Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Communication Server 1000E R7.5, Avaya Aura® Session Manager R6.1 and Avaya Session Border Controller Advanced for Enterprise R4.0.5 to support Frontier SIP Trunk Service – Issue 1.1

Abstract

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between Frontier SIP Trunk service and an Avaya SIP enabled Enterprise Solution. The Avaya solution consists of Avaya Session Border Controller Advanced for Enterprise, Avaya Aura® Session Manager and Avaya Communication Server 1000E. Frontier Communications is a member of the DevConnect Service Provider program.

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

1. Introduction

These Application Notes describe the steps used to configure Session Initiation Protocol (SIP) trunking between Frontier SIP Trunk Service and an Avaya SIP-enabled Enterprise Solution. The Avaya solution consists of Avaya Session Border Controller Advanced for Enterprise, Avaya Aura® Session Manager and Avaya Communication Server 1000E (CS1000E). Customers using this Avaya SIP-enabled enterprise solution with Frontier SIP Trunk Service are able to place and receive PSTN calls via a dedicated Internet connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks. This approach generally results in lower cost for the Enterprise customer.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using an Avaya SIP telephony solution consisting of CS1000E, Session Manager and Session Border Controller. The enterprise site was configured to use the SIP Trunk service provided by Frontier.

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 calls to the enterprise site from the PSTN routed to the DDI numbers assigned by Frontier
- Incoming PSTN calls made to SIP, Unistim and Digital telephones at the enterprise
- Outgoing calls from the enterprise site completed via Frontier to PSTN destinations
- Outgoing calls from the enterprise to the PSTN made from SIP, Unistim and Digital telephones
- Inbound and outbound PSTN calls to/from the Avaya one-X® Communicator soft phone.
- Calls using the G.711MU and G.729 codecs supported by Frontier
- G729 annex b (silence suppression) is not supported by Frontier's SIP Trunk Service and thus was not tested.
- DTMF transmission using RFC 2833 with successful Voice Mail/IVR navigation for 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
- Transmission and response of SIP OPTIONS messages sent by Frontier requiring Avaya response and sent by Avaya requiring Frontier response

2.2. Test Results

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

- No inbound toll free numbers were tested as none were available from the Service Provider
- No Emergency Services numbers tested as test calls to these numbers should be pre-arranged with the Operator
- T.38 Fax is not supported by Frontier. G.711MU fax was tested but is not supported by Avaya
- Outbound blind transfer calls to the PSTN needs patch MPLR30253 applied in order to hear ring back tone at the calling party when the call is being transferred. Note patch MPLR30253 is not generally available but can be obtained via the Avaya Technical Support Case request process

2.3. Support

For technical support on Frontier products please visit the website at www.frontier.com for contact an authorized Frontier representative.

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an Enterprise site connected to the Frontier SIP Trunk Service. Located at the Enterprise site is a Session Border Controller, Session Manager and CS1000E. Endpoints are Avaya 1140 series IP telephones, Avaya 1200 series (not shown in **Figure 1**) IP telephones (with Unistim and SIP firmware), Avaya IP Softphones (SMC3456, 2050 and Avaya 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.

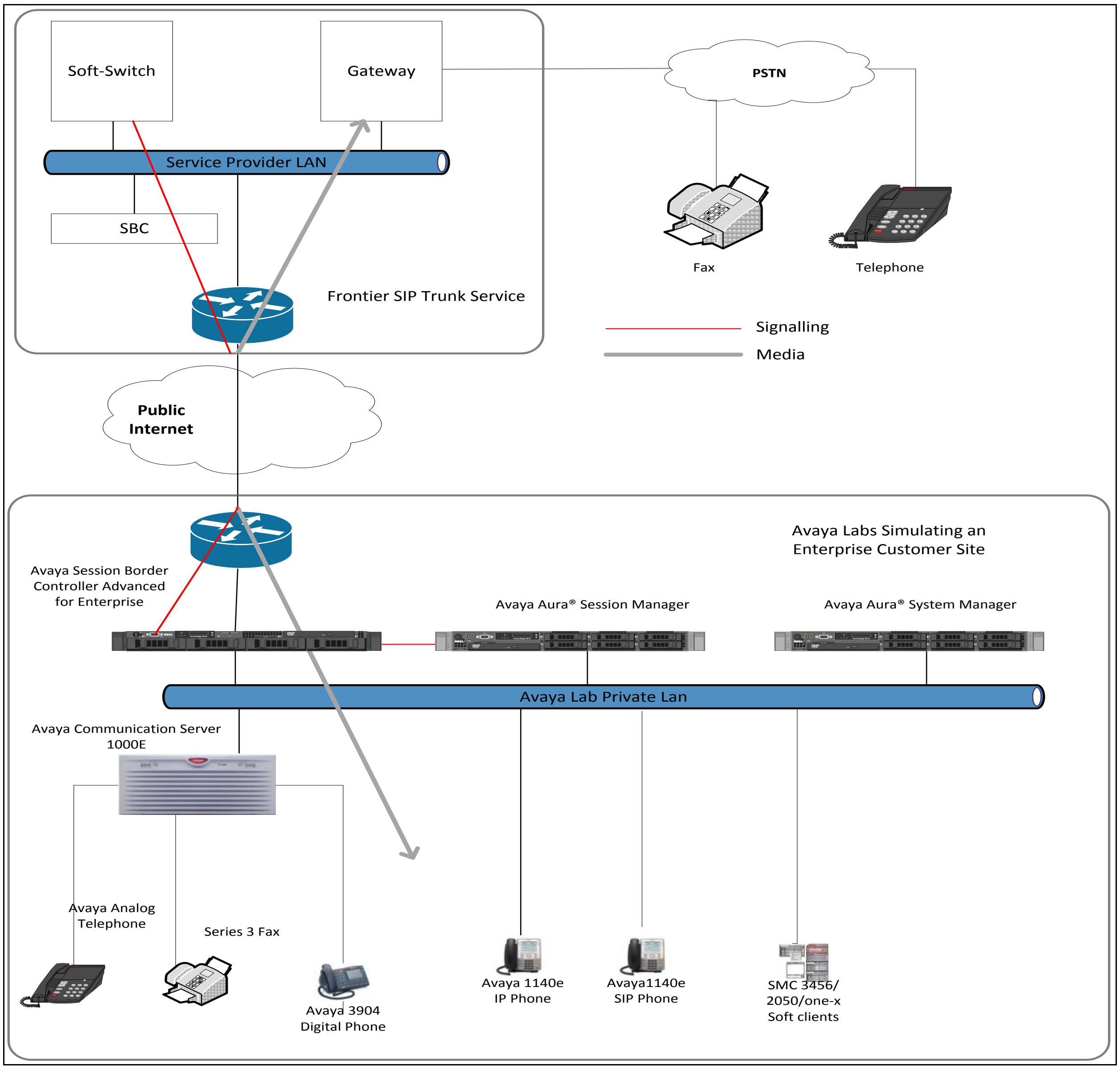


Figure 1: Test Setup Frontier SIP Trunk Service to Avaya Enterprise

4. Equipment and Software Validated

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

Equipment	Software
Avaya S8800 Server	Avaya Aura® Session Manager R6.1 Service Pack 5 (6.1.4.0.614005)
Avaya S8800 Server	Avaya Aura® System Manager R6.1 Service Pack 5 (6.1.8.1.1551)
Dell R310 Server running Avaya Session Border Controller Advanced for Enterprise	Avaya Session Border Controller Advanced for Enterprise R4.0.5.Q02
Avaya Communication Server 1000E running on CP+PM server as co-resident configuration	Avaya Communication Server 1000E R7.5 Version 7.50.17 Deplist: CPL_X21_07_50Q All CS1000E patches listed in **Appendix A**
Avaya Communication Server 1000E Media Gateway	CSP Version: MGCC CD01 MSP Version: MGCM AB01 APP Version: MGCA BA07 FPGA Version: MGCF AA18 BOOT Version: MGCB BA07 DSP1 Version: DSP1 AB04
Avaya 1140e and 1230 Unistim Telephones	FW: 0625C8A
Avaya 1140e and 1230 SIP Telephones	FW: 04.01.13.00.bin
Avaya SMC 3456	Version 2.6 build 57666
Avaya Analog Telephone	N/A
Avaya M3904 Digital Telephone	N/A
FRONTIER Equipment	**Software**
Metaswitch	version 7.3.035
Acme Packet 3820 NET-NET	version 6.2m3p8

5. Configure Avaya Communication Server 1000E

This section describes the steps for configuring Communication Server 1000E for SIP Trunking. SIP trunks are established between Communication Server 1000E and Session Manager. These SIP trunks will carry SIP Signalling associated with the Frontier SIP Trunk Service. For incoming calls, the Session Manager receives SIP messages from the SBC and directs the incoming SIP messages to Communication Server 1000E. Once the 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 automatic 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 Session Border Controller at the enterprise site that then sends the SIP messages to Frontier'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. **Appendix A** has a list of all CS1000E patches, deplist and service packs loaded on the system.

5.1. Logging into the Avaya Communication Server 1000E

Log in using SSH to the ELAN ip address of the Call Server using a user with correct privileges. Once logged in, type **csconsole,** 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 Frontier'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.

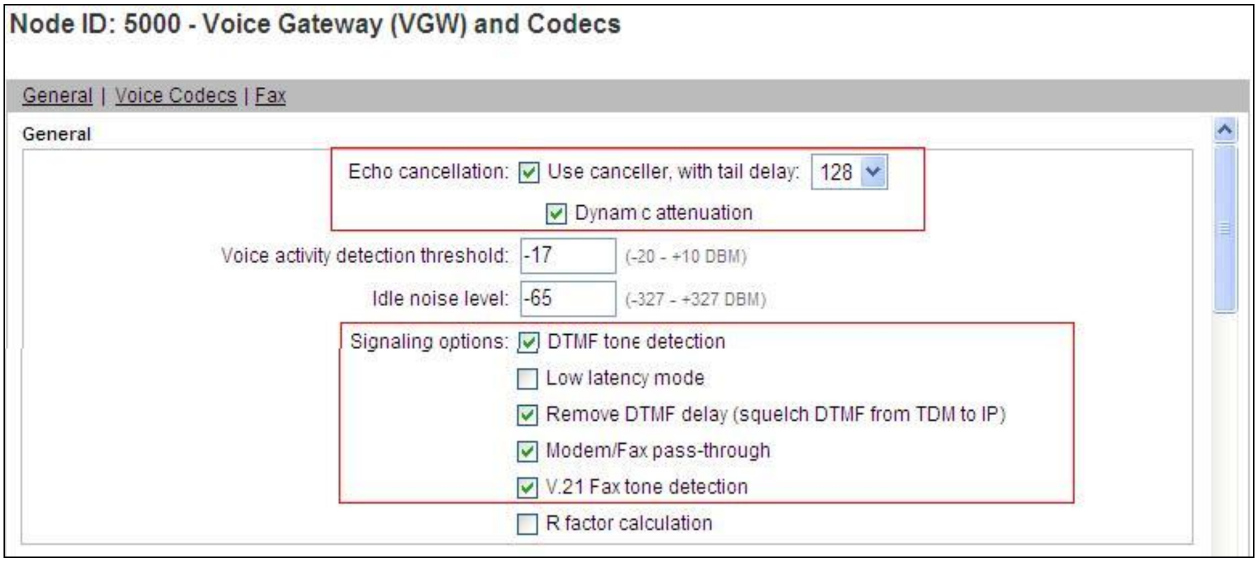
```
Load Overlay 22
req: SLT

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

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

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

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

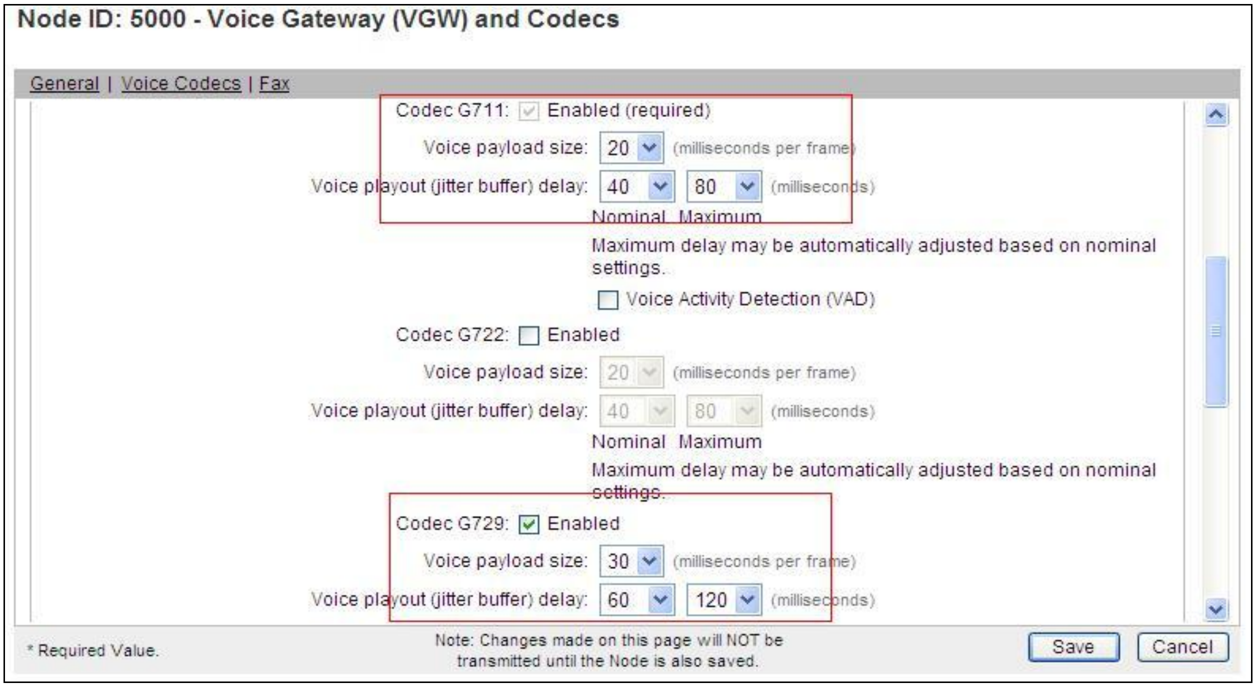
```
Load Overlay 21
REQ: PRT
TYPE: net
TYPE NET_DATA
CUST 0

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

Frontier's SIP Trunk service supports G.711MU and G.729 voice codecs. Using the Communication Server 1000E element manager sidebar, navigate to the **IP Network → IP Telephony Nodes → Node Details → Voice Gateway (VGW) and Codecs** property page and configure the Communication Server 1000E General codec settings as shown in the screenshot below. The values highlighted are required for correct operation; most of the options are turned on by default but its good practice to ensure that they are set as shown below.

