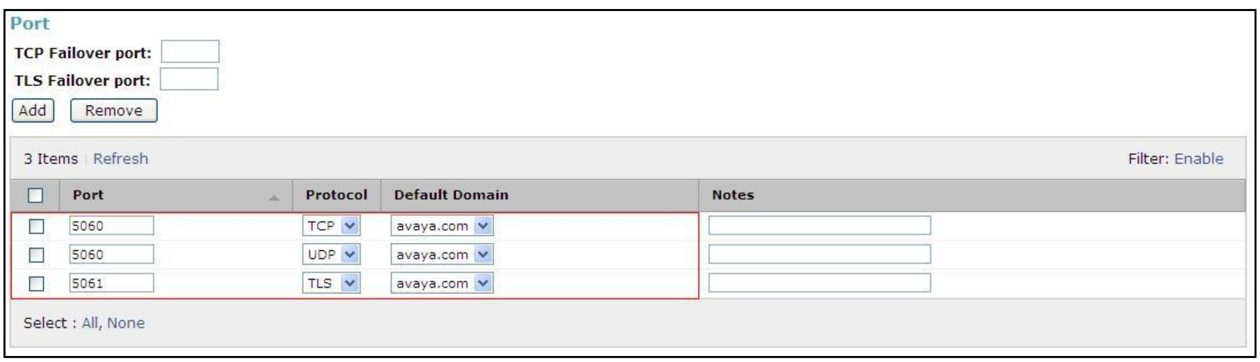
6.5.1. Avaya Aura® Session Manager SIP Entity

The following screens show the SIP entity for Session Manager. The **FQDN or IP Address** field is set to the IP address of the Session Manager SIP signalling interface.



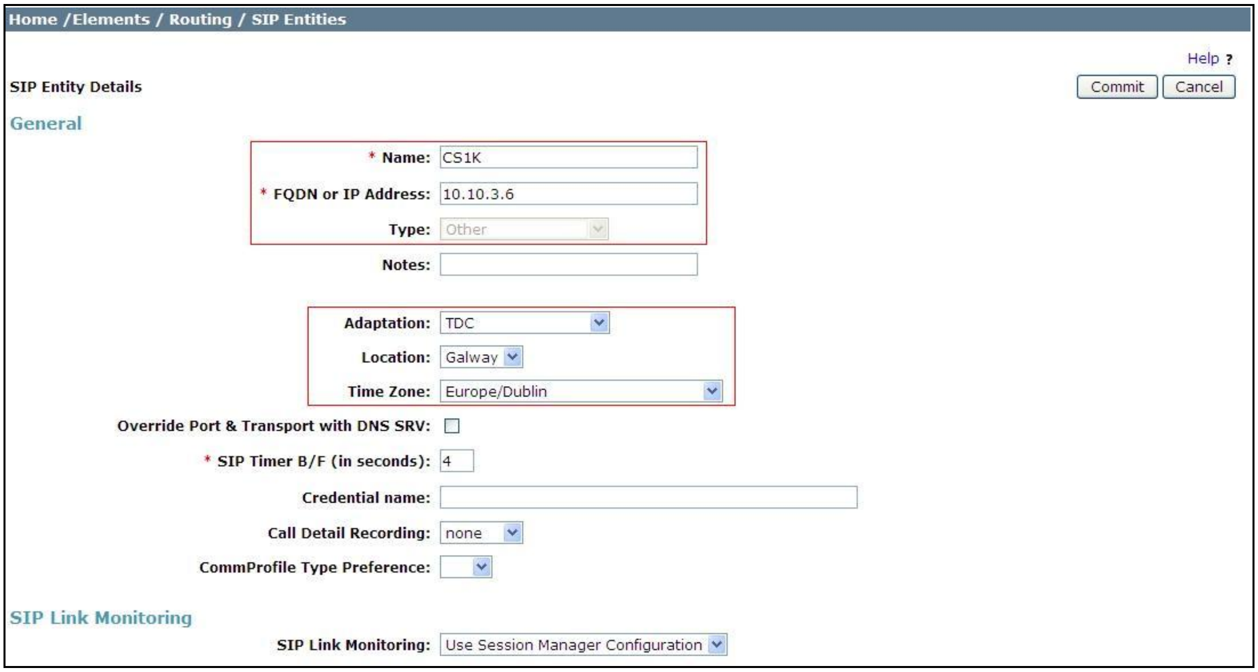
The Session Manager must be configured with the port numbers on the protocols that will be used by the other SIP entities. To configure these scroll to the bottom of the page and under **Port**, click **Add**, then edit the fields in the resulting new row.

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



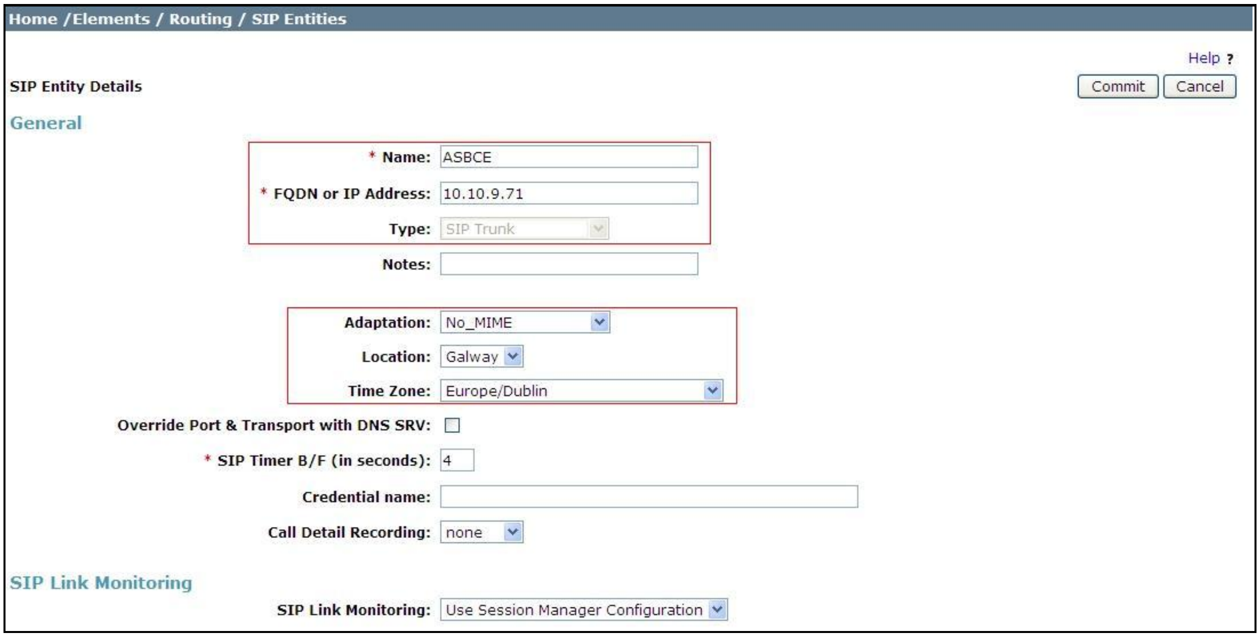
6.5.2. Avaya Communication Server 1000E SIP Entity

The following screen shows the SIP entity for CS1000E. The FQDN or IP Address field is set to the TLAN Node IP address defined in **Section 5.4**. Set the **Adaptation** to the appropriate Adaptation defined in **Section 6.4** for traffic to and from the CS100OE and set the location to that defined in **Section 6.3.**



6.5.3. Avaya Aura® Session Border Controller SIP Entity

The following screen shows the SIP Entity for the Avaya SBCE. The **FQDN or IP Address** field is set to the IP address of the Avaya SBCE private network interface (see **Figure 1**). Set the **Adaptation** to the appropriate Adaptation defined in **Section 6.4** for outbound traffic and set the location defined for use with Avaya SBCE**.**

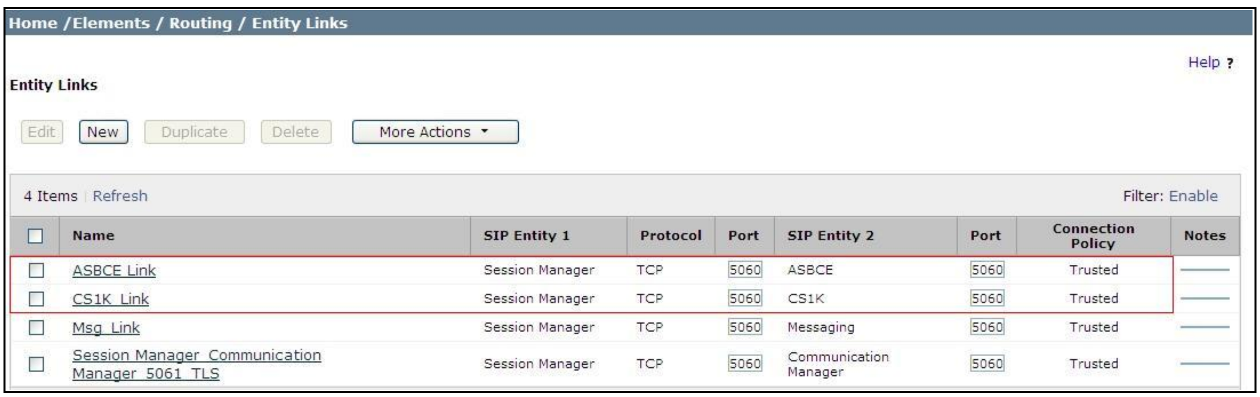


6.6. Administer Entity Links

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

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

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



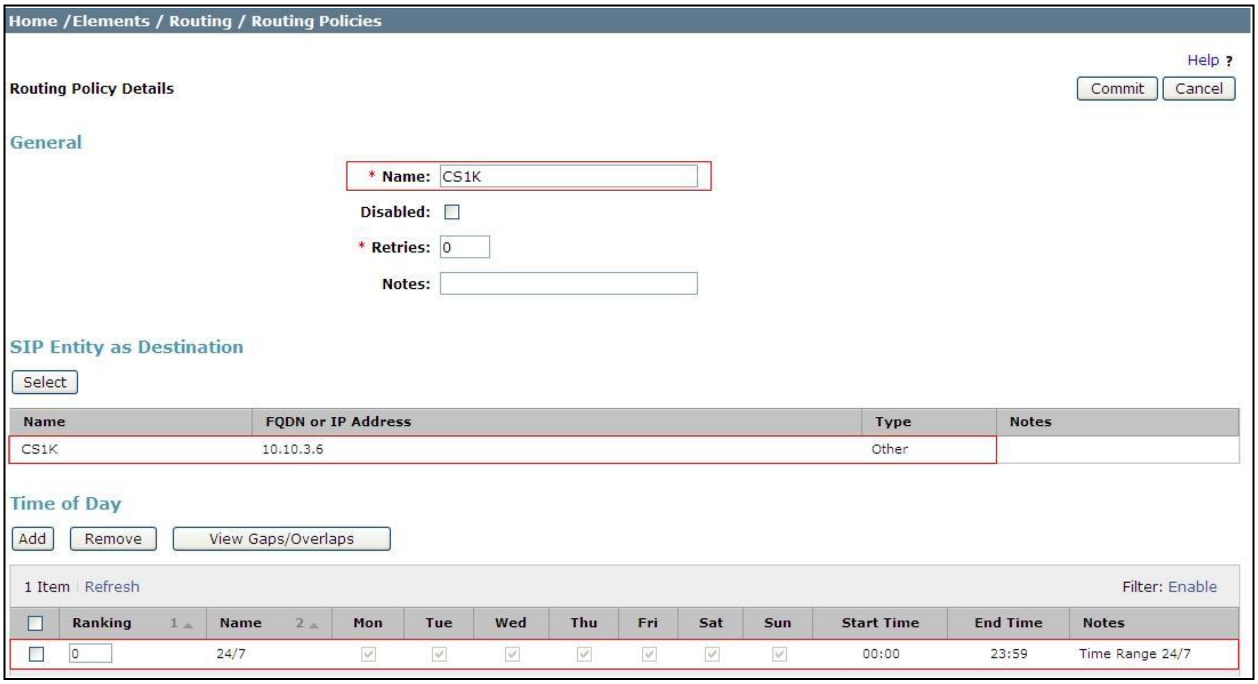
	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
☐	ASBCE Link	Session Manager	TCP	5060	ASBCE	5060	Trusted	
☐	CS1K Link	Session Manager	TCP	5060	CS1K	5060	Trusted	
☐	Msg Link	Session Manager	TCP	5060	Messaging	5060	Trusted	
☐	Session Manager Communication Manager 5061 TLS	Session Manager	TCP	5060	Communication Manager	5060	Trusted	