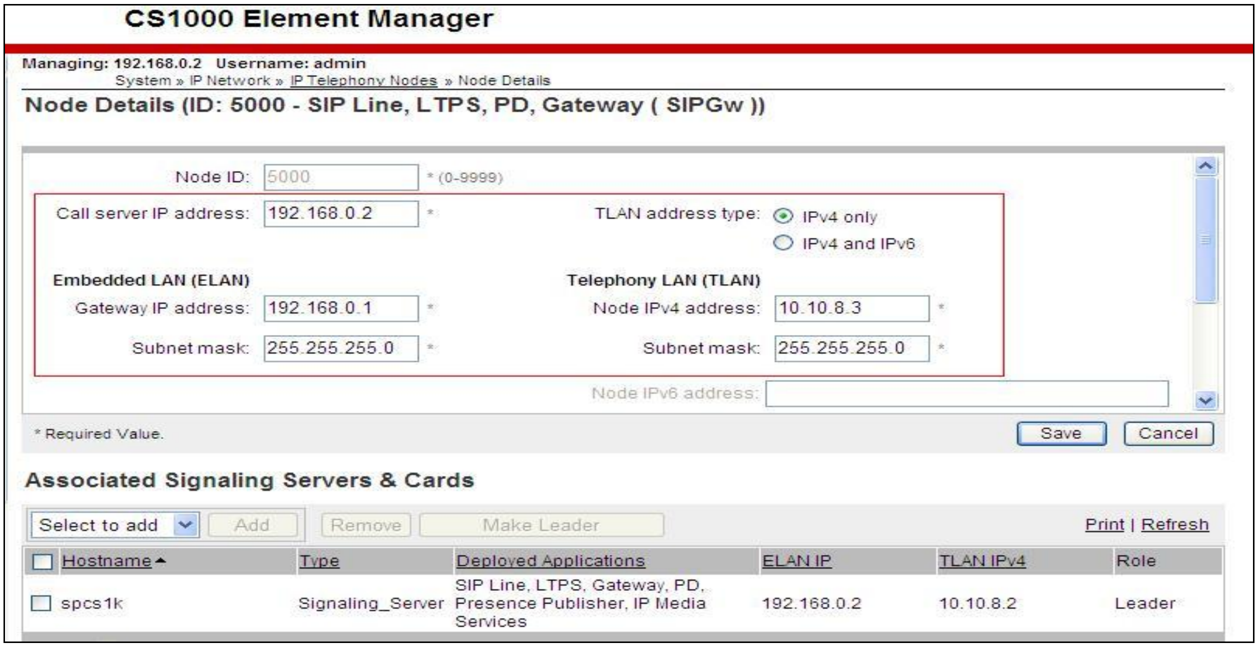


Next, scroll down and configure the CS1000E to use **Codec G.711 and G.729**. Default values were configured. This aligns with what Frontier support on their SIP network.



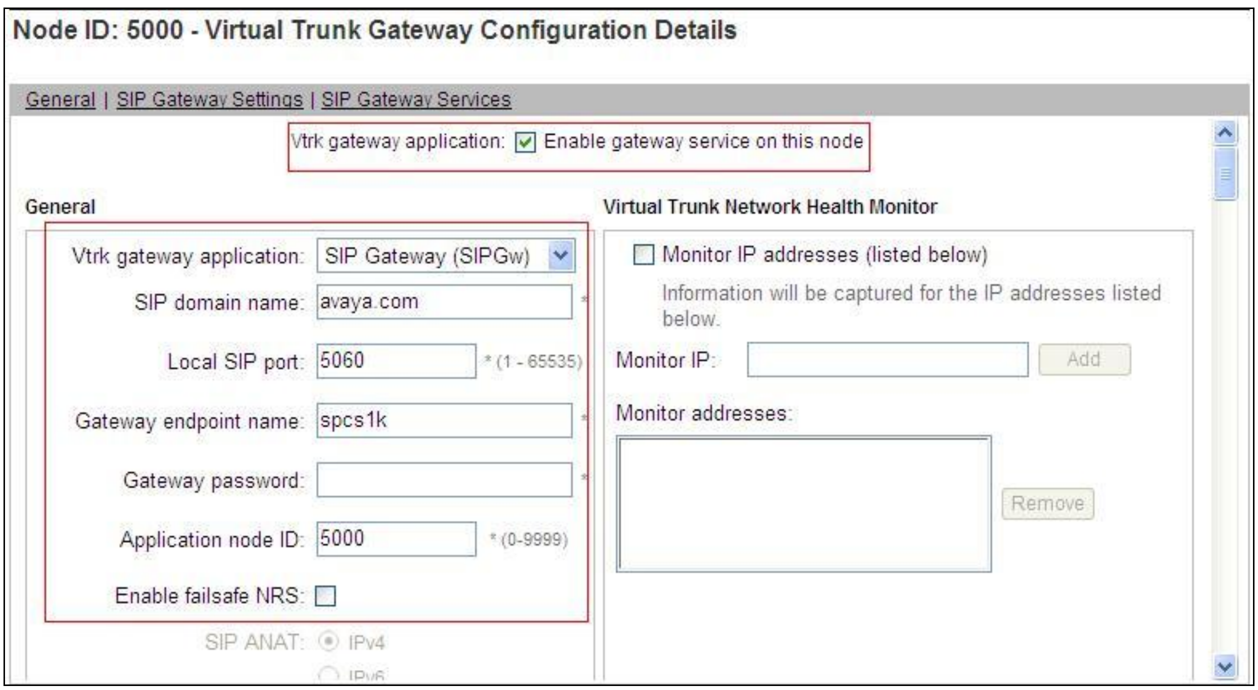
5.4. Virtual Trunk Gateway Configuration

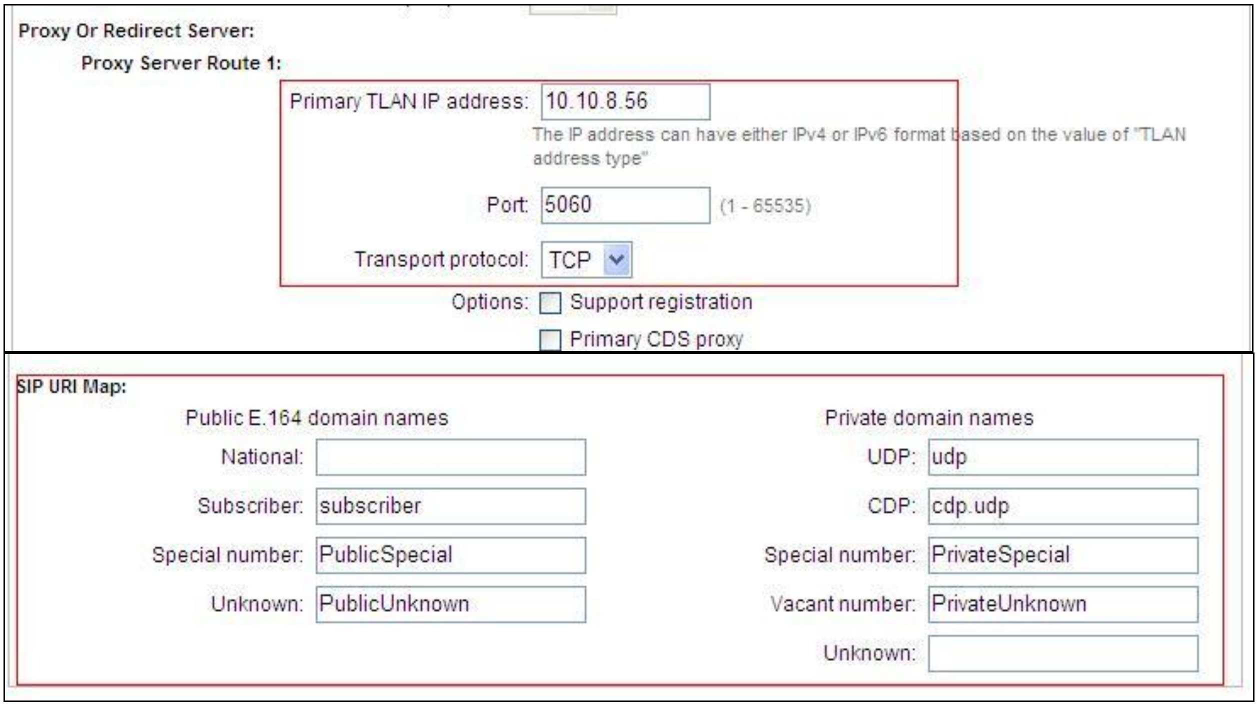
Use Communication Server 1000E Element Manager to configure the system node properties. Navigate to the **System → IP Networks → IP Telephony Nodes → Node Details** and verify the highlighted section is completed with the correct IP addresses and subnet masks of the Node. At this stage the call server has an ip address and so too does the signalling server. The Node IPv4 address 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 CS1000E it is the Node IPv4 address that is used (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**
- **SIP domain name:** The SIP Domain Name is the SIP Service Domain. The SIP Domain Name configured in the Signaling Server properties must match the Service Domain name configured in the Session Manager, 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 **5000**
- **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 E.164 - National** and **Private - Unknown** are left blank. All other fields in the SIP URI Map are left with default values




Proxy Or Redirect Server:
Proxy Server Route 1:
Primary TLAN IP address: 10.10.8.56
The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"
Port: 5060 (1 - 65535)
Transport protocol: TCP
Options: Support registration
Primary CDS proxy
SIP URI Map:
Public E.164 domain names
National:
Subscriber: subscriber
Special number: PublicSpecial
Unknown: PublicUnknown
Private domain names
UDP: udp
CDP: cdp.udp
Special number: PrivateSpecial
Vacant number: PrivateUnknown
Unknown:

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 Frontier's SIP Trunk Service. Five separate steps are required to configure Communication Server 1000E virtual trunks:

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

The following is an example DCH configuration for SIP trunks. **Load Overlay 17** at the Communication Server 1000E system terminal and enter the following values. The highlighted entries are required for correct SIP trunk operation. Exit overlay 17 when completed.

```
Load Overlay 17
ADAN     DCH 10
  CTYP DCIP
  DES  VIR_TRK
  USR  ISLD
  ISLM 4000
  SSRC 1800
  OTBF 32
  NASA YES
  IFC  SL1
  CNEG 1
  RLS  ID  5
  RCAP ND2
  MBGA NO
  H323
    OVLR NO
    OVLS NO
```

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

```
Load Overlay 16
TYPE: RDB
CUST 00
ROUT 100
TYPE RDB
CUST 00
ROUT 100
DES  VIR_TRK
TKTP TIE
NPID_TBL_NUM   0
ESN  NO
RPA  NO
CNVT NO
SAT  NO
RCLS EXT
VTRK YES
ZONE 00020
PCID SIP
CRID NO
NODE 5000
DTRK NO
ISDN YES
    MODE ISLD
    DCH  10
    IFC  SL1
    PNI  00001
    NCNA YES
    NCRD YES
    TRO  NO
    FALT NO
    CTYP UKWN
    INAC NO
    ISAR NO
    DAPC NO
MBXR NO
MBXOT NPA
MBXT 0
PTYP ATT
CNDP UKWN
AUTO NO
DNIS NO
DCDR NO
ICOG IAO
SRCH LIN
TRMB YES
STEP
```

```
ACOD 1600
TCPP NO
PII NO
AUXP NO
TARG
CLEN 1
BILN NO
OABS
INST
IDC  YES
DCNO 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 **Load 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.