6.7. Administer Routing Policies

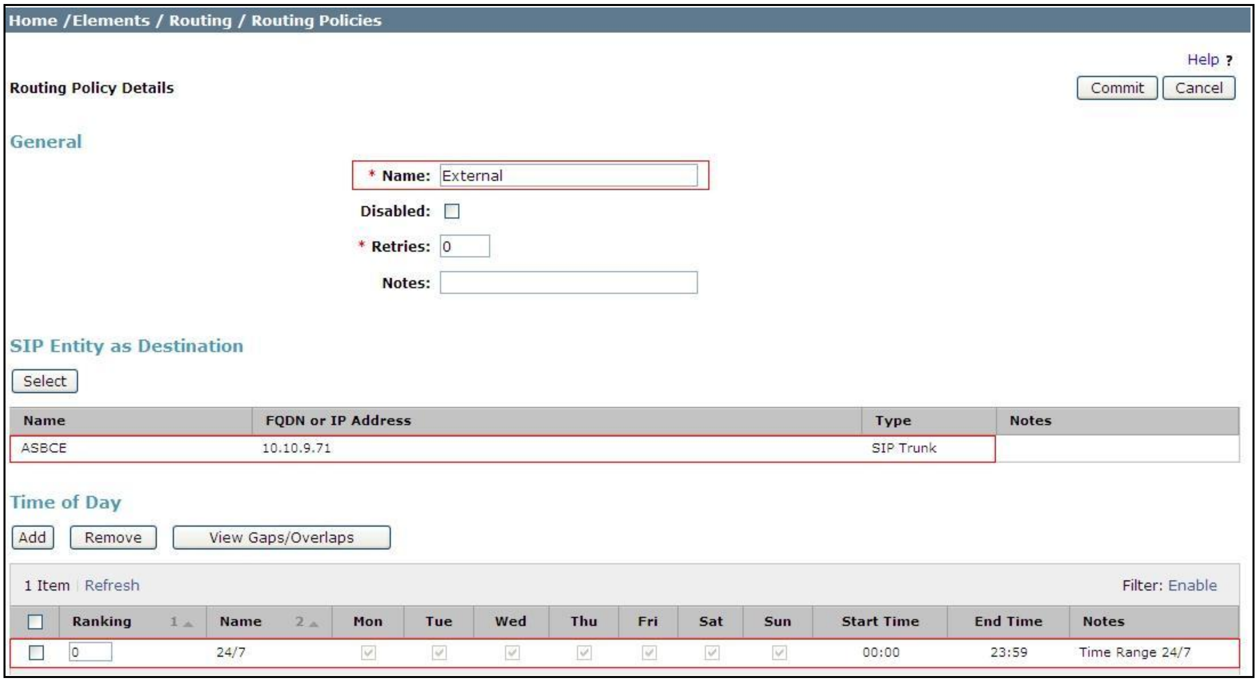
Routing policies must be created to direct how calls will be routed to a system. To add a routing policy, select **Routing Policies** on the left panel menu and then click on the **New** button (not shown).

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

The following screen shows the routing policy for CS1000E.



The following screen shows the routing policy for the Avaya SBCE.



6.8. Administer Dial Patterns

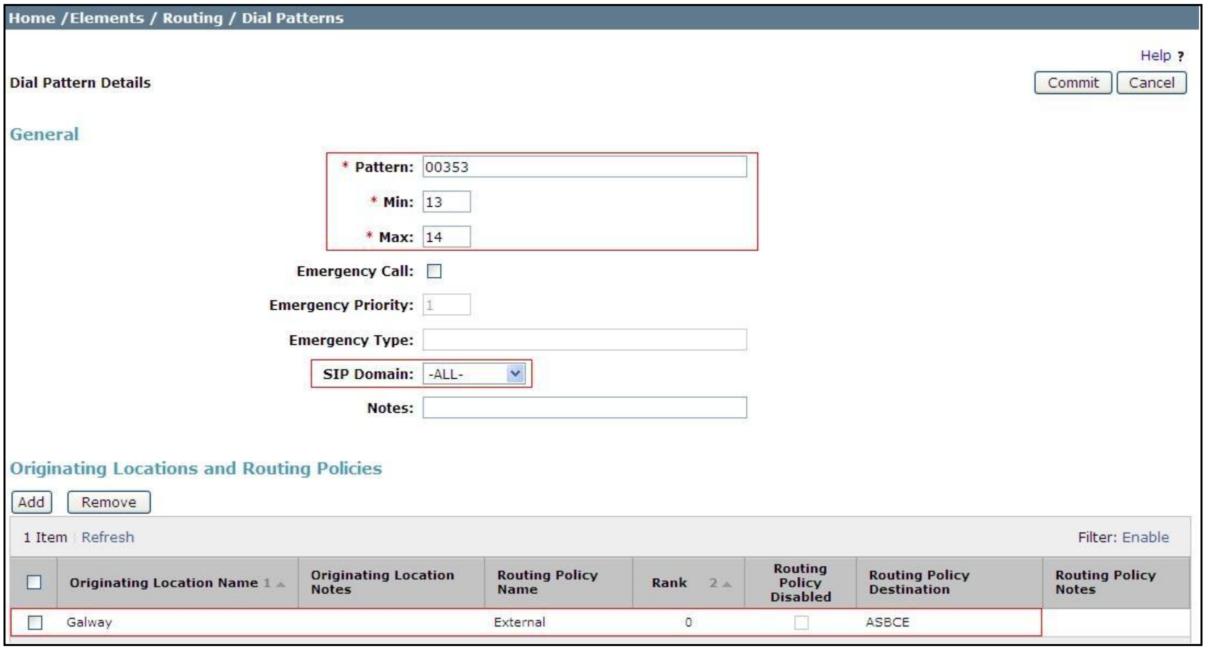
A dial pattern must be defined to direct calls to the appropriate telephony system. To configure a dial pattern select **Dial Patterns** on the left panel menu and then click on the **New** button (not shown).

Under **General**:

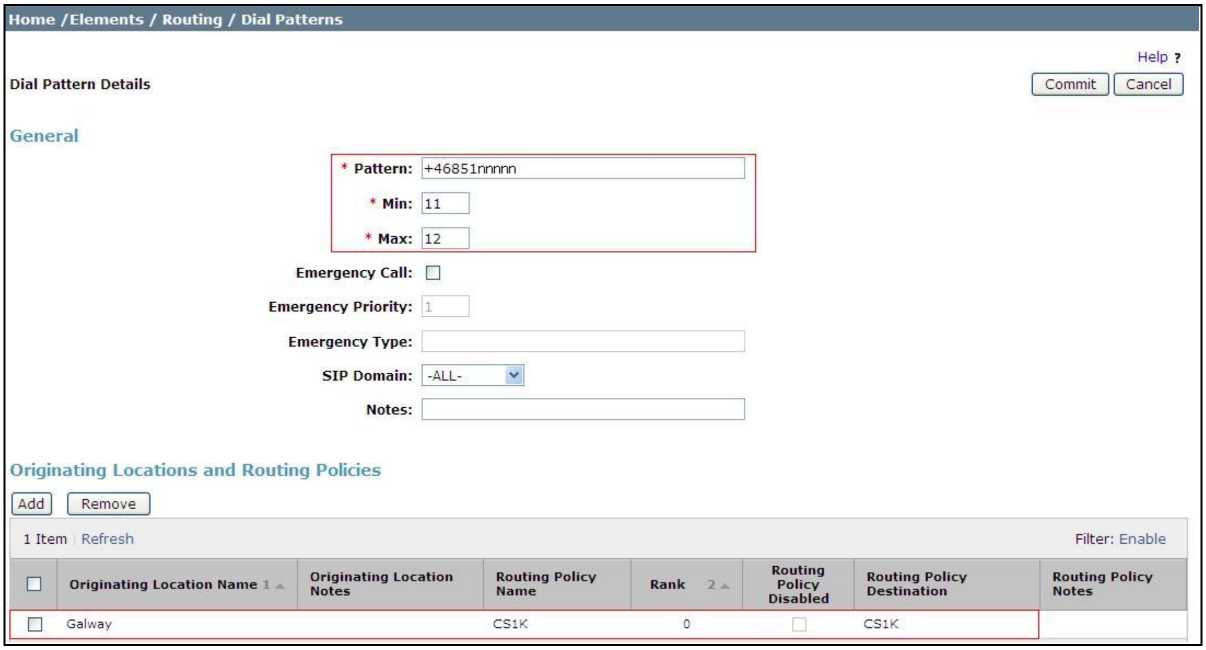
- In the **Pattern** field enter a dialled number or prefix to be matched
- In the **Min** field enter the minimum length of the dialled number
- In the **Max** field enter the maximum length of the dialled number
- In the **SIP Domain** field select **ALL** or alternatively one of those configured in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

Configuration is continued on the next page.

Under **Originating Locations and Routing Policies**, click **Add**. In the resulting screen (not shown), under **Originating Location** select the location defined in **Section 6.3** or **ALL** and under **Routing Policies** select one of the routing policies defined in **Section 6.7.** Click **Select** button to save. The following screen shows an example dial pattern configured for the Avaya SBCE which will route the calls out to the TDC Business Trunk service.



The following screen shows the test dial pattern configured for CS1000E.



Note: The pattern to be matched has been obscured.

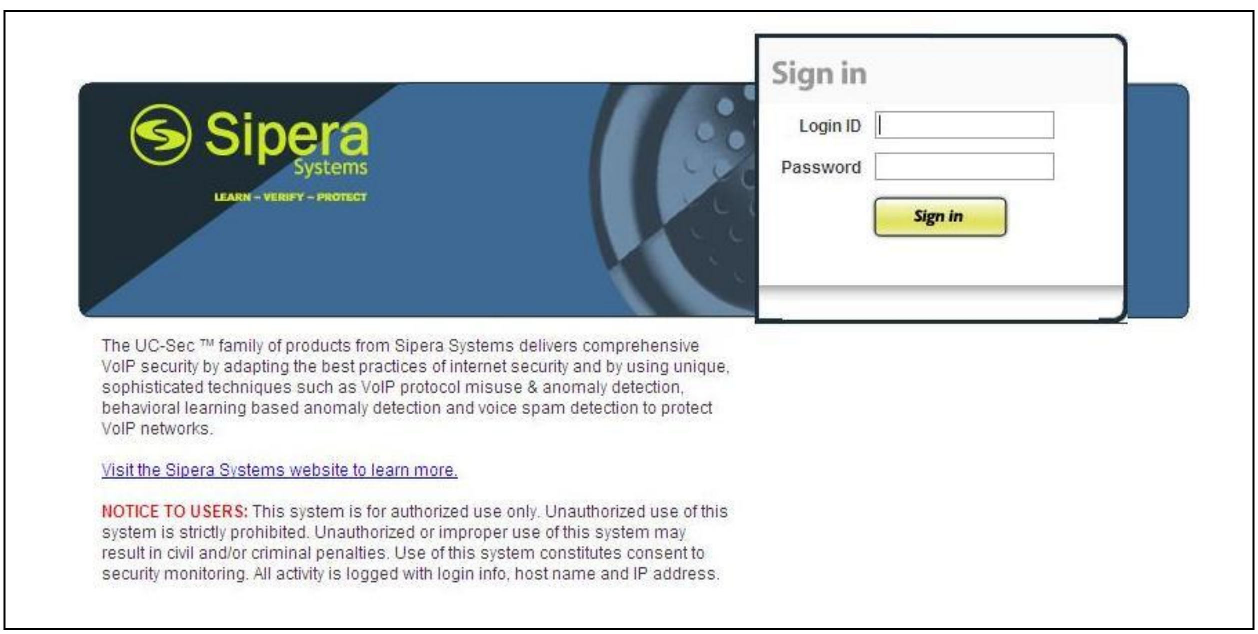
7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Session Border Controller for Enterprise. At the time of writing the Avaya Session Border Controller for Enterprise was badged as the Sipera E-SBC (Enterprise Session Border Controller) developed for Unified Communications Security (UC-Sec). The Avaya Session Border Controller for Enterprise is administered using the UC-Sec Control Center.

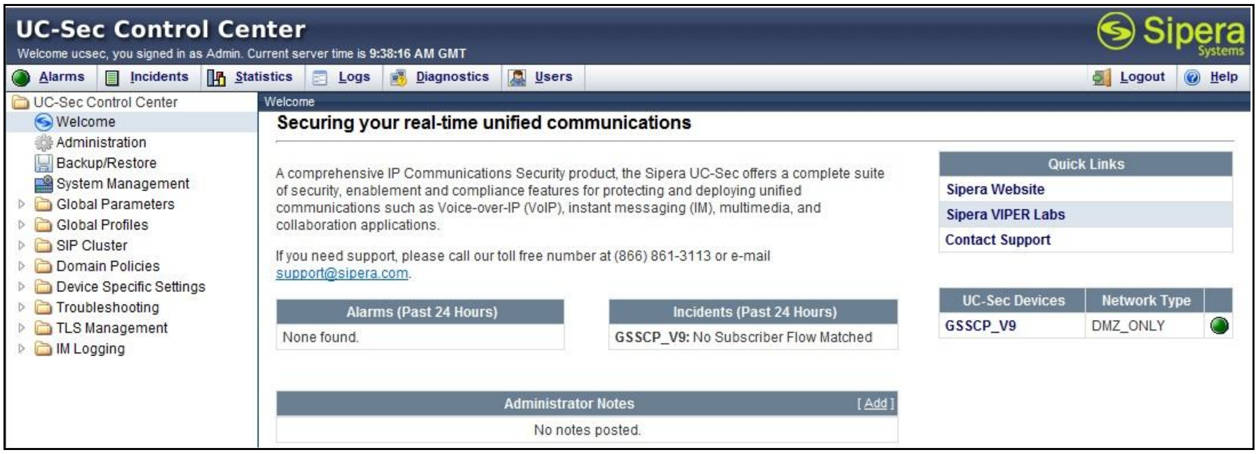
7.1. Access Avaya Session Border Controller for Enterprise

Access the Session Border Controller using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the private IP address configured at installation. Select the **UC-Sec Control Center.**

Log in with the appropriate credentials.



The following screenshot shows the opening screen. Navigation of the GUI is done in the **UC-Sec Control Center** menu on the left hand side.



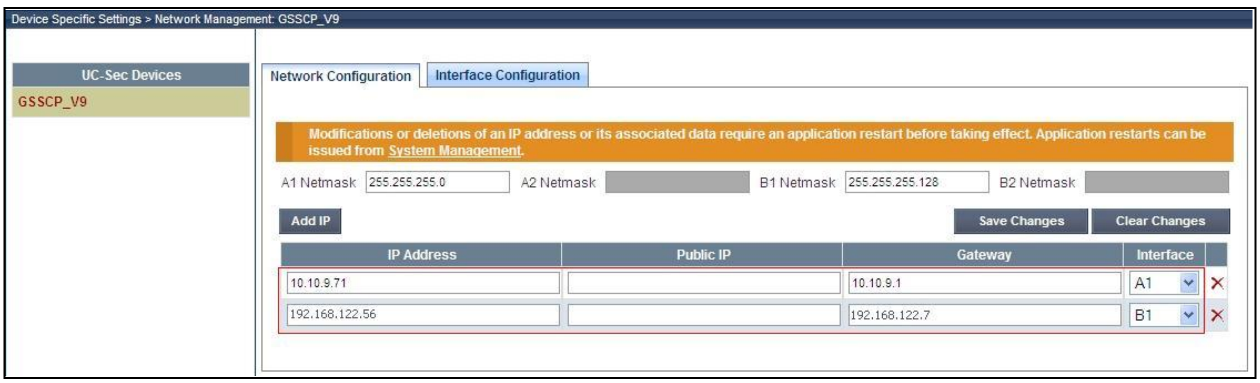
So that screenshots can be focused on the areas of the GUI where configuration takes place, the **UC-Sec Control Center** menu is not shown in subsequent screenshots

7.2. Define Network Information

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

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

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



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

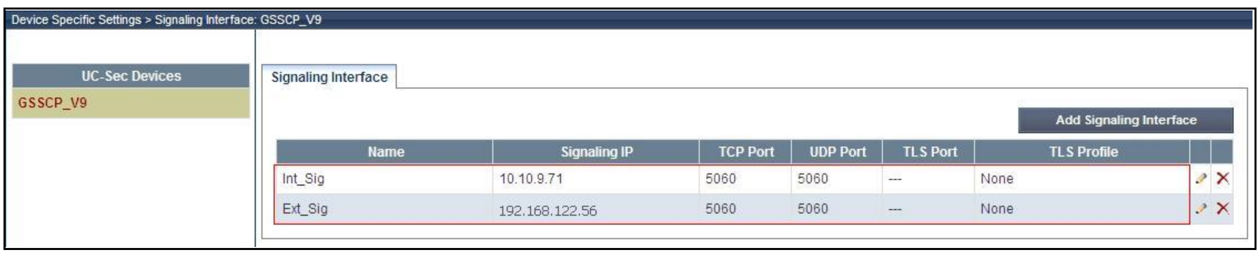
7.3. Define Interfaces

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

7.3.1. Signalling Interfaces

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

- Select **Add Signaling Interface** and enter details in the pop-up menu (not shown)
- In the **Name** field enter a descriptive name for the internal signalling interface
- For **Signaling IP**, select an **internal** signalling interface IP address defined in **Section 7.2**
- Select **UDP** and **TCP** port numbers, **5060** is used for the Session Manager
- Select **Add Signaling Interface** and enter details in the pop-up menu (not shown)
- In the **Name** field enter a descriptive name for the external signalling interface
- For **Signaling IP**, select an **external** signalling interface IP address defined in **Section 7.2**
- Select **UDP** and **TCP** port numbers, **5060** is used for TDC



7.3.2. Media Interfaces

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

- Select **Add Media Interface** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the internal media interface
- For **Media IP**, select an **internal** media interface IP address defined in **Section 7.2**
- Select **RTP port** ranges for the media path with the enterprise end-points
- Select **Add Media Interface** and enter details in the pop-up menu
- In the **Name** field enter a descriptive name for the external media interface
- For **Media IP**, select an **external** media interface IP address defined in **Section 7.2**
- Select **RTP port** ranges for the media path with the TDC network

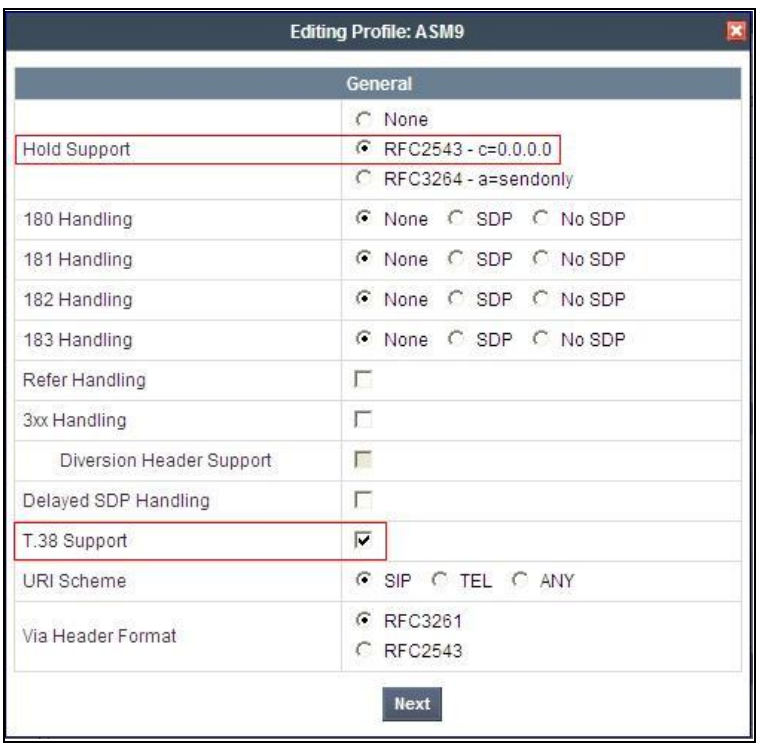
Note: During test the port ranges for the external media interface were left at the default values

7.4. Define Server Interworking

Server interworking is defined for each server connected to the Avaya SBCE. In this case, the TDC SBC is connected as the Trunk Server and the Session Manager is connected as the Call Server. Configuration of interworking includes Hold support, T.38 fax support and SIP extensions. Also included in this configuration is Request-URI header manipulation on the trunk Server to remove the international dialling prefix of "00" and insert a "+". Although this can be achieved using digit manipulation on the Session manager, it is included here for information.

To define server interworking on the Avaya SBCE, navigate to **Global Profiles → Server Interworking** in the **UC-Sec Control Center** menu on the left hand side. To define Server Interworking for the Session Manager, highlight the **avaya-ru** profile which is a factory setting appropriate for Avaya equipment and select **Clone Profile**. A pop-up menu is generated headed **Clone Profile** (not shown)

- In the **Clone Name** field enter a descriptive name for the Session Manager and click **Finish** – in test **ASM9** was used
- In the **General** tab (not shown) Select **Edit** and enter details in the pop-up menu.
- Check the **T.38** box
- Change the **Hold Support** RFC to **RFC2543** then click **Next** and **Finish**



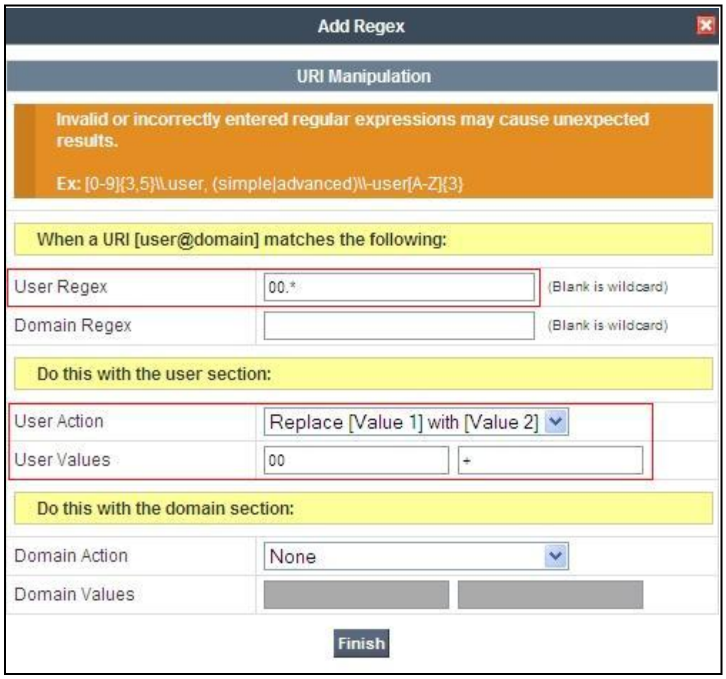
- In the **Advanced** tab (not shown) Select **Edit** and enter details in the pop-up menu.
- Uncheck the **AVAYA Extensions** box

To define Server Interworking for the TDC SBC, highlight the previously defined profile for the Session Manager and select **Clone Profile**. A pop-up menu is generated headed **Clone Profile** (not shown)

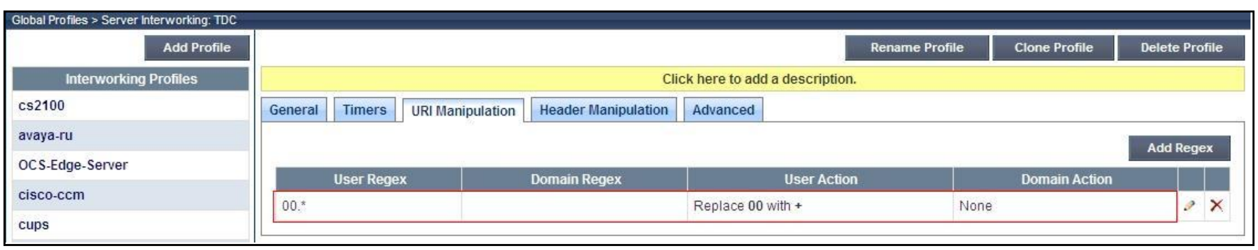
- In the **Clone Name** field enter a descriptive name for server interworking profile for the TDC SBC and click **Finish** – in test **TDC** was used
- Select **Edit** and enter details in the pop-up menu
- Check the **T.38** box
- Select **Next** three times and **Finish**

The Trunk Server interworking includes the Request-URI header manipulation

- In the **URI Manipulation** tab (not shown) Select **Add Regex** and enter details in the pop-up menu.
- Enter **00.*** in the **User Regex** box (the "." denotes any character and the "*" allows any subsequent characters.
- Select **Replace [Value 1] with [Value 2]** in the **User Action** drop down menu and enter **00** as Value 1and **+** as Value 2 in the **User Values** boxes
- Select **Finish**



The resultant URI manipulation appears under the **URI manipulation** tab as follows:



7.5. Define Signalling Manipulation

Signalling manipulation is required in some cases to ensure effective interworking. During test, some issues were found in the interworking between the TDC Business Trunk service and the enterprise. Two of these issues could not be resolved by other methods such as **Server Interworking** and **Signaling Rules.** The first issue is that re-INVITEs from One-X Communicator, e.g. for call hold, included Payload Type 120 for DTMF. These re-INVITEs were resulting in the call being cleared by the network.