```
Load Overlay 14
new 30
TN   160 0 0 0
DATE
PAGE
DES  VIR_TRK
TN   160 0 00 00  VIRTUAL
TYPE IPTI
CUST 0
XTRK VTRK
ZONE 0020
TIMP 600
BIMP 600
AUTO_BIMP NO
NMUS NO
TRK  ANLG
NCOS 0
RTMB 100 1
CHID 1
TGAR 1
STRI/STRO WNK WNK
SUPN YES
AST  NO
IAPG 0
CLS  TLD DTN CND ECD WTA LPR APN THFD XREP SPCD MSBT
     P10 NTC
TKID
AACR NO
```

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

Load Overlay 86 **new** CUST 0 FEAT rlb **RLI 24** ELC NO ENTR 0 LTER NO **ROUT 100** TOD 0 ON 1 ON 2 ON 3 ON 4 ON 5 ON 6 ON 7 ON VNS NO SCNV NO CNV NO EXP NO FRL 0 DMI 0 CTBL 0 ISDM 0	FCI 0 FSNI 0 BNE NO DORG NO SBOC NRR PROU 1 IDBB DBD IOHQ NO OHQ NO CBQ NO ISET 0 NALT 5 MFRL 0 OVLL 0

Next, configure Special Prefix Number(s) (SPN) which users will dial to reach PSTN numbers. Use the Communication Server 1000E system terminal and overlay 90. The following are some example SPN entries used. The highlighted **RLI** value previously configured in overlay 86 is used as the Route List Index (**RLI**), this is the default PSTN route to the SIP Trunk service.

SPN 999 FLEN 3 ITOH NO CLTP NONE **RLI 24** SDRR NONE ITEI NONE	SPN 90 FLEN 7 ITOH NO CLTP NONE **RLI 24** SDRR NONE ITEI NONE	SPN 2 FLEN 7 ITOH NO CLTP NONE **RLI 24** SDRR NONE ITEI NONE	SPN 15 FLEN 3 ITOH NO CLTP NONE **RLI 24** SDRR NONE ITEI NONE

5.7. Configure Analog, Digital and IP Telephones

A variety of telephone types were used during the testing. The following is the configuration for the Avaya 1140e Unistim IP telephone. **Load Overlay 20** at the system terminal and enter the following values. A unique four 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 **MAINOFFICE**.

```
Load Overlay 20 IP Telephone configuration
DES  1140
TN   096 0 01 16  VIRTUAL
TYPE 1140
CDEN 8D
CTYP XDLC
CUST 0
NUID
NHTN
CFG_ZONE 00010
CUR_ZONE 00010
ERL  0
ECL  0
FDN  0
TGAR 0
LDN  NO
NCOS 0
SGRP 0
RNPG 1
SCI  0
SSU
LNRS 16
XLST
SCPW
SFLT NO
CAC_MFC 0
CLS  UNR FBA WTA LPR PUA MTD FNA HTA TDD HFA CRPD
     MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
     POD SLKD CCSD SWD LNA CNDA
     CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBD
     ICDA CDMD LLCN MCTD CLBD AUTR
     GPUD DPUD DNDA CFXA ARHD FITD CLTD ASCD
     CPFA CPTA ABDD CFHD FICD NAID BUZZ AGRD MOAD
     UDI RCC HBTA AHD IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
     DRDD EXR0
     USMD USRD ULAD CCBD RTDD RBDD RBHD PGND OCBD FLXD FTTC DNDY DNO3 MCBN
     FDSD NOVD VOLA VOUD CDMR PRED RECA MCDD T87D SBMD KEM3 MSNV FRA  PKCH MUTA MWTD
---continued on next page----
```

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

DVLD CROD CROD
CPND_LANG ENG
RCO  0
HUNT 0
LHK  0
PLEV 02
PUID
DANI NO
AST  00
IAPG 1
AACS NO
ITNA NO
DGRP
MLWU_LANG 0
MLNG ENG
DNDR 0
KEY  00 MCR 8000 0     MARP
        CPND
          CPND_LANG ROMAN
            NAME IP1140
            XPLN 10
            DISPLAY_FMT FIRST,LAST
     01 MCR 8000 0
        CPND
          CPND_LANG ROMAN
            NAME IP1140
            XPLN 10
            DISPLAY_FMT FIRST,LAST
     02
     03 BSY
     04 DSP
     05
     06
     07
     08
     09
     10
     11
     12
     13
     14
     15
     16
     17 TRN
     18 AO6
     19 CFW 16
     20 RGA
     21 PRK
     22 RNP
     23
     24 PRS
     25 CHG
     26 CPN
```

Digital telephones are also configured using **Load 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.

```
Load Overlay 20 – Digital Set configuration
TYPE: 3904
DES  3904
TN   000 0 09 08  VIRTUAL
TYPE 3904
CDEN 8D
CTYP XDLC
CUST 0
MRT
ERL  0
FDN  0
TGAR 0
LDN  NO
NCOS 0
SGRP 0
RNPG 1
SCI  0
SSU
LNRS 16
XLST
SCPW
SFLT NO
CAC_MFC 0
CLS  UNR FBD WTA LPR PUA MTD FND HTD TDD HFA GRLD CRPA STSD
     MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
     POD SLKD CCSD SWD LNA CNDA
     CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBD
     ICDA CDMA LLCN MCTD CLBD AUTU
     GPUD DPUD DNDA CFXA ARHD FITD CNTD CLTD ASCD
     CPFA CPTA ABDA CFHD FICD NAID BUZZ AGRD MOAD
     UDI RCC HBTD AHA IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
     DRDD EXR0
     USMD USRD ULAD CCBD RTDD RBDD RBHD PGND OCBD FLXD FTTC DNDY DNO3 MCBN
     FDSD NOVD CDMR PRED RECA MCDD T87D SBMD PKCH CROD CROD
CPND_LANG ENG
RCO  0
HUNT
PLEV 02
PUID
DANI NO
SPID NONE
AST
IAPG 1
AACS
ACQ
ASID
SFNB
SFRB
USFB
CALB
FCTB
ITNA NO
DGRP
PRI  01
MLWU_LANG 0

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

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

MLNG ENG
DNDR 0
KEY  00 MCR 8866 0     MARP
        CPND
          CPND_LANG ROMAN
            NAME Digital Set
            XPLN 10
            DISPLAY_FMT FIRST,LAST
     01 MCR 8866 0
        CPND
          CPND_LANG ROMAN
            NAME Digital Set
            XPLN 10
            DISPLAY_FMT FIRST,LAST
     02 DSP
     03 MSB
     04
     05
     06
     07
     08
     09
     10
     11
     12
     13
     14
     15
     16
     17 TRN
     18 AO6
     19 CFW 16
     20 RGA
     21 PRK
     22 RNP
     23
     24 PRS
     25 CHG
     26 CPN
     27 CLT
     28 RLT
     29
     30
     31
```

Analog telephones are also configured using **Load Overlay 20**. The following example shows an analog port configured for Plain Ordinary Telephone Service (POTS) and also configured to allow pass thru Fax transmission. A unique value is entered for **DN**, this is the extension number. **DTN** is required if the telephone uses DTMF dialing. Values **FAXD** and **MPTA** configure the port for pass thru Fax transmissions.

Load Overlay 20 – Analog Telephone Configuration

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

ERL 00000
WRLS NO
DN   8888
AST  NO
IAPG 0
HUNT
TGAR 0
LDN  NO
NCOS 0
SGRP 0
RNPG 0
XLST
SCI  0
SCPW
SFLT NO
CAC_MFC 0
CLS  UNR DTN FBD XFD WTA THFD FND HTD ONS
     LPR XRD AGRD CWD SWD MWD RMMD SMWD LPD XHD SLKD CCSD LND TVD
     CFTD SFD MRD C6D CNID CLBD AUTU
     ICDD CDMD LLCN EHTD MCTD
     GPUD DPUD CFXD ARHD OVDD AGTD CLTD LDTD ASCD SDND
     MBXD CPFA CPTA UDI RCC HBTD IRGD  DDGA NAMA MIND
     NRWD NRCD NROD SPKD CRD PRSD MCRD
     EXR0 SHL SMSD ABDD CFHD DNDY DNO3
     CWND USMD USRD CCBD BNRD OCBD RTDD RBDD RBHD FAXD CNUD CNAD PGND FTTC
     FDSD NOVD CDMR PRED MCDD T87D SBMD PKCH MPTA
PLEV 02
PUID
AACS NO
MLWU_LANG 0
FTR  DCFW 4
```

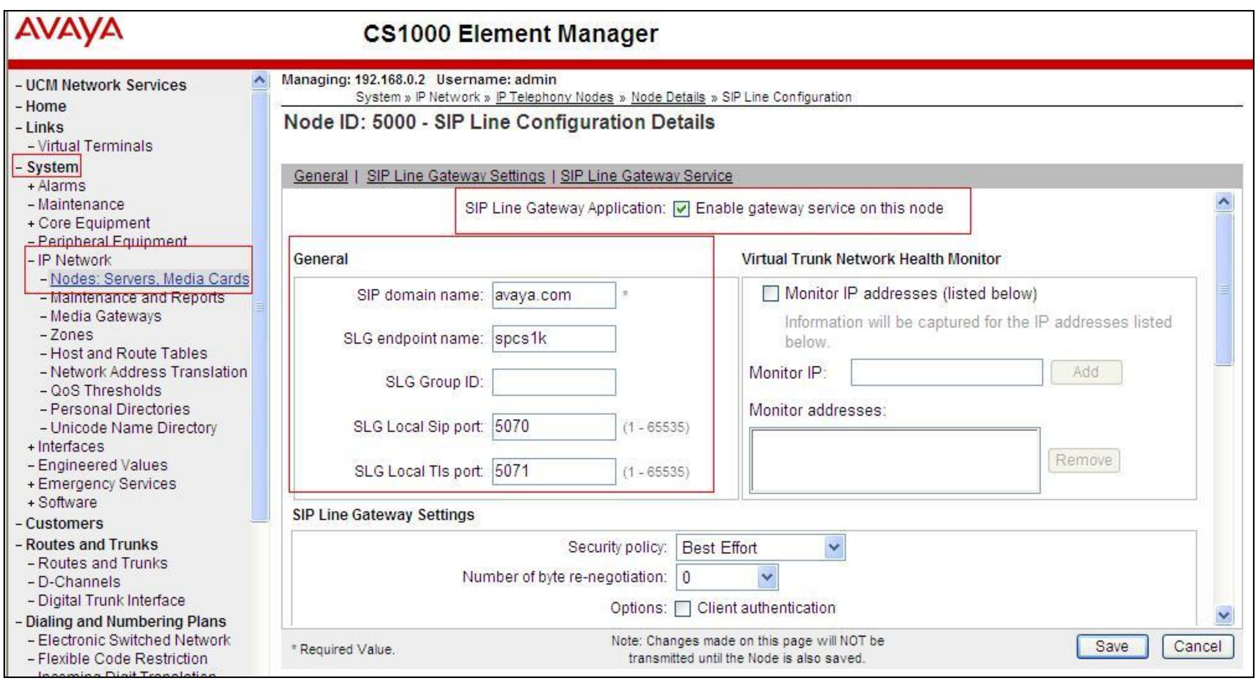
5.8. Configure the SIP Line Gateway Service

SIP terminal operation requires the Communication Server node to be configured as a SIP Line Gateway (SLG) before SIP telephones can be configured. Prior to configuring the SIP Line node properties, the SIP Line service must be enabled in the customer data block. Use the Communication Server 1000E system terminal and overlay 15 to activate SIP Line services, as in the following example where **SIPL_ON** is set to **YES**.