The second issue is that calls to the mobile extension for the Mobile Extension (MEX) service require two numbers in the To header, these are the Angöringsnummer (ANG) and the Calling Party Number. This could only be achieved with a script on the Avaya SBCE.

To define the signalling manipulation to change the Payload Type for DTMF in the re-INVITE sent for call hold, navigate to **Global Profiles → Signaling Manipulation** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Script** and enter a title and the script in the script editor (not shown). The title use in test was **Video_Removal**. The script text is as follows:

```
within session "ALL"
{
  act on message where %DIRECTION="INBOUND" and %ENTRY_POINT="AFTER_NETWORK" and
%METHOD="INVITE"
  {
    if(exists(%SDP[1]["s"]["m"][2].ATTRIBUTES["video"][1]))then
    {
      %BODY[1].regex_replace("b=TIAS:13952000","");
      %SDP[1]["s"]["m"][1].FORMATS[4]="101";
      %SDP[1]["s"]["m"][1].ATTRIBUTES["rtpmap"][4]="101 telephone-event/8000/1";
      remove(%SDP[1]["s"]["m"][2]);
    }
  }
}
```

Note: This script also removes video attributes present in the SDP for call hold, hence the name.

To define the signalling manipulation to reformat the To header in line with the requirements of the MEX service, navigate to **Global Profiles → Signaling Manipulation** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Script** and enter a title and the script in the script editor. The title used in test was **MEX_Mobile_From**. The script text is as follows:

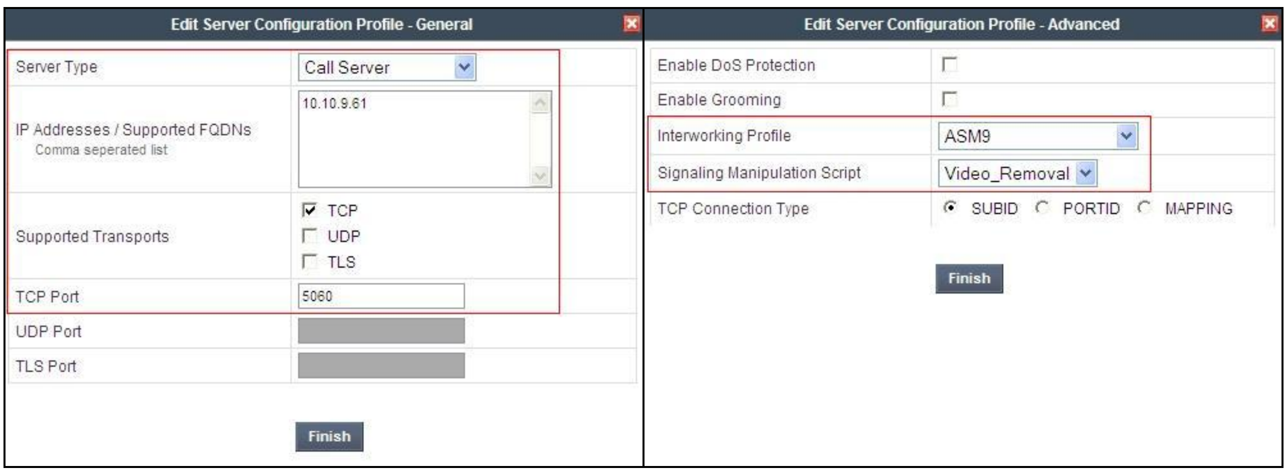
```
within session "ALL"
{
  act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING" and
%METHOD="INVITE"
  {
    if(%HEADERS["To"][1].URI.USER.regex_match("^.46394980"))then
    {
      %HEADERS["From"][1].URI.USER.regex_replace("^\+","00");
      %FromUser = %HEADERS["From"][1].URI.USER;
      %HEADERS["From"][1].URI.USER  = "+46752468911";
      append(%HEADERS["From"][1].URI.USER, %FromUser);
    }
  }
}
```

Note: The above script prefixes the ANG to the calling party number in the From header, and also reformats the calling party number to insert the international dialling prefix. This avoids a "+" appearing in the middle of the number.

7.6. Define Servers

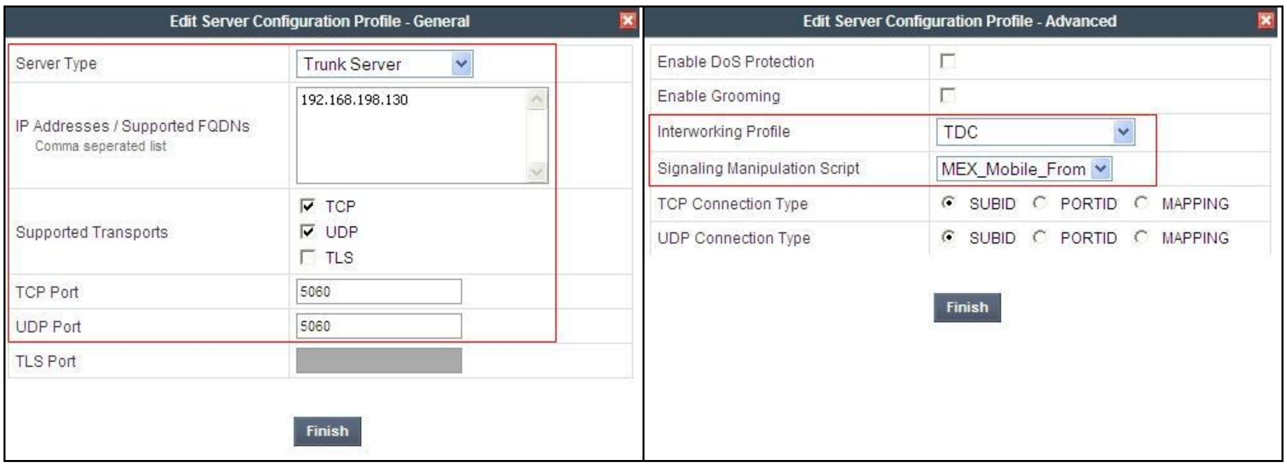
Servers are defined for each server connected to the Avaya SBCE. In this case, the TDC SBC is connected as the Trunk Server and the Session Manager is connected as the Call Server. To define the Session Manager, navigate to **Global Profiles → Server Configuration** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** (not shown) and enter details in the pop-up menu

- In the **Profile Name** field enter a descriptive name for the Session Manager and click **Next** (not shown)
- In the **Server Type** drop down menu, select **Call Server**
- In the **IP Addresses / Supported FQDNs** box, type the Session Manager SIP interface address which is the same as that defined on Session Manager in **Section 6.5**
- Check **TCP** in **Supported Transports**
- Define the **TCP** port for SIP signalling, **5060** is used for the Session Manager
- Click **Next** three times then select the **Interworking Profile** for the Session Manager defined in **Section 7.4** from the drop down menu
- Select the **Video_Removal** Signaling Manipulation Script defined in **Section 7.5** from the drop down menu and click **Finish**



To define the TDC SBC as a Trunk Server, navigate to **Global Profiles → Server Configuration** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** (not shown) and enter details in the pop-up menu

- In the **Profile Name** field enter a descriptive name for the TDC SBC and click **Next** (not shown)
- In the **Server Type** drop down menu, select **Trunk Server**
- In the **IP Addresses / Supported FQDNs** box, type the IP address of the TDC SBC
- Check **UDP** in **Supported Transports**
- Define the **UDP** port for SIP signaling, **5060** is used for TDC
- Click **Next** three times then select the **Interworking Profile** for the TDC SBC defined in **Section 7.4** from the drop down menu
- Select the **MEX_Mobile_From** Signaling Manipulation Script defined in **Section 7.5** from the drop down menu and click **Finish**



7.7. Define Routing

Routing information is required for routing to the Session Manager on the internal side and the TDC SBC on the external side. The IP addresses and ports defined here will be used as the destination addresses for signalling. If no port is specified in the **Next Hop IP Address**, default 5060 is used. To define routing to the Session Manager, navigate to **Global Profiles → Routing** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and enter details in the **Routing Profile** pop-up menu (not shown).

- In the **Profile Name** field enter a descriptive name for the Session Manager, in this case **ASM9**, and click **Next**
- Enter the Session Manager SIP interface address and port in the **Next Hop Server 1** field
- Select **TCP** for the **Outgoing Transport**
- Click **Finish**

To define routing to the TDC SBC, navigate to **Global Profiles → Routing** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and enter details in the **Routing Profile** pop-up menu.

- In the **Profile Name** field enter a descriptive name for the TDC SBC, in this case a generic name of **Trunk Server** was used, and click **Next**
- Enter the TDC SBC IP address and port in the **Next Hop Server 1** field
- Select **UDP** for the **Outgoing Transport**
- Click **Finish**

7.8. Topology Hiding

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

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

- In the **Profile Name** field enter a descriptive name for the Session Manager and click **Next**
- If the **Request-Line**, **Record-Route** and **Via** Headers aren't shown, click on **Add Header** and select from the **Header** drop down menu
- For each of the above headers, leave the **Replace Action** at the default value of **Auto**
- If the **From**, **To** and **SDP** Headers aren't shown, click on **Add Header** and select from the **Header** drop down menu
- For each of the above headers, select **IP** from the **Criteria** drop down menu (important for the **From** header so that the "anonymous.invalid" domain name for restricted CLI is not overwritten)
- For each of the headers leave the **Replace Action** at the default value of **Auto**

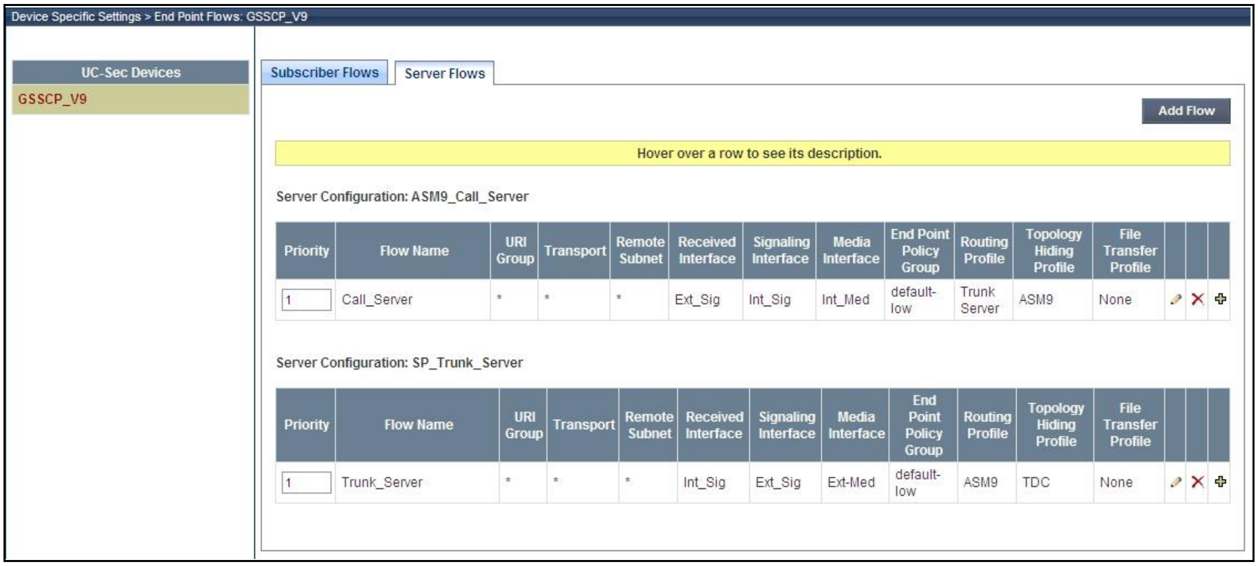
Note: The use of **Auto** results in an IP address being inserted in the host portion of the Request-URI as opposed to a domain name. If a domain name is required, the action **Overwrite** must be used where appropriate, and the required domain names entered in the **Overwrite Value** field. Different domain names could be used for the enterprise and the TDC network.