```
SLS_DATA
  SIPL_ON YES
  UAPR 78
  NMME NO
```

If a numerical value is entered against the **UAPR** setting, this number will be pre appended to all SIP Line configurations, and is used internally in the SIP Line server to track SIP terminals. Use Element Manager and navigate to the **IP Network → IP Telephony Nodes → Node Details → SIP Line Gateway Configuration** page. See the following screenshot for highlighted critical parameters. The value for **SIP Domain Name** must match that configured in **Section 6.1**.

- **SIP Line Gateway Application: Enable the SIP line service on the node**, check the box to enable
- **SIP domain name:** Enter the SIP domain, in this case **avaya.com**
- **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 the SIP Line service configuration is completed, use the Communication Server 1000E system terminal and **Load Overlay 20** to add a Universal Extension (UEXT). See the following example of a SIP Line extension. The value for **UXTY** must be **SIPL**. This example is for an Avaya SIP telephone, so the value for **SIPN** is 1. The **SIPU** value is the username, **SCPW** is the logon password, and these values are required to register the SIP telephone to the SLG. The value for **CFG_ZONE** is the value set for **MAINOFFICE** in **Section 5.4**. A unique telephone number is entered for value **KEY 00**. The value for **KEY 01** is comprised of the **UAPR** value (set to 78 at the beginning of this section) and the telephone number used in **KEY 00**.

Load Overlay 20 – SIP Telephone Configuration

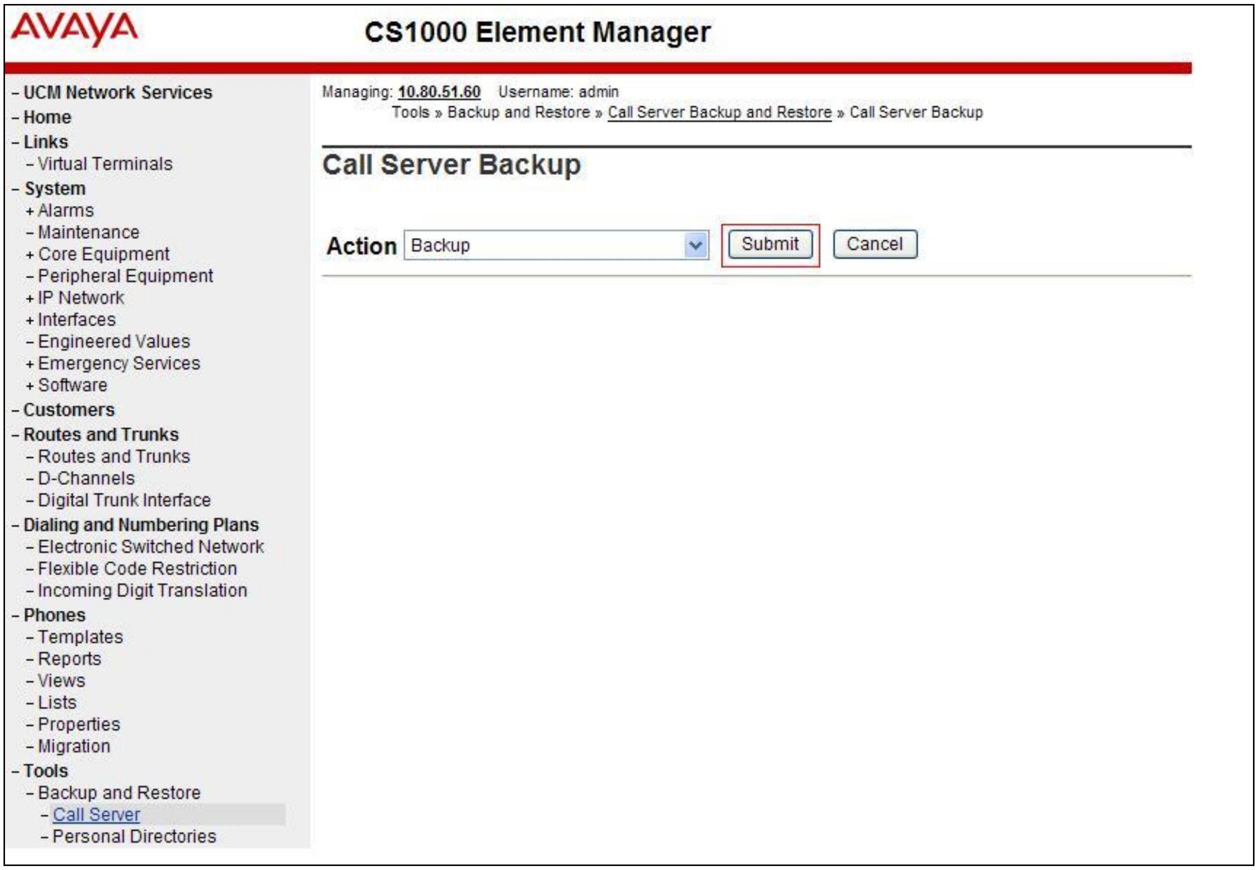
```
DES  SIPD
TN   096 0 01 15  VIRTUAL
TYPE UEXT
CDEN 8D
CTYP XDLC
CUST 0
UXTY SIPL
MCCL YES
SIPN 1
SIP3 0
FMCL 0
TLSV 0
SIPU 8889
NDID 5
SUPR NO
SUBR DFLT MWI RGA CWI MSB
UXID
NUID
NHTN
CFG_ZONE 00010
CUR_ZONE 00010
ERL  0
ECL  0
VSIT NO
FDN
TGAR 0
LDN  NO
NCOS 0
SGRP 0
RNPG 0
SCI  0
SSU
XLST
SCPW 1234
SFLT NO
CAC_MFC 0
CLS  UNR FBD WTA LPR MTD FNA HTA TDD HFD CRPD
     MWD LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
     POD SLKD CCSD SWD LND CNDA
     CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBD
     ICDD CDMD LLCN MCTD CLBD AUTU
     GPUD DPUD DNDA CFXA ARHD FITD CLTD ASCD
     CPFA CPTA ABDD CFHD FICD NAID BUZZ AGRD MOAD
```

---continued on next page---

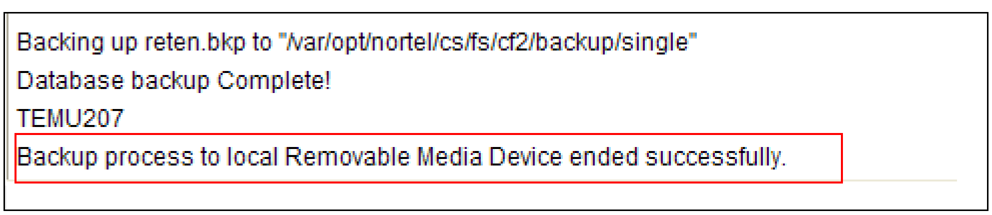
```
---continued from previous page---

     UDI RCC HBTD AHA IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
     DRDD EXR0
     USMD USRD ULAD CCBD RTDD RBDD RBHD PGND OCBD FLXD FTTC DNDY DNO3 MCBN
     FDSD NOVD VOLA VOUD CDMR PRED RECD MCDD T87D SBMD ELMD MSNV FRA  PKCH MWTD DVLD
CROD CROD
CPND_LANG ENG
RCO  0
HUNT
LHK  0
PLEV 02
PUID
DANI NO
AST
IAPG 0 *