To define Topology Hiding for the TDC SBC, navigate to **Global Profiles → Topology Hiding** in the **UC-Sec Control Center** menu on the left hand side. Click on **Add Profile** and enter details in the **Topology Hiding Profile** pop-up menu (not shown).

- In the **Profile Name** field enter a descriptive name for the TDC SBC and click **Next**
- If the **Request-Line**, **From and To** Headers aren't shown, click on **Add Header** and select from the **Header** drop down menu
- For each of the above headers, change the **Replace Action** to **Overwrite** and define the required domain name in the **Overwrite Value** field
- If the **Record-Route** and **Via** Headers aren't shown, click on **Add Header** and select from the **Header** drop down menu
- For each of the above headers, select **IP** from the **Criteria** drop down menu
- For each of the headers leave the **Replace Action** at the default value of **Auto**
- Repeat the above steps for the **SDP** if required and set the **Criteria** to **IP**

7.9. Server Flows

Server Flows combine the previously defined profiles into an outgoing flow from the Session Manager to the TDC SBC and an incoming flow from the TDC SBC to the Session Manager. This configuration ties all the previously entered information together so that calls can be routed from the Session Manager to the TDC SBC and vice versa. The information for all Server Flows is shown on a single screen on the Avaya SBCE.



To define an outgoing Server Flow, navigate to **Device Specific Settings → End Point Flows**.

- Click on the **Server Flows** tab
- Select **Add Flow** and enter details in the pop-up menu (not shown)
- In the **Name** field enter a descriptive name for the outgoing server flow to the TDC SBC, in this case a generic name of **Trunk_Server** was used
- In the **Received Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.3**
- In the **Signaling Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3**
- In the **Media Interface** drop-down menu, select the external media interface defined in **Section 7.3**
- In the **Routing Profile** drop-down menu, select the routing profile of the Session Manager defined in **Section 7.7**
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the TDC SBC defined in **Section 7.8** and click **Finish**

Server Configuration: SP_Trunk_Server

Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile			
1	Trunk_Server	*	*	*	Int_Sig	Ext_Sig	Ext-Med	default-low	ASM9	TDC	None			

An incoming Server Flow is defined as a reversal of the outgoing Server Flow

- Click on the **Server Flows** tab
- Select **Add Flow** and enter details in the pop-up menu (not shown)
- In the **Name** field enter a descriptive name for the incoming server flow to the Session Manager, in this case a generic name of **Call_Server** was used
- In the **Received Interface** drop-down menu, select the external SIP signalling interface defined in **Section 7.3**
- In the **Signaling Interface** drop-down menu, select the internal SIP signalling interface defined in **Section 7.3**
- In the **Media Interface** drop-down menu, select the internal media interface defined in **Section 7.3**
- In the **Routing Profile** drop-down menu, select the routing profile of the TDC SBC defined in **Section 7.7**
- In the **Topology Hiding Profile** drop-down menu, select the topology hiding profile of the Session Manager defined in **Section 7.8** and click **Finish**

Server Configuration: ASM9_Call_Server

Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile			
1	Call_Server	*	*	*	Ext_Sig	Int_Sig	Int_Med	default-low	Trunk Server	ASM9	None			

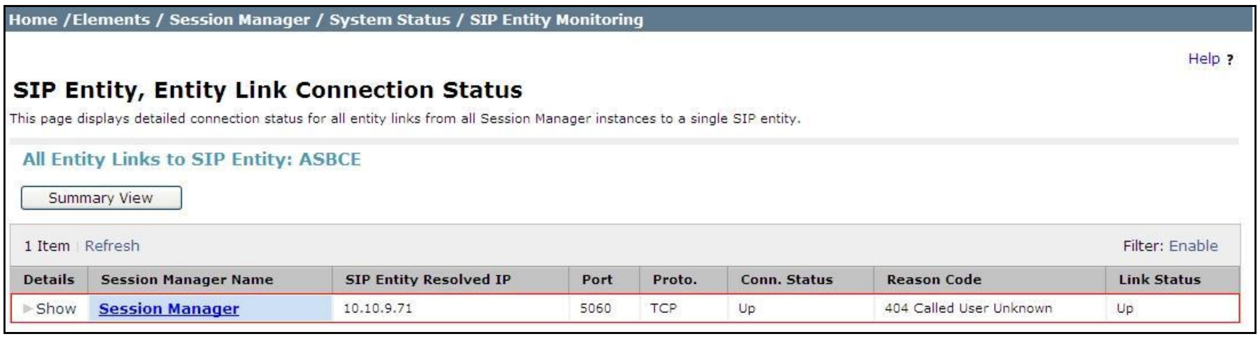
8. Configure TDC Equipment

The configuration of the TDC equipment used to support the TDC Business Trunk service is outside of the scope of these Application Notes and will not be covered. To obtain further information on TDC equipment and system configuration please contact an authorised TDC representative.

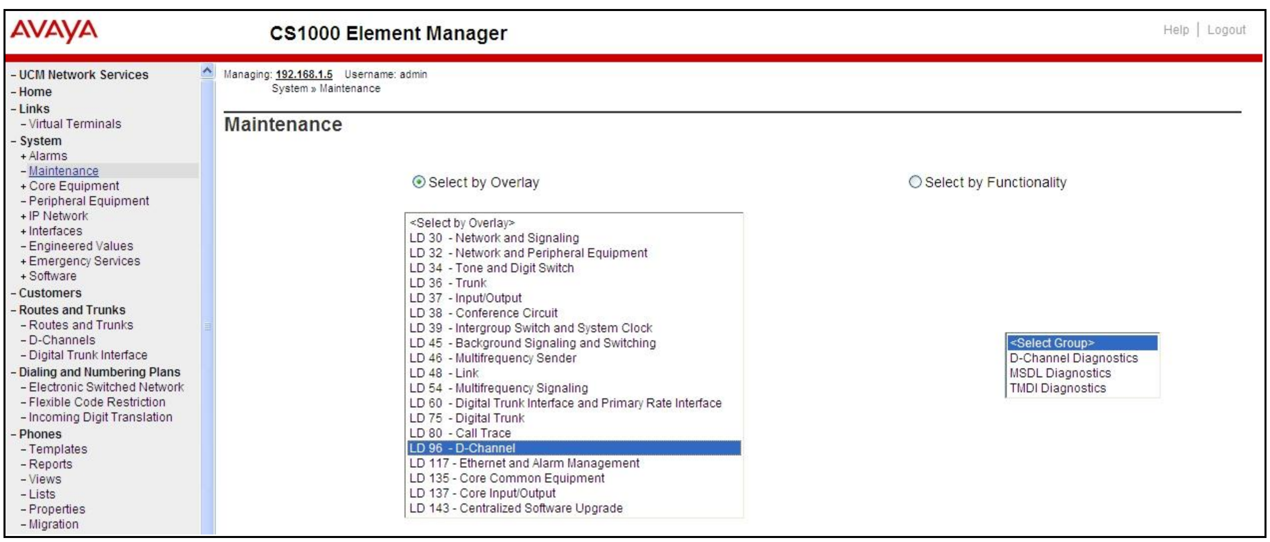
9. Verification Steps

This section provides steps that may be performed to verify that the solution is configured correctly.

1. From System Manager **Home** tab click on **Session Manager** and navigate to **Session Manager → System Status → SIP Entity Monitoring**. Select the relevant SIP Entity from the list and observe if the **Conn Status** and **Link Status** are showing as **up**.

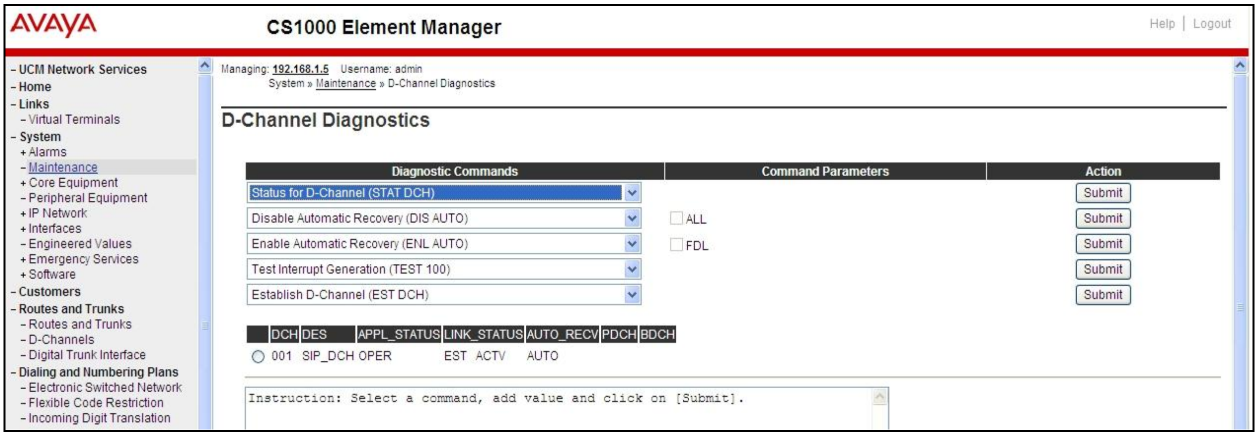


2. From CS1000E Element Manager, expand **System** on the left navigation panel and select **Maintenance.** Select **LD 96 - D-Channel** from the **Select by Overlay** table and the **D-Channel Diagnostics** function from the **Select Group** table as shown below.

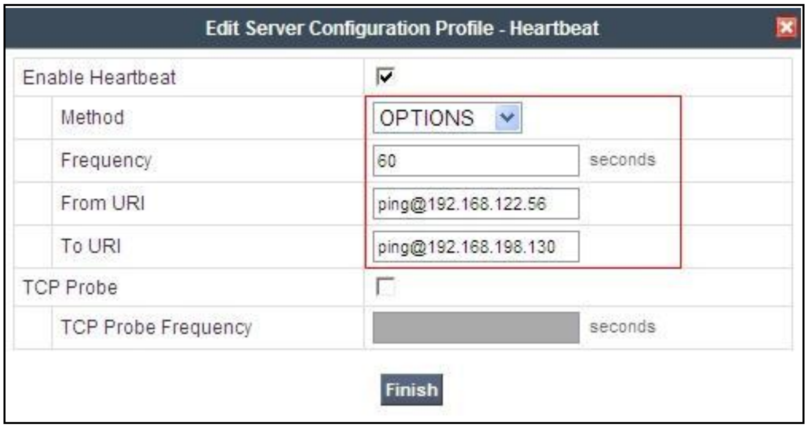


Select **Status for D-Channel (STAT DCH)** command and click **Submit** to verify status of virtual D-Channel as shown below. Verify the status of the following fields.

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

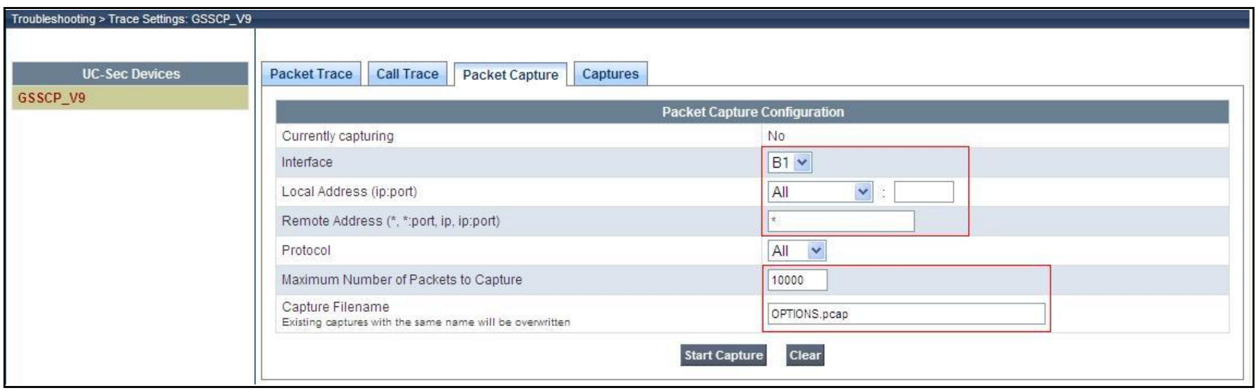


3. Verify that endpoints at the enterprise site can place calls to the PSTN and that the call remains active
4. Verify that endpoints at the enterprise site can receive calls from the PSTN and that the call can remain active
5. Verify that the user on the PSTN can end an active call by hanging up
6. Verify that an endpoint at the enterprise site can end an active call by hanging up.
7. Should issues arise with the SIP trunk, check from the Avaya SBCE using OPTIONS. This is done by defining the heartbeat in the Server configuration then running a trace. To define the heartbeat, navigate to **Global Profiles → Server Configuration** in the **UC-Sec Control Center** menu on the left hand side and click on the Trunk Server profile. Select the **Heartbeat** tab and click on **Edit**
   - Check the **Enable Heartbeat** box
   - Select **OPTIONS** from the **Method** drop down menu
   - Enter the **Frequency** in seconds, for convenience this can be set to the minimum value of **60** seconds
   - Enter the **From URI** in Fully Qualified Domain Name format
   - Enter the **To URI** in FQDN
   - Click on **Finish**



To define the trace, navigate to **Troubleshooting → Trace Settings** in the **UC-Sec Control Center** menu on the left hand side and select the **Packet Capture** tab.

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



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

The trace is viewed as a standard pcap file in Wireshark. If the SIP trunk is working correctly, a SIP response will be seen from the Service Provider.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Communication Server 1000E R7.5, Avaya Aura® Session Manager R6.2 and Avaya Session Border Controller for Enterprise R4.0.5 to the TDC Business Trunk service. TDC Business Trunk is a SIP-based Voice over IP solution providing businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. The service was successfully tested with a number of observations listed in **Section 2.2**.

11. Additional References

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

[1] *Installing and Configuring Avaya Aura® System Platform Release 6.2*, March 2012.

[2] *Administering Avaya Aura® System Platform Release 6.2*, February 2012.

[3] *Co-resident Call Server and Signaling Server Fundamentals, Avaya Communication Server 1000E Release 7.5*, Document Number NN43001-509

[4] *Signaling Server and IP Line Fundamentals, Avaya Communication Server 1000E Release 7.5*, Document Number NN43001-125

[5] *Implementing Avaya Aura® System Manager Release 6.2*, March 2012.

[6] *Implementing Avaya Aura® Session Manager*, February 2012, Document Number 03-603473

[7] *Administering Avaya Aura® Session Manager*, February 2012, Document Number 03-603324.

[8] *E-SBC (Avaya Session Border Controller for Enterprise) Administration Guide*, November 2011

[9] *RFC 3261 SIP: Session Initiation Protocol*, http://www.ietf.org/

[10] *TDC Business Trunk Technical Specification*, Release A5, September 2012

Appendix A – Avaya Communication Server 1000E Software

Avaya Communication Server 1000E call server patches and plug ins

```
TID: 46379

VERSION 4121

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

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

RELEASE 7
ISSUE 50 Q  +
IDLE_SET_DISPLAY NORTEL
DepList 1: core Issue: 01  ALTERED(created: 2012-07-16 17:52:47 (est))

MDP>LAST SUCCESSFUL MDP REFRESH :2012-10-02 13:46:39(Local Time)
MDP>USING DEPLIST ZIP FILE DOWNLOADED :2012-08-20 11:29:05(est)
SYSTEM HAS NO USER SELECTED PEPS IN-SERVICE


LOADWARE VERSION: PSWV 100+

INSTALLED LOADWARE PEPS : 3
PAT#  CR #          PATCH REF #     NAME            DATE        FILENAME
00    wi00832543    ISS1:1OF1       DSP1AB04        10/08/2012  DSP1AB04.LW
01    wi00946113    ISS1:1OF1       MGCBBA15        24/04/2012  MGCBBA15.LW
02    wi00890367    ISS1:1OF1       MGCCCD02        24/04/2012  MGCCCD02.LW
```

Avaya Communication Server 1000E call server deplists

```
VERSION 4121
RELEASE 7
ISSUE 50 Q +
DepList 1: core Issue: 01 (created: 2012-07-16 17:52:47 (est)) ALTERED

IN-SERVICE PEPS
PAT# CR #         PATCH REF #    NAME      DATE        FILENAME       SPECINS
000  wi00891626   ISS1:1OF1      p31051_1  11/10/2012  p31051_1.cpl   YES
001  wi00951837   ISS1:1OF1      p31485_1  11/10/2012  p31485_1.cpl   NO
002  wi00946477   ISS1:1OF1      p31426_1  11/10/2012  p31426_1.cpl   NO
003  wi00906163   ISS1:1OF1      p31205_1  11/10/2012  p31205_1.cpl   NO
004  wi00962211   ISS1:1OF1      p31580_1  11/10/2012  p31580_1.cpl   NO
005  wi00877592   ISS1:1OF1      p30880_1  11/10/2012  p30880_1.cpl   NO
006  wi00839134   ISS1:1OF1      p30698_1  11/10/2012  p30698_1.cpl   YES
007  wi00984888   ISS1:1OF1      p31795_1  11/10/2012  p31795_1.cpl   NO
008  wi00868729   ISS1:1OF1      p31163_1  11/10/2012  p31163_1.cpl   NO
009  wi00886321   ISS1:1OF1      p31009_1  11/10/2012  p31009_1.cpl   NO
010  wi00946282   ISS1:1OF1      p31204_1  11/10/2012  p31204_1.cpl   NO
011  wi00841980   ISS1:1OF1      p30618_1  11/10/2012  p30618_1.cpl   NO
012  wi00968448   ISS1:1OF1      p31648_1  11/10/2012  p31648_1.cpl   YES
013  wi00977002   ISS2:1OF1      p30786_2  11/10/2012  p30786_2.cpl   NO
014  wi00843623   ISS1:1OF1      p30731_1  11/10/2012  p30731_1.cpl   YES
015  wi00958776   ISS1:1OF1      p31542_1  11/10/2012  p31542_1.cpl   YES
017  wi00865477   ISS1:1OF1      p30893_1  11/10/2012  p30893_1.cpl   YES
018  wi00879526   ISS1:1OF1      p31007_1  11/10/2012  p31007_1.cpl   NO
019  wi00894243   ISS1:1OF1      p31087_1  11/10/2012  p31087_1.cpl   NO
020  wi00890475   p30952         p31048_1  11/10/2012  p31048_1.cpl   NO
021  WI00927300   ISS1:1OF1      p30999_1  11/10/2012  p30999_1.cpl   NO
022  wi00856991   ISS1:1OF1      p17588_1  11/10/2012  p17588_1.cpl   NO
023  wi00688381   ISS1:1OF1      p30104_1  11/10/2012  p30104_1.cpl   NO
024  wi00881777   ISS1:1OF1      p25747_1  11/10/2012  p25747_1.cpl   NO
025  WI00853473   ISS1:1OF1      p30625_1  11/10/2012  p30625_1.cpl   NO
026  wi00855423   ISS1:1OF1      p31328_1  11/10/2012  p31328_1.cpl   YES
027  wi00943172   ISS1:1OF1      p31402_1  11/10/2012  p31402_1.cpl   NO
```

```
028  wi00865477    ISS1:1OF1    p30898_1  11/10/2012  p30898_1.cpl   YES
029  wi00850521    ISS1:1OF1    p30709_1  11/10/2012  p30709_1.cpl   YES
030  wi00898327    ISS1:1OF1    p31136_1  11/10/2012  p31136_1.cpl   NO
031  wi00871739    ISS1:1OF1    p30856_1  11/10/2012  p30856_1.cpl   NO
032  wi00984178    ISS1:1OF1    p31786_1  11/10/2012  p31786_1.cpl   NO
033  wi00839821    ISS1:1OF1    p30619_1  11/10/2012  p30619_1.cpl   NO
034  wi00854130    ISS1:1OF1    p30443_1  11/10/2012  p30443_1.cpl   NO
035  wi00871969    ISS1:1OF1    p30768_1  11/10/2012  p30768_1.cpl   NO
036  wi00973241    ISS1:1OF1    p31715_1  11/10/2012  p31715_1.cpl   NO
037  wi00946876    ISS1:1OF1    p31430_1  11/10/2012  p31430_1.cpl   NO
038  wi01008943    ISS1:1OF1    p31382_1  11/10/2012  p31382_1.cpl   NO
039  wi00969890    ISS1:1OF1    p31664_1  11/10/2012  p31664_1.cpl   YES
040  wi00937672    ISS1:1OF1    p31276_1  11/10/2012  p31276_1.cpl   NO
041  wi00875425    ISS1:1OF1    p30943_1  11/10/2012  p30943_1.cpl   NO
042  wi00862574    iss1:1of1    p30870_1  11/10/2012  p30870_1.cpl   NO
043  wi00859499    ISS1:1OF1    p30694_1  11/10/2012  p30694_1.cpl   NO
044  wi00925208    ISS1:1OF1    p30986_1  11/10/2012  p30986_1.cpl   NO
045  wi00965285    ISS1:1OF1    p31476_1  11/10/2012  p31476_1.cpl   NO
046  wi00900668    ISS1:1OF1    p30456_1  11/10/2012  p30456_1.cpl   NO
047  wi00967509    ISS1:1OF1    p31294_1  11/10/2012  p31294_1.cpl   NO
048  wi00879322    ISS1:1OF1    p30954_1  11/10/2012  p30954_1.cpl   NO
049  wi00976209    ISS1:1OF1    p31717_1  11/10/2012  p31717_1.cpl   YES
050  wi00956788    ISS1:1OF1    p31638_1  11/10/2012  p31638_1.cpl   NO
051  wi00865477    ISS1:1OF1    p30894_1  11/10/2012  p30894_1.cpl   YES
052  wi00991523    ISS1:1OF1    p31603_1  11/10/2012  p31603_1.cpl   NO
053  wi00865477    ISS1:1OF1    p30892_1  11/10/2012  p30892_1.cpl   YES
054  wi01007604    ISS1:1OF1    p31983_1  11/10/2012  p31983_1.cpl   NO
055  wi00931028    ISS1:1OF1    p31354_1  11/10/2012  p31354_1.cpl   YES
056  wi00932948    ISS1:1OF1    p31077_1  11/10/2012  p31077_1.cpl   NO
057  wi01001911    ISS1:1OF1    p31920_1  11/10/2012  p31920_1.cpl   NO
058  wi00838073    ISS1:1OF1    p30588_1  11/10/2012  p30588_1.cpl   NO
059  wi00852365    ISS1:1OF1    p30707_1  11/10/2012  p30707_1.cpl   NO
060  wi00927321    ISS1:1OF1    p31286_1  11/10/2012  p31286_1.cpl   YES
061  wi00937114    ISS1:1OF1    p31310_1  11/10/2012  p31310_1.cpl   NO
062  wi00877367    ISS1:1OF1    p30534_1  11/10/2012  p30534_1.cpl   NO
063  wi00900096    ISS1:1OF1    p31006_1  11/10/2012  p31006_1.cpl   NO
064  wi00905660    ISS1:1OF1    p27968_1  11/10/2012  p27968_1.cpl   NO
065  wi00925141    ISS1:1OF1    p30802_1  11/10/2012  p30802_1.cpl   NO
066  wi00943748    ISS1:1OF1    p31516_1  11/10/2012  p31516_1.cpl   NO
067  wi00827950    ISS2:1OF1    p30471_2  11/10/2012  p30471_2.cpl   NO
068  wi00930649    ISS1:1OF1    p31570_1  11/10/2012  p31570_1.cpl   NO
069  wi00897279    ISS1:1OF1    p31129_1  11/10/2012  p31129_1.cpl   NO
070  wi00961267    ISS1:1OF1    p30288_1  11/10/2012  p30288_1.cpl   NO
071  wi00936714    ISS1:1OF1    p31379_1  11/10/2012  p31379_1.cpl   NO
072  wi00906022    ISS1:1OF1    p31202_1  11/10/2012  p31202_1.cpl   NO
073  wi00852389    ISS1:1OF1    p30641_1  11/10/2012  p30641_1.cpl   NO
074  wi00857566    ISS1:1OF1    p30766_1  11/10/2012  p30766_1.cpl   NO
075  wi00932204    ISS2:1OF1    p31305_2  11/10/2012  p31305_2.cpl   NO
077  wi00891621    ISS1:1OF1    p31037_1  11/10/2012  p31037_1.cpl   NO
078  wi00957235    ISS1:1OF1    p31798_1  11/10/2012  p31798_1.cpl   NO
079  wi00948274    ISS1:1OF1    p31365_1  11/10/2012  p31365_1.cpl   NO
080  wi00923899    ISS1:1OF1    p31270_1  11/10/2012  p31270_1.cpl   NO
081  wi00856410    ISS1:1OF1    p30749_1  11/10/2012  p30749_1.cpl   NO
082  wi00854415    ISS1:1OF1    p30593_1  11/10/2012  p30593_1.cpl   NO
083  wi00896394    ISS1:1OF1    p30807_1  11/10/2012  p30807_1.cpl   NO
084  wi00826075    ISS1:1OF1    p30452_1  11/10/2012  p30452_1.cpl   NO
085  wi00863876    ISS1:1OF1    p30787_1  11/10/2012  p30787_1.cpl   NO
086  wi00880386    ISS1:1OF1    p30977_1  11/10/2012  p30977_1.cpl   NO
087  wi00840590    ISS1:1OF1    p30767_1  11/10/2012  p30767_1.cpl   NO
088  wi00949627    ISS1:1OF1    p31462_1  11/10/2012  p31462_1.cpl   NO
089  wi00842409    ISS1:1OF1    p30621_1  11/10/2012  p30621_1.cpl   NO
090  wi00865477    ISS1:1OF1    p30896_1  11/10/2012  p30896_1.cpl   YES
091  wi00897096    ISS1:1OF1    p30676_1  11/10/2012  p30676_1.cpl   NO
092  wi00899584    ISS1:1OF1    p30809_1  11/10/2012  p30809_1.cpl   NO
093  wi01007960    ISS1:1OF1    p31965_1  11/10/2012  p31965_1.cpl   NO
094  wi00949273    ISS1:1OF1    p31411_1  11/10/2012  p31411_1.cpl   NO
095  wi00839255    ISS1:1OF1    p30591_1  11/10/2012  p30591_1.cpl   NO
096  wi00945997    ISS1:1OF1    p31641_1  11/10/2012  p31641_1.cpl   NO
097  wi00903369    ISS1:1OF1    p31165_1  11/10/2012  p31165_1.cpl   NO
098  wi00875701    ISS1:1OF1    p30942_1  11/10/2012  p30942_1.cpl   NO
```