AACS NO
ITNA NO
DGRP
MLWU_LANG 0
MLNG ENG
DNDR 0
KEY  00 MCR 8889 0     MARP
        CPND
          CPND_LANG ROMAN
            NAME Sigma 1140
            XPLN 11
            DISPLAY_FMT FIRST,LAST*
     01 HOT U 788889 MARP 0
     02
     03
     04
     05
     06
     07
     08
     09
     10
     11
     12
     13
     14
     15
     16
     17 TRN
     18 AO6
     19 CFW 16
     20 RGA
     21 PRK
     22 RNP
     23      *
     24 PRS
     25 CHG
     26 CPN
     27
     28
     29
     30
     31
```

5.10. Save Configuration

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



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



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:

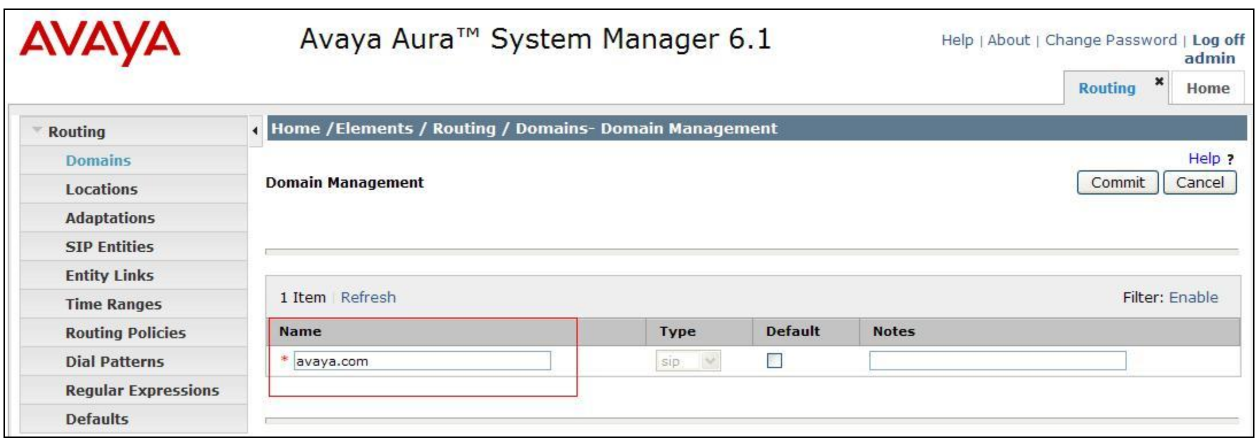
- Define SIP Domain
- Define Location for Avaya Communication Server 1000E
- Configure the Adaptation Module.
- Define SIP Entities
- Define Entity Links
- Define Routing Policies
- Define Dial Patterns

6.1. Define SIP Domain

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

- **Name** Enter the Domain Name specified for the SIP Gateway in **Section 5.4.** In the sample configuration, **avaya.com** was used
- **Type** Verify **sip** is selected
- **Notes** Add a brief description [Optional]

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



6.2. Define Location for Avaya Communication Server 1000E

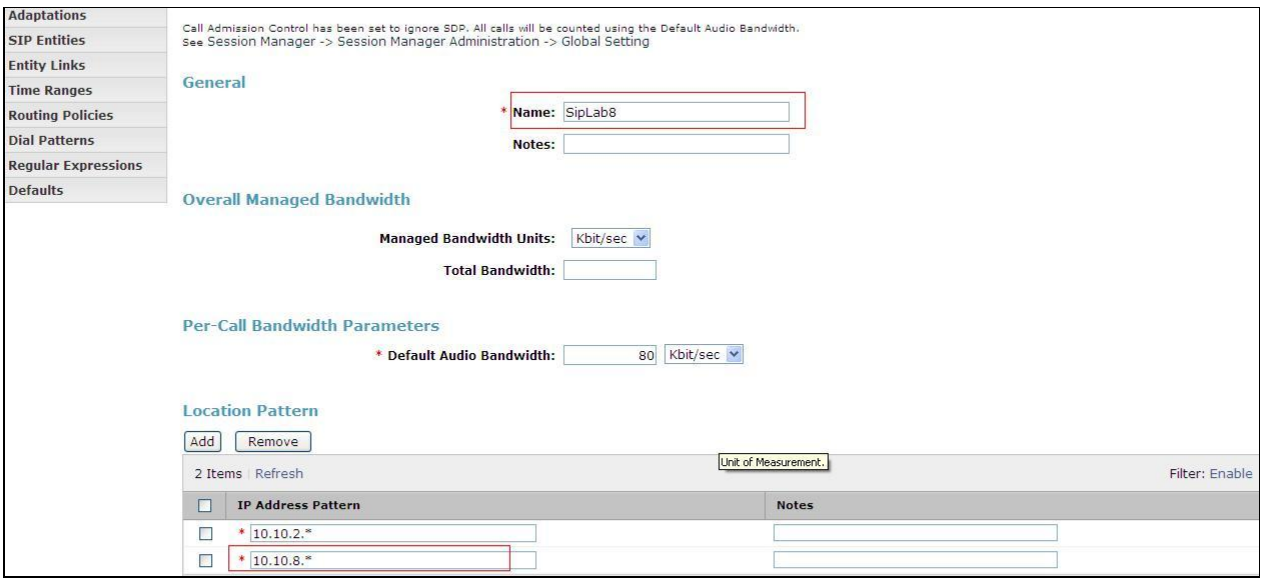
Locations are used to identify logical and/or physical locations where SIP Entities reside, for purposes of bandwidth management or location-based routing. Expand **Elements → Routing** and select **Locations** from the left navigational menu. Click **New** (not shown). In the **General** section**,**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

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

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

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

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



6.3. Configure Adaptation Module

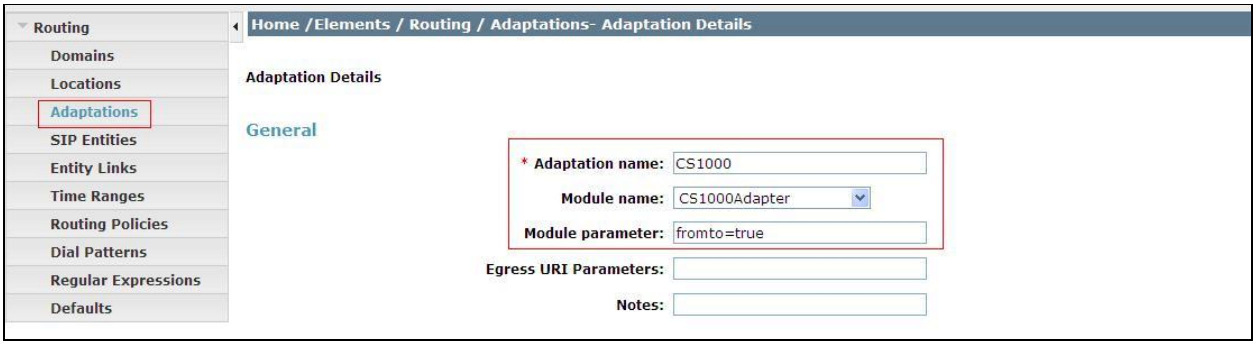
Session Manager can be configured to use an Adaptation Module designed for Avaya Communication Server 1000E to convert SIP headers in messages sent by Avaya Communication Server to the format used by other Avaya products and endpoints.

6.3.1. Adaptation for Avaya Communication Server 1000E Entity

This adaptation is used to change incoming digits received from the PSTN (DDIs) to extensions on the CS1000E and conversely to match outgoing calls from extension on the CS1000E to DDI numbers that are going to be presented to the PSTN.

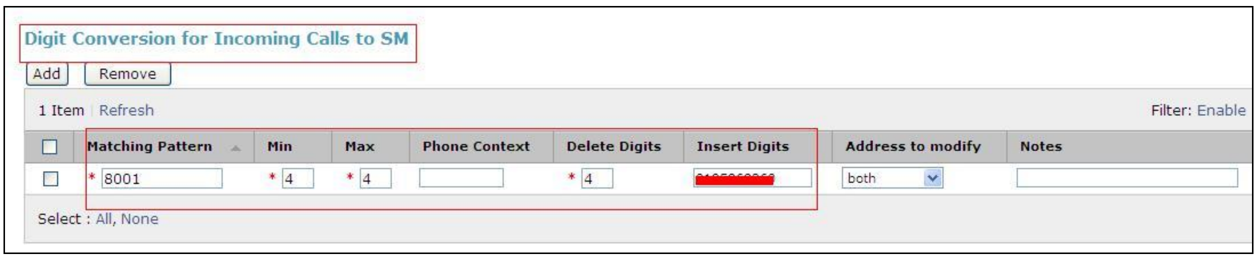
Select **Adaptations** from the left navigational menu. Click **New (**not shown**).** In the **General** section, enter the following values and use default values for remaining fields**.**

- **Adaptation Name:** Enter an identifier for the Adaptation Module (e.g., "CS1000")
- **Module Name:** Select "**CS1000Adapter**" from drop-down menu (or add an adapter with name "CS1000Adapter" if not previously defined)
- **Module Parameter:** Enter "fromto=true" to allow the From and To headers to be modified by Session Manager (i.e., in addition to other headers such as the P-Asserted-Identity and Request-URI headers).

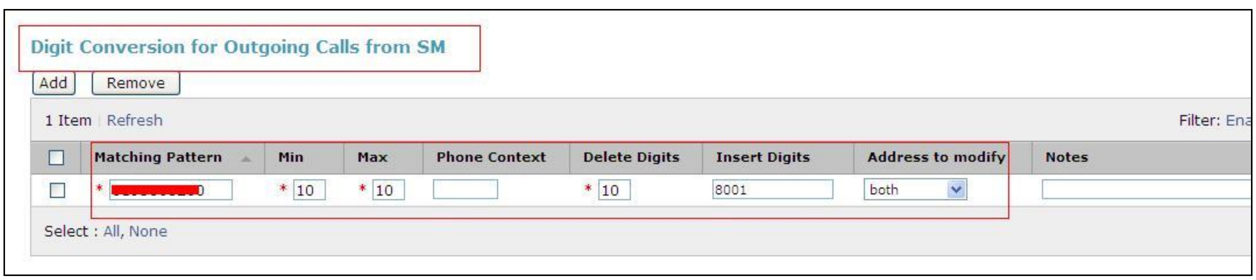


Scrolling down, in the **Digit Conversion for Incoming Calls to SM** section, click **Add** to configure entries for calls from CS1000E users to Frontier. The text below and the screen example that follows explain how to use Session Manager to convert between CS1000E directory numbers and the corresponding Frontier DID numbers.

- **Matching Pattern:** Enter Avaya CS1000E extensions (or extension ranges via wildcard pattern matching). For other entries, enter the dialed prefix for any SIP endpoints registered to Session Manager (if any).
- **Min:** Enter minimum number of digits (e.g., 4)
- **Max:** Enter maximum number of digits (e.g., 4)
- **Delete Digits:** Enter "**4**", unless digits should not be removed from dialed number before routing by Session Manager.