099	wi00884699	ISS1:1OF1	p31000_1	11/10/2012	p31000_1.cpl	YES
100	wi00834382	ISS1:1OF1	p30548_1	11/10/2012	p30548_1.cpl	NO
101	wi00960133	ISS2:1OF1	p31557_2	11/10/2012	p31557_2.cpl	NO
102	wi00929140	ISS1:1OF1	p31284_1	11/10/2012	p31284_1.cpl	NO
103	wi00948931	ISS1:1OF1	p31407_1	11/10/2012	p31407_1.cpl	NO
104	wi00887744	ISS2:1OF1	p31026_2	11/10/2012	p31026_2.cpl	NO
105	wi00905600	ISS1:1OF1	p31201_1	11/10/2012	p31201_1.cpl	NO
106	wi00869243	ISS1:1OF1	p30848_1	11/10/2012	p30848_1.cpl	NO
107	WI00854150	ISS1:1OF1	p30468_1	11/10/2012	p30468_1.cpl	NO
108	wi00897176	ISS1:1OF1	p30418_1	11/10/2012	p30418_1.cpl	NO
109	wi00903381	ISS1:1OF1	p30421_1	11/10/2012	p30421_1.cpl	NO
110	wi00950575	ISS1:1OF1	p31724_1	11/10/2012	p31724_1.cpl	NO
111	wi00908598	ISS1:1OF1	p31235_1	11/10/2012	p31235_1.cpl	NO
112	wi00903437	ISS1:1OF1	p31167_1	11/10/2012	p31167_1.cpl	NO
113	wi00900766	ISS1:1OF1	p31159_1	11/10/2012	p31159_1.cpl	NO
114	wi00946558	ISS1:1OF1	p31358_1	11/10/2012	p31358_1.cpl	NO
115	wi00932958	ISS1:1OF1	p31115_1	11/10/2012	p31115_1.cpl	NO
116	wi00895090	ISS1:1OF1	p31105_1	11/10/2012	p31105_1.cpl	NO
117	wi00824257	ISS1:1OF1	p30447_1	11/10/2012	p30447_1.cpl	NO
118	wi00895181	ISS1:1OF1	p31106_1	11/10/2012	p31106_1.cpl	NO
119	WI00928455	ISS1:1OF1	p31297_1	11/10/2012	p31297_1.cpl	NO
120	wi00832106	ISS1:1OF1	p30550_1	11/10/2012	p30550_1.cpl	NO
121	wi00953900	ISS1:1OF1	p31494_1	11/10/2012	p31494_1.cpl	NO
122	wi00942734	ISS1:1OF1	p31409_1	11/10/2012	p31409_1.cpl	NO
123	wi00986337	ISS1:1OF1	p31803_1	11/10/2012	p31803_1.cpl	NO
124	wi00882293	ISS1:1OF1	p31010_1	11/10/2012	p31010_1.cpl	NO
125	WI00843571	ISS1:1OF1	p30627_1	11/10/2012	p30627_1.cpl	NO
126	wi00835294	ISS1:1OF1	p30565_1	11/10/2012	p30565_1.cpl	NO
127	WI00836292	ISS1:1OF1	p30554_1	11/10/2012	p30554_1.cpl	NO
128	wi00969581	ISS1:1OF1	p31661_1	11/10/2012	p31661_1.cpl	YES
129	wi00921295	ISS1:1OF1	p31265_1	11/10/2012	p31265_1.cpl	NO
130	wi00964006	ISS1:1OF1	p31595_1	11/10/2012	p31595_1.cpl	YES
131	WI00836334	ISS1:1OF1	p30481_1	11/10/2012	p30481_1.cpl	NO
132	wi00858335	ISS1:1OF1	p30819_1	11/10/2012	p30819_1.cpl	NO
133	wi00859123	ISS1:1OF1	p30648_1	11/10/2012	p30648_1.cpl	NO
134	wi00959820	ISS1:1OF1	p31562_1	11/10/2012	p31562_1.cpl	NO
135	wi00905297	ISS1:1OF1	p31195_1	11/10/2012	p31195_1.cpl	NO
136	wi00907697	ISS1:1OF1	p31227_1	11/10/2012	p31227_1.cpl	NO
137	wi00951427	ISS1:1OF1	p31478_1	11/10/2012	p31478_1.cpl	NO
138	wi00883604	ISS1:1OF1	p30973_1	11/10/2012	p30973_1.cpl	NO
139	wi00962955	ISS1:1OF1	p31585_1	11/10/2012	p31585_1.cpl	NO
140	wi00860279	ISS1:1OF1	p30789_1	11/10/2012	p30789_1.cpl	NO
141	wi00909476	ISS1:1OF1	p31340_1	11/10/2012	p31340_1.cpl	NO
142	wi00925218	ISS1:1OF1	p30675_1	11/10/2012	p30675_1.cpl	NO
143	wi00836182	ISS1:1OF1	p30450_1	11/10/2012	p30450_1.cpl	NO
144	wi00841273	ISS1:1OF1	p30713_1	11/10/2012	p30713_1.cpl	NO
145	WI00889786	ISS1:1OF1	p30750_1	11/10/2012	p30750_1.cpl	NO
146	wi00894443	ISS1:1OF1	p31093_1	11/10/2012	p31093_1.cpl	NO
147	wi00896420	ISS1:1OF1	p30867_1	11/10/2012	p30867_1.cpl	NO
148	wi00971029	ISS1:1OF1	p31794_1	11/10/2012	p31794_1.cpl	NO
149	wi00955753	ISS1:1OF1	p31733_1	11/10/2012	p31733_1.cpl	NO
150	wi00968531	ISS1:1OF1	p31645_1	11/10/2012	p31645_1.cpl	NO
151	wi00930864	ISS1:1OF1	p31325_1	11/10/2012	p31325_1.cpl	NO
152	wi00957252	ISS1:1OF1	p31530_1	11/10/2012	p31530_1.cpl	NO
153	wi00880836	ISS1:1OF1	p30976_1	11/10/2012	p30976_1.cpl	NO
154	wi00959457	ISS1:1OF1	p31551_1	11/10/2012	p31551_1.cpl	NO
155	wi00896680	ISS1:1OF1	p30357_1	11/10/2012	p30357_1.cpl	NO
156	wi00856702	ISS1:1OF1	p30573_1	11/10/2012	p30573_1.cpl	NO
157	wi00897082	ISS1:1OF1	p31124_1	11/10/2012	p31124_1.cpl	NO
158	wi00853178	ISS1:1OF1	p30719_1	11/10/2012	p30719_1.cpl	NO
159	wi00938555	ISS1:1OF1	p30881_1	11/10/2012	p30881_1.cpl	YES
160	WI00839794	ISS1:1OF1	p28647_1	11/10/2012	p28647_1.cpl	NO
161	wi00965838	ISS1:1OF1	p31623_1	11/10/2012	p31623_1.cpl	NO
162	wi00977393	ISS1:1OF1	p31744_1	11/10/2012	p31744_1.cpl	YES
163	wi00959284	ISS1:1OF1	p31531_1	11/10/2012	p31531_1.cpl	NO
164	wi00968353	ISS1:1OF1	p31412_1	11/10/2012	p31412_1.cpl	NO
165	wi00998121	ISS1:1OF1	p31897_1	11/10/2012	p31897_1.cpl	NO
166	wi00968157	ISS1:1OF1	p31637_1	11/10/2012	p31637_1.cpl	NO
167	wi00967510	ISS1:1OF1	p31147_1	11/10/2012	p31147_1.cpl	NO
168	wi00949410	ISS1:1OF1	p31248_1	11/10/2012	p31248_1.cpl	NO