  Insert Digits: Enter the Frontier DID corresponding to the matched extension. DID is masked for security.
- **Address to modify:** Select **"both"**



Scroll down and make corresponding changes in the **Digit Conversion for Outgoing Calls from SM** section for calls from Frontier to CS1000E users. DID masked for security purposes.



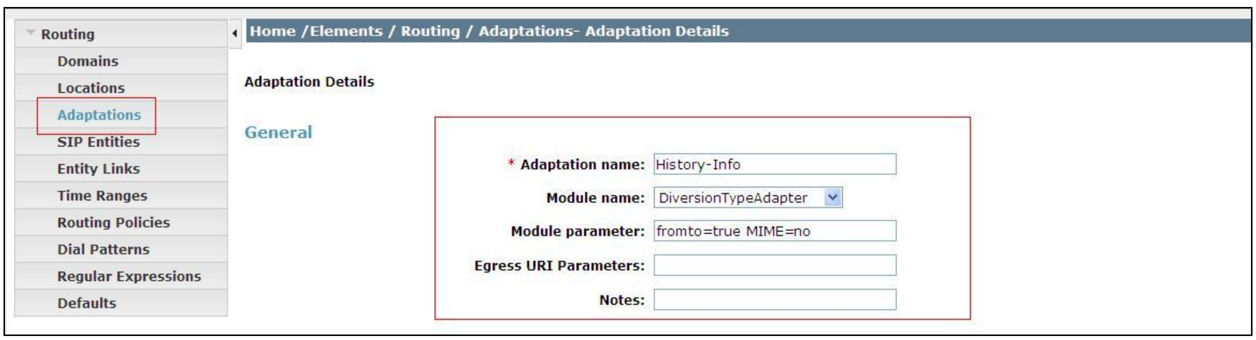
Click **Commit** to save.

6.3.2. Adaptation for Avaya Aura® Session Border Controller Entity

This adapatation is used to create a Diversion header in an INVITE for a call forward scneraio that is originated from the PSTN and is forwarded back out to the PSTN. This adaptation copies the History header and creates a new Diversion header in the INVITE that is sent out to Frontier.

Select **Adaptations** from the left navigational menu. Click **New (**not shown**).** In the **General** section, enter the following values and use default values for remaining fields**.**

- **Adaptation Name:** Enter an identifier for the Adaptation Module
- **Module Name:** Select "**DiversionTypeAdapter** " from drop-down menu (or add an adapter with name "DiversionTypeAdapter" if not previously defined)
- **Module Parameter:** Enter "fromto=true" to allow the From and To headers to be modified by Session Manager (i.e., in addition to other headers such as the P-Asserted-Identity and Request-URI headers). Enter **MIME=no** to have Session Manager strip MIME message bodies on egress to Frontier's SBC, such that only SDP is present in the message body sent to Frontier's SBC



Click **Commit (not shown).**

6.4. Define 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:**

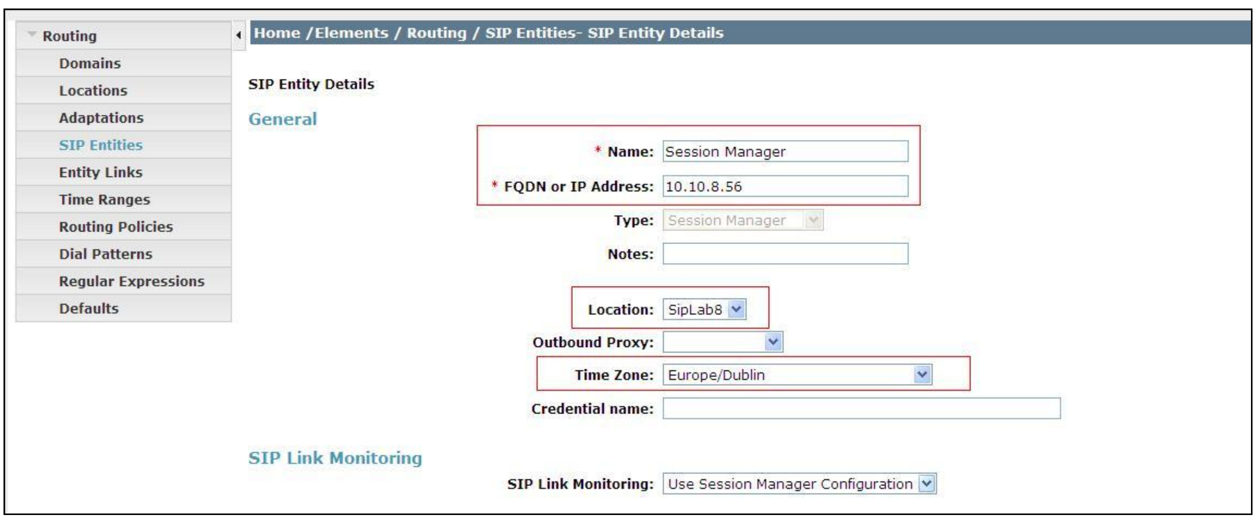
- In the **Name** field enter an informative name
- In the **FQDN or IP Address** field enter the IP address of Session Manager or the signalling interface on the connecting system
- In the **Type** field use **Session Manager** for a Session Manager SIP entity, **Other** for a Communication Server 1000E SIP entity and **Gateway** for the Session Border Controller 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 Communication Server 1000E SIP Entity
- Avaya Session Border Controller Advanced for Enterprise SIP Entity

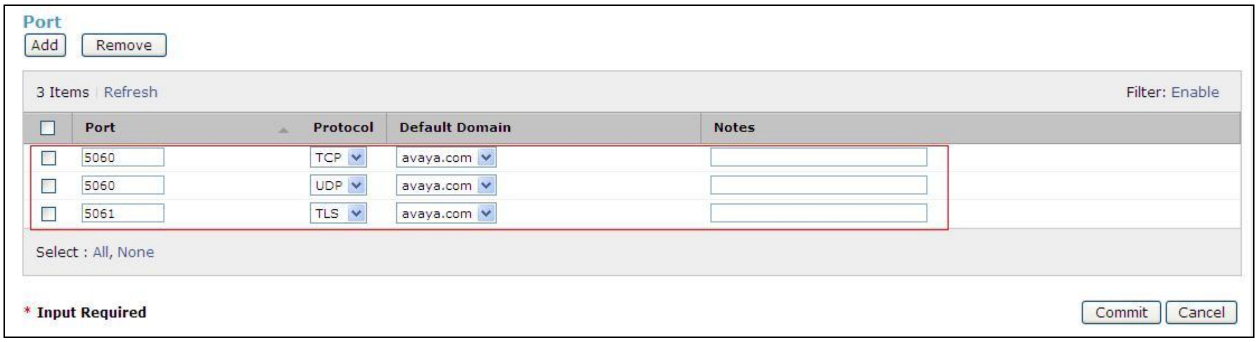
6.4.1. Avaya Aura® Session Manager SIP Entity

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.



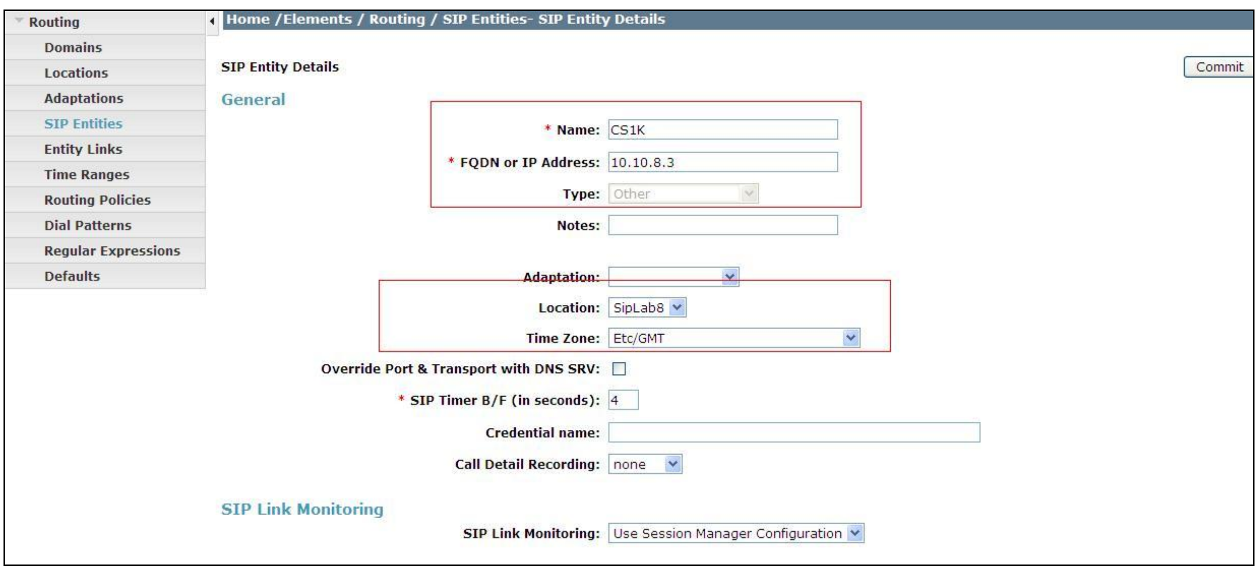
The Session Manager must be configured with the port numbers on the protocols that will be used by the other SIP entities. To configure these scroll to the bottom of the page and under **Port**, click **Add,** then edit the fields in the resulting new row.

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



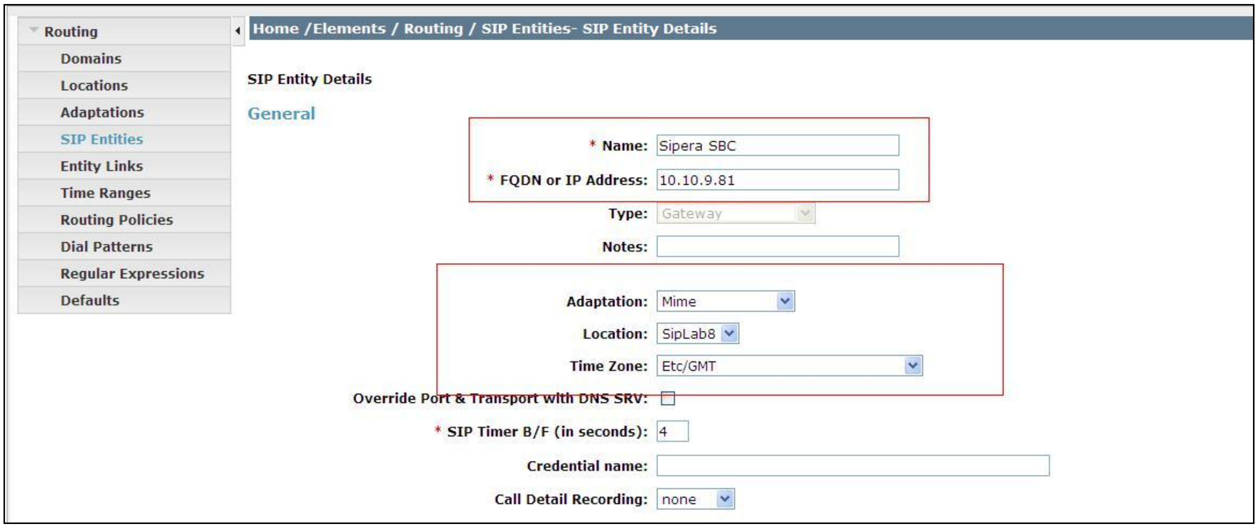
6.4.2. Avaya Communication Server 1000E SIP Entity

The following screen shows the SIP entity for Communication Server 1000E. The **FQDN or IP Address** field is set to the Node IP address of the interface on CS1000E that will be providing SIP signalling, as shown in **Section 5.4**.



6.4.3. Avaya Session Border Controller Advanced for Enterprise SIP Entity

The following screen shows the SIP Entity for the Session Border Controller. The **FQDN or IP Address** field is set to the IP address of the Session Border Controller private network interface (see **Figure 1**). Note the adaption module configured in **Section 6.3** is applied to this entity link.

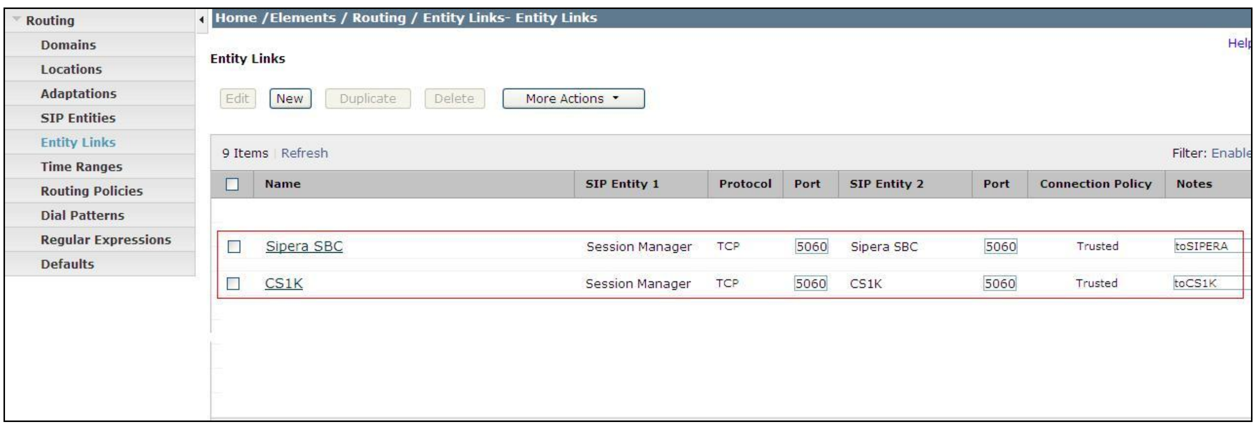


6.5. Configure Entity Links

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 1**
- 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 6.4**
- 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 (not shown)** to save changes. The following screen shows the Entity Links used in this configuration.



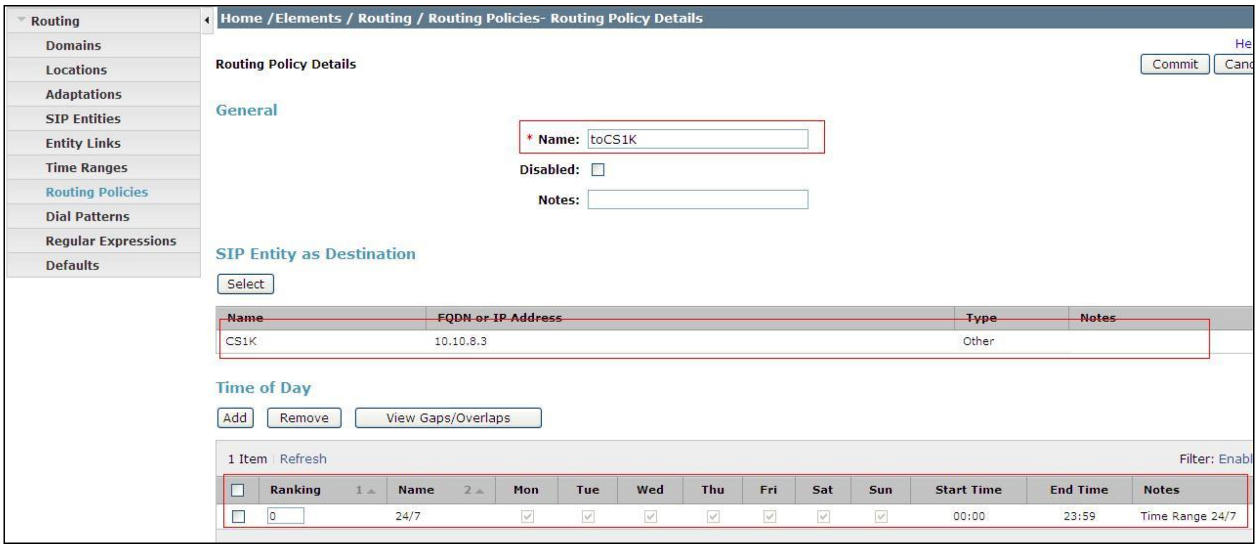
6.6. Define Routing Policies

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).

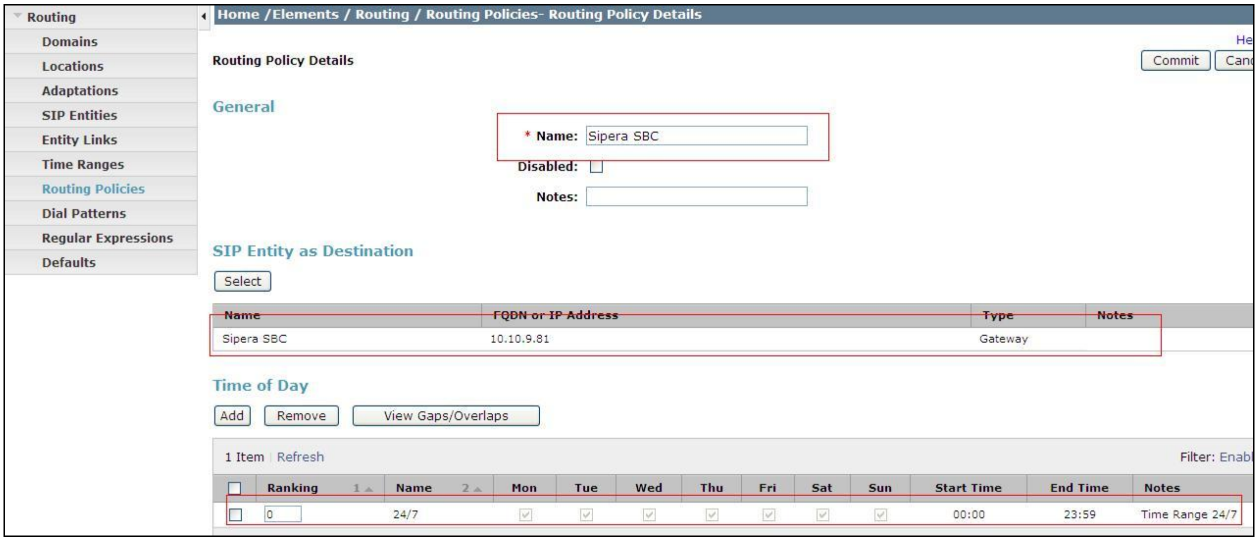
Under **General:**

- 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 Communication Server 1000E