169	wi00969039	ISS1:1OF1	p31643_1	11/10/2012	p31643_1.cpl	NO
170	wi00959463	ISS1:1OF1	p31528_1	11/10/2012	p31528_1.cpl	NO
171	wi00983505	ISS1:1OF1	p31758_1	11/10/2012	p31758_1.cpl	NO
172	wi00924886	ISS1:1OF1	p31062_1	11/10/2012	p31062_1.cpl	YES
173	wi00969208	ISS1:1OF1	p31656_1	11/10/2012	p31656_1.cpl	NO
174	wi00974272	ISS1:1OF1	p31690_1	11/10/2012	p31690_1.cpl	YES
175	wi00988285	ISS1:1OF1	p31824_1	11/10/2012	p31824_1.cpl	NO
176	wi00975659	ISS1:1OF1	p31707_1	11/10/2012	p31707_1.cpl	NO
177	wi00960809	ISS1:1OF1	p31564_1	11/10/2012	p31564_1.cpl	NO
178	wi00936935	ISS1:1OF1	p31362_1	11/10/2012	p31362_1.cpl	NO
179	wi01012229	ISS1:1OF1	p31993_1	11/10/2012	p31993_1.cpl	NO
180	wi00989828	ISS1:1OF1	p31836_1	11/10/2012	p31836_1.cpl	NO
182	wi00985760	ISS1:1OF1	p31913_1	11/10/2012	p31913_1.cpl	NO
183	wi01003896	ISS1:1OF1	p31631_1	11/10/2012	p31631_1.cpl	NO
184	wi00978064	ISS1:1OF1	p31760_1	11/10/2012	p31760_1.cpl	NO
185	wi00996889	ISS1:1OF1	p31933_1	11/10/2012	p31933_1.cpl	NO
186	wi00991907	iss1:1of1	p31907_1	11/10/2012	p31907_1.cpl	NO
187	wi01005653	ISS1:1OF1	p31952_1	11/10/2012	p31952_1.cpl	NO
188	wi01005513	ISS1:1OF1	p31951_1	11/10/2012	p31951_1.cpl	NO
189	wi00967512	ISS1:1OF1	p31384_1	11/10/2012	p31384_1.cpl	NO
190	wi01003814	ISS1:1OF1	p31940_1	11/10/2012	p31940_1.cpl	NO
191	wi00984652	ISS1:1OF1	p31792_1	11/10/2012	p31792_1.cpl	NO
192	wi00967514	ISS1:1OF1	p31351_1	11/10/2012	p31351_1.cpl	NO
193	wi00978818	ISS1:1OF1	p31919_1	11/10/2012	p31919_1.cpl	NO
194	WI00980321	ISS1:1OF1	p31912_1	11/10/2012	p31912_1.cpl	YES
195	wi00999802	ISS1:1OF1	p31577_1	11/10/2012	p31577_1.cpl	NO
196	wi01008316	ISS1:1OF1	p32026_1	11/10/2012	p32026_1.cpl	YES
197	wi01003384	ISS1:1OF1	p31479_1	11/10/2012	p31479_1.cpl	NO
198	wi01003999	ISS1:1OF1	p31946_1	11/10/2012	p31946_1.cpl	YES
199	wi01011078	ISS1:1OF1	p31996_1	11/10/2012	p31996_1.cpl	NO
200	wi01016398	ISS1:1OF1	p32019_1	11/10/2012	p32019_1.cpl	NO
201	wi00973270	ISS1:1OF1	p31751_1	11/10/2012	p31751_1.cpl	NO
202	wi00981711	ISS1:1OF1	p31766_1	11/10/2012	p31766_1.cpl	NO
203	wi00977978	ISS1:1OF1	p31831_1	11/10/2012	p31831_1.cpl	NO
204	wi00992974	ISS1:1OF1	p31889_1	11/10/2012	p31889_1.cpl	NO
205	wi00980476	ISS1:1OF1	p31387_1	11/10/2012	p31387_1.cpl	NO
206	wi01008106	ISS1:1OF1	p31861_1	11/10/2012	p31861_1.cpl	NO
207	wi00906350	ISS1:1OF1	p31219_1	11/10/2012	p31219_1.cpl	NO
208	wi01006063	ISS1:1OF1	p31957_1	11/10/2012	p31957_1.cpl	NO
209	wi00971980	ISS1:1OF1	p31863_1	11/10/2012	p31863_1.cpl	NO
210	wi01020959	ISS1:1OF1	p32062_1	11/10/2012	p32062_1.cpl	NO
211	wi01011537	ISS1:1OF1	p32024_1	11/10/2012	p32024_1.cpl	NO
212	wi01008505	ISS1:1OF1	p31968_1	11/10/2012	p31968_1.cpl	NO
213	wi01014835	ISS1:1OF1	p32015_1	11/10/2012	p32015_1.cpl	NO
214	wi00983007	ISS1:1OF1	p31778_1	11/10/2012	p31778_1.cpl	YES
215	wi00987424	ISS1:1OF1	p31815_1	11/10/2012	p31815_1.cpl	NO
216	wi00997559	ISS1:1OF1	p31898_1	11/10/2012	p31898_1.cpl	NO
217	wi01012638	ISS1:1OF1	p32008_1	11/10/2012	p32008_1.cpl	NO
218	wi00985153	ISS1:1OF1	p31859_1	11/10/2012	p31859_1.cpl	NO
219	wi00979591	ISS1:1OF1	p31746_1	11/10/2012	p31746_1.cpl	NO
220	wi00978892	ISS1:1OF1	p31894_1	11/10/2012	p31894_1.cpl	NO
221	wi00996639	ISS1:1OF1	p31886_1	11/10/2012	p31886_1.cpl	NO
222	wi00994044	ISS1:1OF1	p31871_1	11/10/2012	p31871_1.cpl	NO
223	wi00991892	ISS1:1OF1	p31853_1	11/10/2012	p31853_1.cpl	NO
224	wi00974856	ISS1:1OF1	p31823_1	11/10/2012	p31823_1.cpl	NO
225	wi00993377	ISS1:1OF1	p31860_1	11/10/2012	p31860_1.cpl	NO
226	wi00982566	ISS1:1OF1	p31774_1	11/10/2012	p31774_1.cpl	NO
227	wi00993743	ISS1:1OF1	p31865_1	11/10/2012	p31865_1.cpl	NO
228	wi00944019	ISS1:1OF1	p31874_1	11/10/2012	p31874_1.cpl	NO
229	wi00998328	ISS1:1OF1	p31899_1	11/10/2012	p31899_1.cpl	NO
230	wi01008188	ISS1:1OF1	p32020_1	11/10/2012	p32020_1.cpl	NO
231	wi00987089	ISS1:1OF1	p31809_1	11/10/2012	p31809_1.cpl	NO
232	wi00979414	ISS1:1OF1	p31748_1	11/10/2012	p31748_1.cpl	YES
233	wi01006811	ISS1:1OF1	p31967_1	11/10/2012	p31967_1.cpl	YES
234	wi01012289	p31274	p31999_1	11/10/2012	p31999_1.cpl	NO
235	wi00971209	ISS1:1OF1	p31750_1	11/10/2012	p31750_1.cpl	NO
236	wi00997316	ISS1:1OF1	p31870_1	11/10/2012	p31870_1.cpl	NO
237	wi00990993	ISS1:1OF1	p31825_1	11/10/2012	p31825_1.cpl	NO
238	wi00977436	ISS1:1OF1	p31834_1	11/10/2012	p31834_1.cpl	NO
239	wi01001938	ISS1:1OF1	p31921_1	11/10/2012	p31921_1.cpl	YES

```
240  wi01012423      ISS1:1OF1       p26155_1  11/10/2012  p26155_1.cpl   NO
241  wi01010472      ISS1:1OF1       p31975_1  11/10/2012  p31975_1.cpl   NO
242  wi01000796      ISS1:1OF1       p31800_1  11/10/2012  p31800_1.cpl   NO
243  wi00981928      ISS1:1OF1       p31869_1  11/10/2012  p31869_1.cpl   NO
244  wi00992921      ISS1:1OF1       p31878_1  11/10/2012  p31878_1.cpl   NO
245  wi01001588      ISS1:1OF1       p31976_1  11/10/2012  p31976_1.cpl   NO
246  wi00976951      ISS1:1OF1       p30112_1  11/10/2012  p30112_1.cpl   NO
MDP>LAST SUCCESSFUL MDP REFRESH :2012-10-02 13:46:39(Local Time)
MDP>USING DEPLIST ZIP FILE DOWNLOADED :2012-08-20 11:29:05(est)
```

Avaya Communication Server 1000E signaling server service updates

```
In System service updates: 33
PATCH#  IN_SERVICE   DATE       SPECINS   REMOVABLE   NAME
3       Yes          20/01/12   NO        YES         cs1000-dbcom-7.50.17-02.i386.000
4       Yes          18/12/12   NO        yes         tzdata-2011h-2.el5.i386.000
5       Yes          20/01/12   NO        YES         cs1000-shared-pbx-7.50.17.16-1.i386.000
6       Yes          20/01/12   NO        YES         cs1000-kcv-7.50.17.16-1.i386.000
7       Yes          20/01/12   NO        YES         cs1000-nrsmWebService-7.50.17.16-1.i386.000
9       Yes          02/10/12   YES       YES         cs1000-baseWeb-7.50.17.16-2.i386.000
10      Yes          20/01/12   NO        YES         cs1000-ipsec-7.50.17.16-1.i386.000
11      Yes          02/10/12   NO        yes         avaya-cs1000-cnd-4.0.20-00.i386.000
12      Yes          02/10/12   NO        YES         cs1000-pd-7.50.17.16-1.i386.000
13      Yes          02/10/12   NO        YES         cs1000-ncs-7.50.17.16-1.i386.000
14      Yes          20/01/12   NO        YES         ipsec-tools-0.6.5-14.el5.3_avaya_1.i386.000
15      Yes          20/01/12   NO        YES         spiritAgent-6.1-1.0.0.108.208.i386.000
16      No           18/12/12   NO        YES         cs1000-tps-7.50.17.16-24.i386.000
17      Yes          02/10/12   NO        YES         cs1000-EmCentralLogic-7.50.17.16-2.i386.000
20      Yes          02/10/12   NO        YES         cs1000-cs1000WebService_6-0-7.50.17.16-
1.i386.000
21      Yes          02/10/12   NO        YES         cs1000-mscMusc-7.50.17.16-11.i386.000
22      Yes          02/10/12   NO        YES         cs1000-mscAnnc-7.50.17.16-10.i386.000
23      No           18/12/12   NO        YES         cs1000-sps-7.50.17.16-10.i386.000
24      Yes          27/03/12   NO        YES         cs1000-mscTone-7.50.17.16-1.i386.000
25      No           18/12/12   NO        YES         cs1000-ftrpkg-7.50.17.16-11.i386.000
26      Yes          18/12/12   NO        YES         cs1000-dmWeb-7.50.17.16-6.i386.000
27      Yes          02/10/12   NO        YES         cs1000-csoneksvrmgr-7.50.17.16-1.i386.000
28      No           18/12/12   NO        YES         cs1000-dbcom-7.50.17.16-1.i386.000
29      No           18/12/12   NO        YES         cs1000-vtrk-7.50.17.16-131.i386.001
30      Yes          27/03/12   NO        YES         cs1000-sps-7.50.17.16-4.i386.000
31      Yes          18/12/12   NO        YES         cs1000-linuxbase-7.50.17.16-13.i386.000
32      Yes          18/12/12   NO        YES         cs1000-mscAttn-7.50.17.16-3.i386.000
35      Yes          02/10/12   YES       YES         cs1000-nrsm-7.50.17.16-4.i386.000
36      Yes          02/10/12   NO        YES         cs1000-csmWeb-7.50.17.16-6.i386.000
37      Yes          02/10/12   NO        YES         cs1000-mscConf-7.50.17.16-1.i386.000
38      Yes          02/10/12   NO        YES         cs1000-emWeb_6-0-7.50.17.16-34.i386.000
40      Yes          02/10/12   NO        YES         cs1000-Jboss-Quantum-7.50.17.16-30.i386.000
42      Yes          02/10/12   NO        YES         cs1000-emWebLocal_6-0-7.50.17.16-3.i386.000
```

Avaya 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]
   cnd                         n/a         [patched]
   lhmonitor                   7.50.17
   baseAppUtils                7.50.17     [patched]
   dfoTools                    7.50.17
   nnnm                        7.50.17
   cppmUtil                    7.50.17
   oam-logging                 7.50.17     [patched]
```

```
   dmWeb                        n/a         [patched]
   baseWeb                      n/a         [patched]
   ipsec                        n/a         [patched]
   Snmp-Daemon-TrapLib          7.50.17     [patched]
   ISECSH                       7.50.17
   patchWeb                     n/a
   EmCentralLogic               n/a         [patched]
Application configuration: CS+SS+NRS+EM
Packages:
CS+SS+NRS+EM
Configuration version:     7.50.17-00
   cs                           7.50.17
   dbcom                        7.50.17.16  [patched]
   cslogin                      7.50.17
   sigServerShare               7.50.17     [patched]
   csv                          7.50.17
   tps                          7.50.17.16
   vtrk                         7.50.17.16
   pd                           7.50.17.16  [patched]
   sps                          7.50.17.16  [patched]
   ncs                          7.50.17.16  [patched]
   gk                           7.50.17
   nrsm                         7.50.17     [patched]
   nrsmWebService               7.50.17     [patched]
   managedElementWebService     7.50.17
   EmConfig                     7.50.17
   emWeb_6-0                    7.50.17     [patched]
   emWebLocal_6-0               7.50.17     [patched]
   csmWeb                       7.50.17     [patched]
   bcc                          7.50.17
   ftrpkg                       n/a
   cs1000WebService_6-0         7.50.17     [patched]
   mscAnnc                      7.50.17.16  [patched]
   mscAttn                      7.50.17.16  [patched]
   mscConf                      7.50.17.16  [patched]
   mscMusc                      7.50.17.16  [patched]
   mscTone                      7.50.17.16  [patched]
```

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.