The following screen shows the routing policy for the Session Border Controller.



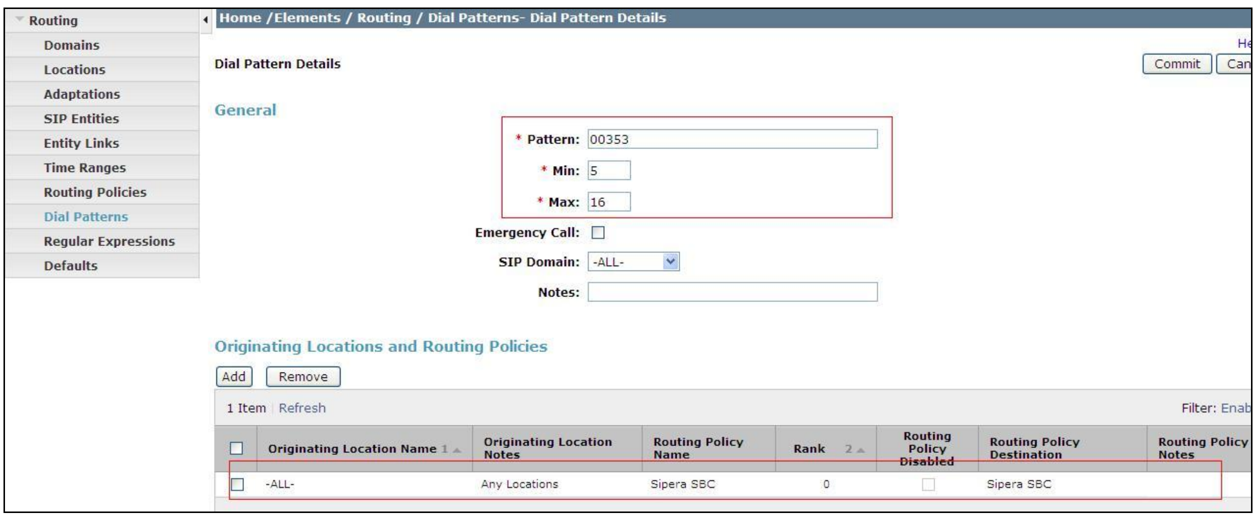
6.7. Define Dial Patterns

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).

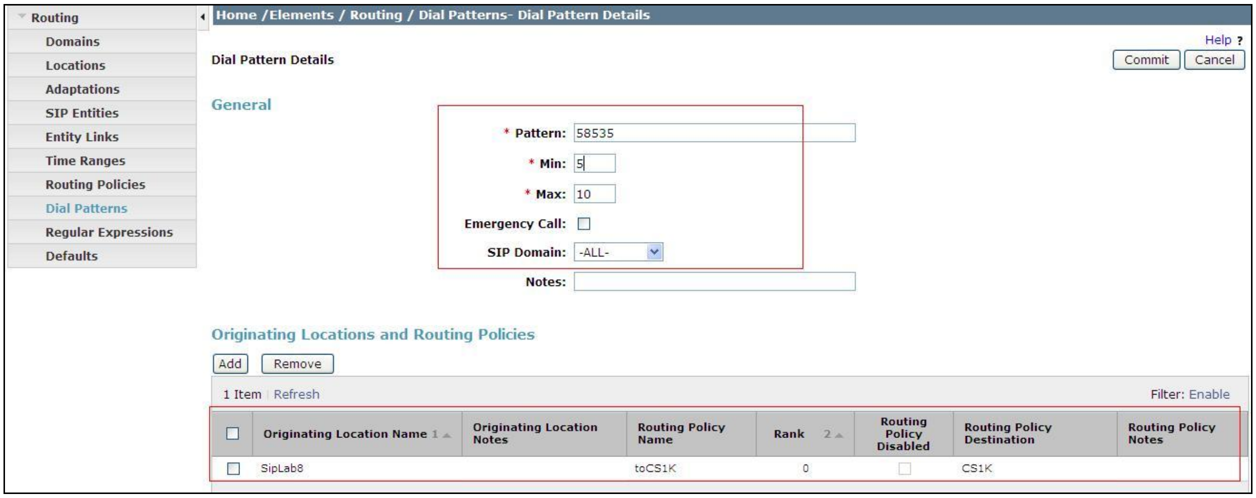
Under **General:**

- 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 6.1**

Under **Originating Locations and Routing Policies.** Click **Add**, in the resulting screen (not shown), under **Originating Location** select **ALL** and under **Routing Policies** select one of the routing policies defined in **Section 6.6** Click **Select** button to save. The following screen shows an example dial pattern configured for the Session Border Controller which will route the calls out to Frontier's SIP Trunk Service.



The following screen shows an example dial pattern configured for the CS1000E. This dial pattern will route the calls to the CS1000E endpoints.



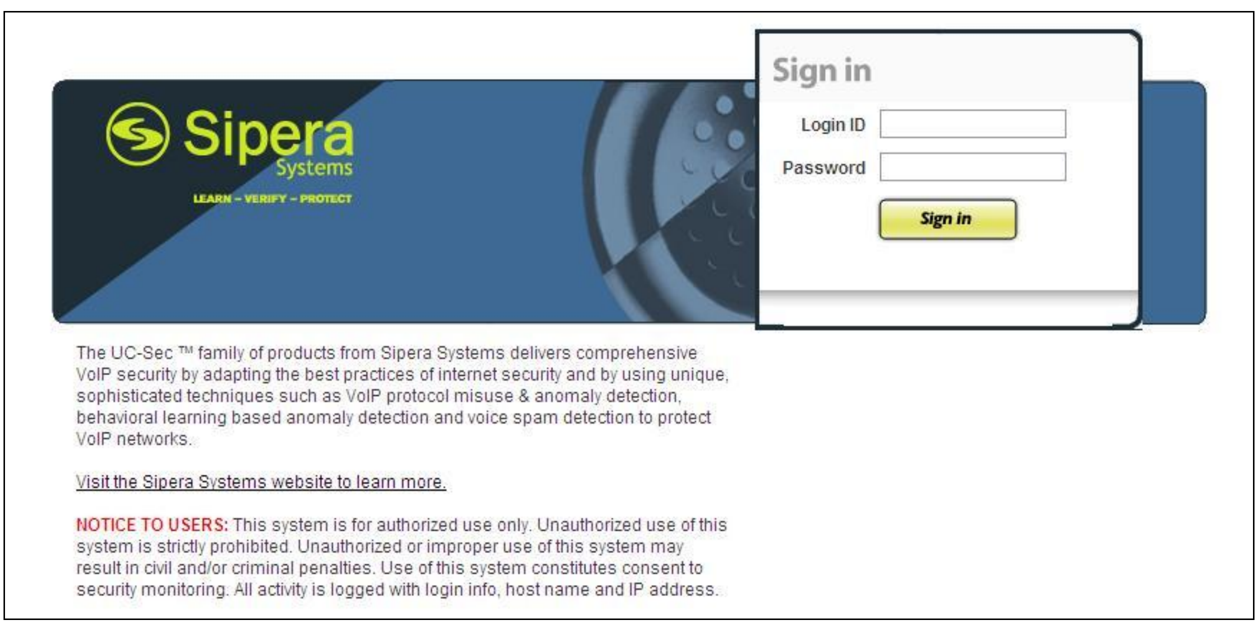
7. Configure Avaya Session Border Controller Advanced for Enterprise

This section describes the configuration of the Session Border Controller. At the time of writing the Avaya Session Border Controller Advanced 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 Advanced for Enterprise is administered using the E-SBC Control Center.

7.1. Access Avaya Session Border Controller Advanced 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.



7.2. Global Profiles

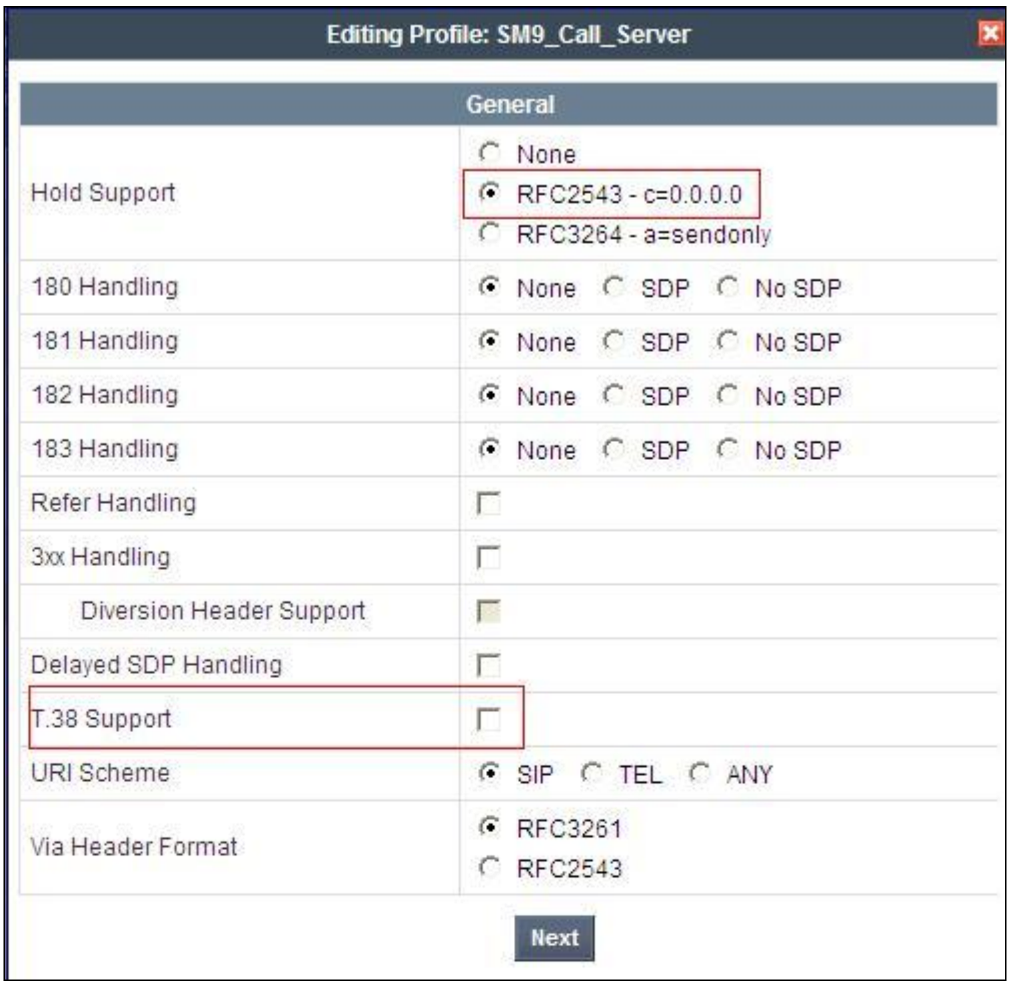
When selected, Global Profiles allows for configuration of parameters across all UC-Sec appliances.

7.2.1. Server Interworking - Avaya Side

Server Internetworking allows you to configure and manage various SIP call server specific capabilities such as call hold and T.38. From the lefthand menu select **Global Profiles → Server Interworking** and click on **Add Profile.**

- Enter profile name**: SM9_Call_Server** and click **Next**
- **Check Hold Support= RFC2543**
- **Uncheck T.38 support**
- All other options on the General Tab can be left at default.

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

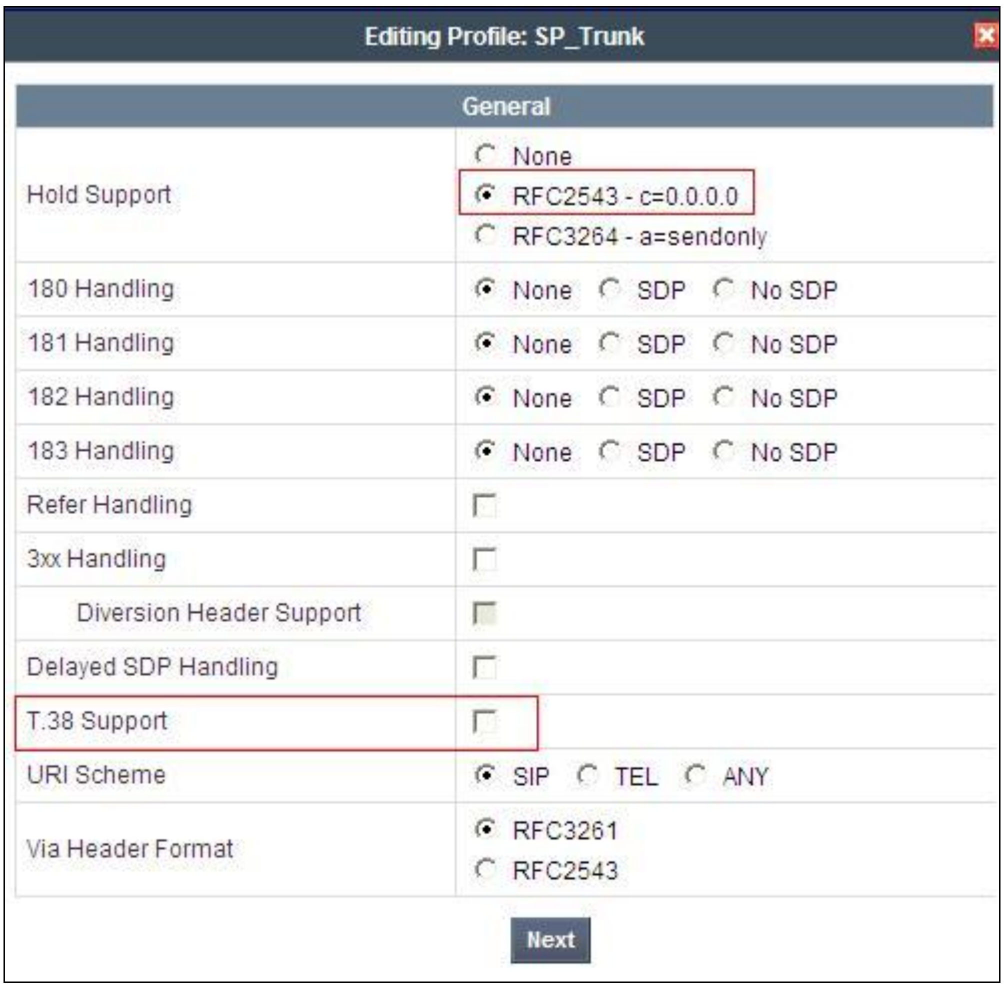


7.2.2. Server Interworking – Frontier side

Server Internetworking allows you to configure and manage various SIP call server specific capabilities such as call hold and T.38. From the lefthand menu select **Global Profiles → Server Interworking** and click on **Add Profile.**

- Enter profile name**: SP_Trunk** and click on **Next**
- **Check Hold Support= RFC2543**
- **Uncheck T.38 support**
- All other options on the General Tab can be left at default.

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



7.2.3. Routing – Avaya side

The Routing Profile allows you to manage parameters related to routing SIP signaling messages. From the lefthand menu select **Global Profiles → Routing** and click on **Add Profile**.

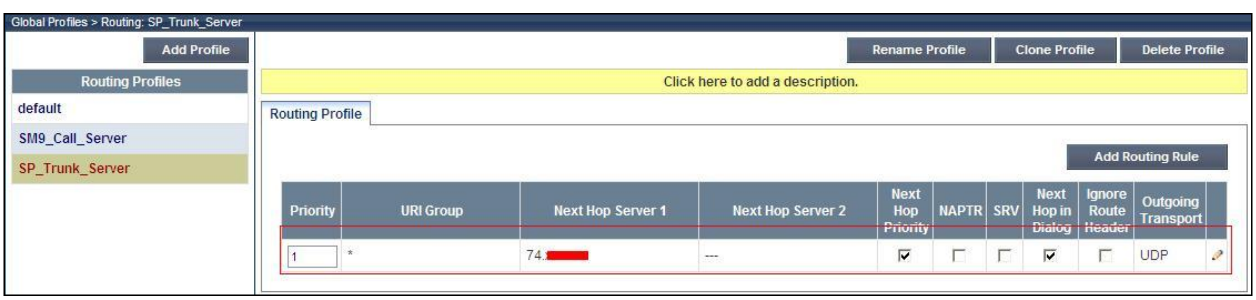
- Enter Profile Name: **SM9_Call_Server**
- Hit **Next** (not shown)
- **Next Hop Server 1: 10.10.8.56 (Session Manager Secuirty Module IP address)**
- Select **Routing Priority Based on Next Hop Server**
- Select **Use Next Hop for In-Dialog Messages**
- **Outgoing Transport: TCP**

Click **Finish** (not shown).

7.2.4. Routing – Frontier side

The Routing Profile allows you to manage parameters related to routing SIP signaling messages. From the lefthand menu select **Global Profiles → Routing** and click on **Add Profile**.

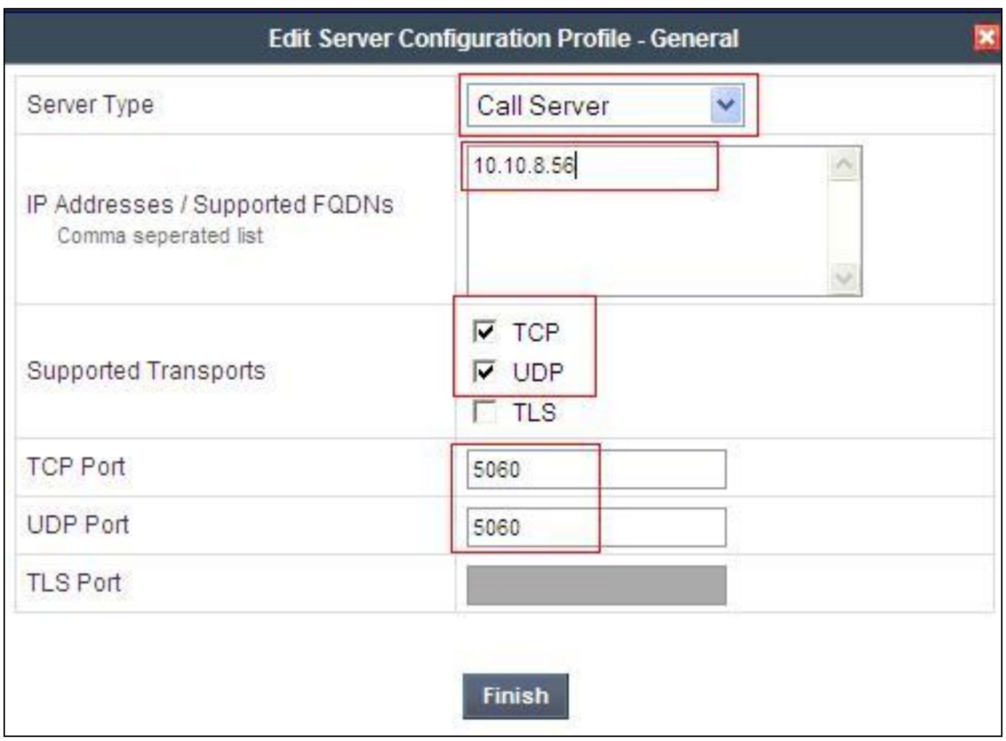
- Enter Profile Name: **SP_Trunk_Server**
- Hit **Next**
- **Next Hop Server 1: 74.xx.xx.xx (IP Address provided by Frontier, partially hidden for security purposes)**
- Select **Routing Priority Based on Next Hop Server**
- Select **Use Next Hop for In-Dialog Messages**
- **Outgoing Transport: UDP**
- Click **Finish** (not shown)

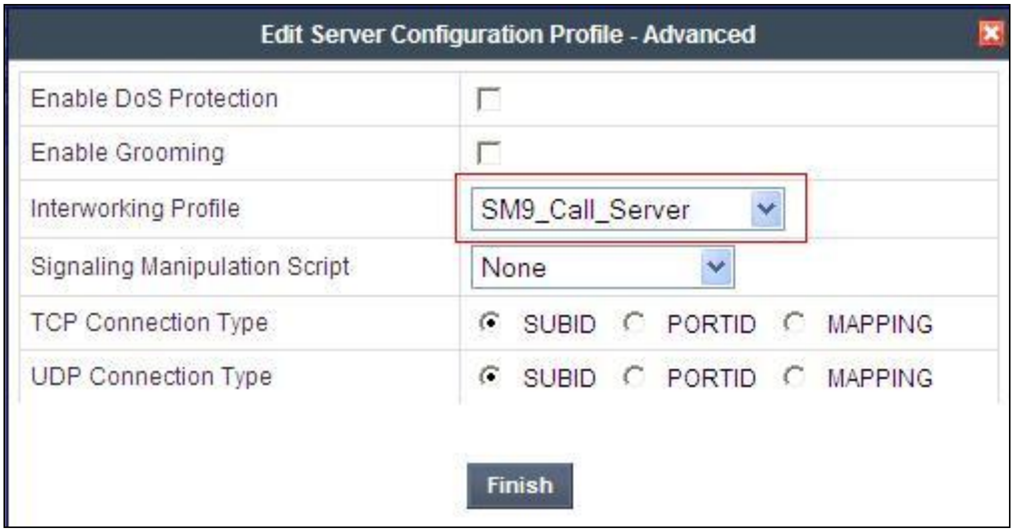


7.2.5. Server Configuration – Avaya CS1000E

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow you to configure and manage various SIP call server specific parameters such as TCP and UDP port assignments, IP Server type, heartbeat signaling parameters and some advanced options. From the lefthand menu select **Global Profiles → Server Configuration** and click on **Add Profile**.

- **Enter profile name: SM9_Call_Server**
- On the **Add Server Configuration Profile** Tab:
- Select Server Type**: Call Server**
- **IP Address: 10.10.8.56**
- **Supported Transports: Check UDP and TCP**
- **TCP Port:5060**
- **UDP Port: 5060**
- Click on **Next** for the **Authentication** and **Heartbeat** tabs.
- On the **Advanced** Tab
- Select **SM9_Call_Sever** for Interworking Profile
- Hit **Next**
- Click **Finish**

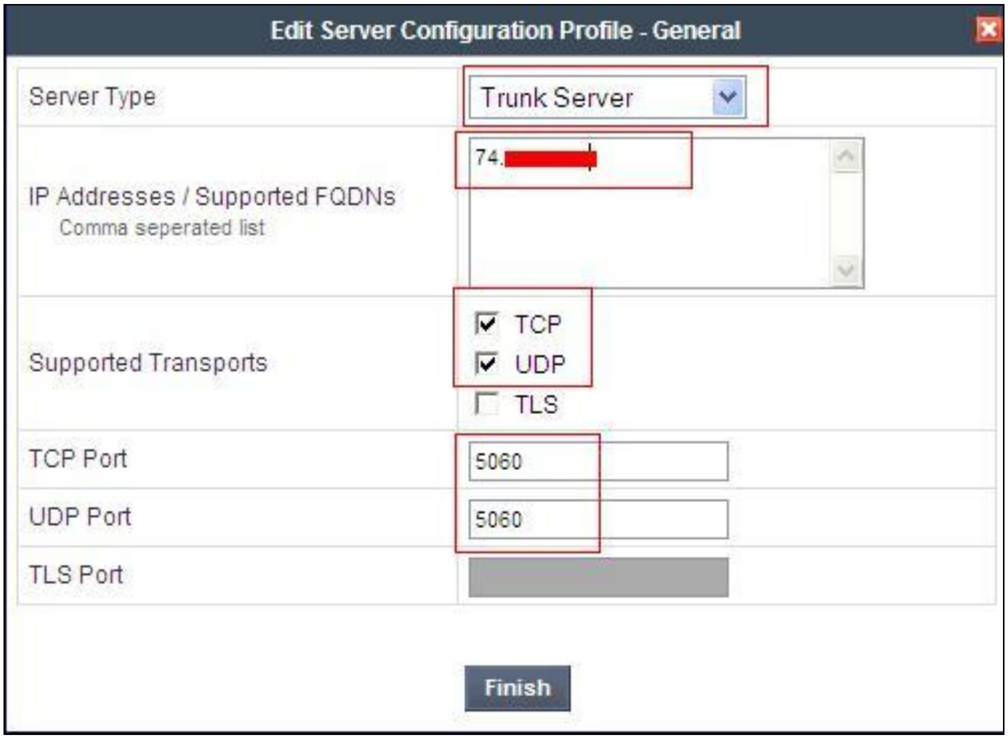




7.2.6. Server Configuration – Frontier side

The **Server Configuration** screen contains fourtabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow you to configure and manage various SIP call server specific parameters such as TCP and UDP port assignments, server type, heartbeat signaling parameters and some advanced options. From the left-hand menu select **Global Profiles → Server Configuration** and click on **Add Profile.**

- **Name: SP_Trunk_Server**
- On the **Add Server Configuration Profile** Tab:
- Click on **Edit**
- Select Server Type**: Trunk Server**
- **IP Address: 74.xx.xx.xx (Frontier Trunk Server, IP address hidden for secuirtiy purposes)**
- **Supported Transports**: Check **UDP**
- **UDP Port: 5060**
- Hit **Next**
- Click on **Next** for the **Authentication** and **Heartbeat** tabs.
- On the **Advanced** Tab
- Select **SP_Trunk** for Interworking Profile
- Hit **Next**
- Click **Finish**


Edit Server Configuration Profile - General
Server Type
Trunk Server
IP Addresses / Supported FQDNs
Comma seperated list
74.[redacted]
Supported Transports
TCP
UDP
TLS
TCP Port
5060
UDP Port
5060
TLS Port
Finish


Edit Server Configuration Profile - Advanced
Enable DoS Protection
Enable Grooming
Interworking Profile
SP_Trunk
Signaling Manipulation Script
None
TCP Connection Type
SUBID
PORTID
MAPPING
UDP Connection Type
SUBID
PORTID
MAPPING
Finish

7.2.7. Topology Hiding – Avaya side

The **Topology Hiding** screen allows you to manage how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks. From the left-hand menu select **Global Profiles → Topology Hiding.**

- Click **default** profile and select **Clone Profile**
- Enter Profile Name**: SM9_CS**
- For the **Header To, From** and **Request Line** select **IP/Domain** under **Criteria** and **Overwrite** under **Replace Action.** For **Override Value** type **avaya.com**
- Click **Finish**

The screen below is a result of the details configured above

7.2.8. Topology Hiding – Frontier side

The **Topology Hiding** screen allows you to manage how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the integrity of the network. It hides the topology of the enterprise network from external networks. From the left-hand menu select **Global Profiles → Topology Hiding.**

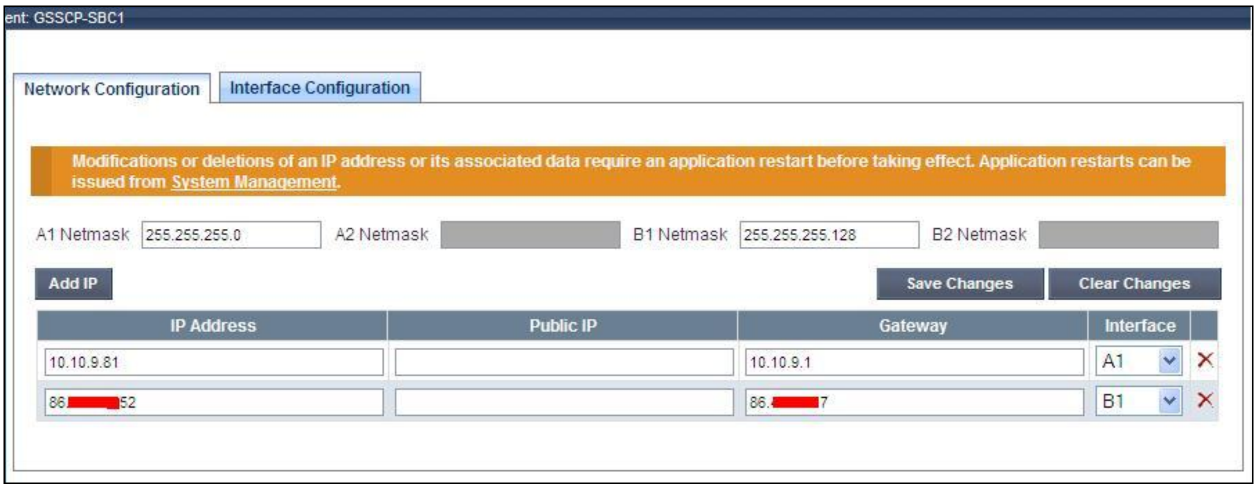
- Click **default** profile and select **Clone Profile**
- **Enter Profile Name: SP_Trunk**
- For the Header **To, From** and **Request Line** select **IP/Domain** under **Criteria** and **Next Hop** under **Replace Action**
- Click **Finish**

The screen below is a result of the details configured above

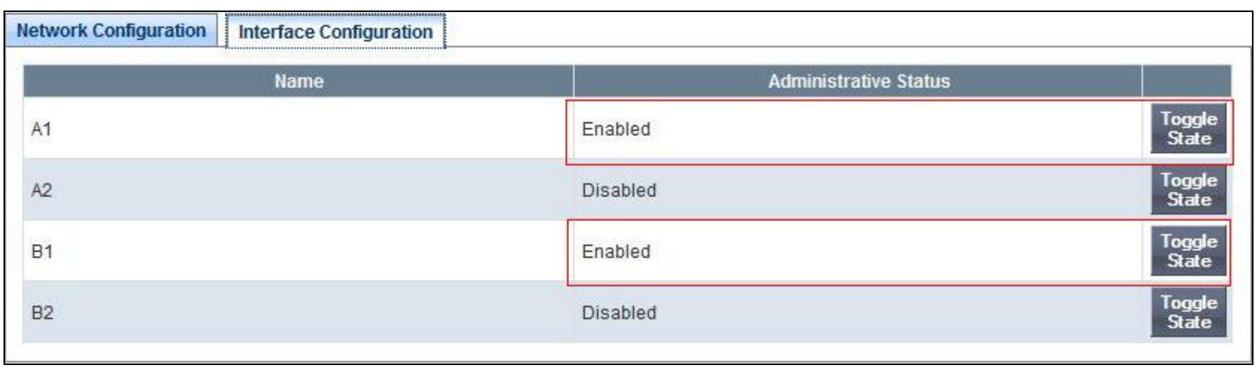
7.3. Device Specific Settings

7.3.1. The **Network Management** feature allows the public and private interface addresses and state to be set. From the left-hand menu select **Device Specific Settings → Network Management.**

- Enter in the **IP Address** and **Gateway Address** for both the Inside and the Outside interfaces
- Select the physical interface used in the **Interface** column



Select the **Interface Configuration** Tab and use the **Toggle State** button to enable the interfaces.



7.3.2. The **Media Interfaces** feature allows the IP Address and ports to be set for transporting Media over the SIP trunk. From the left-hand menu select **Device Specific Settings → Media Interface.**

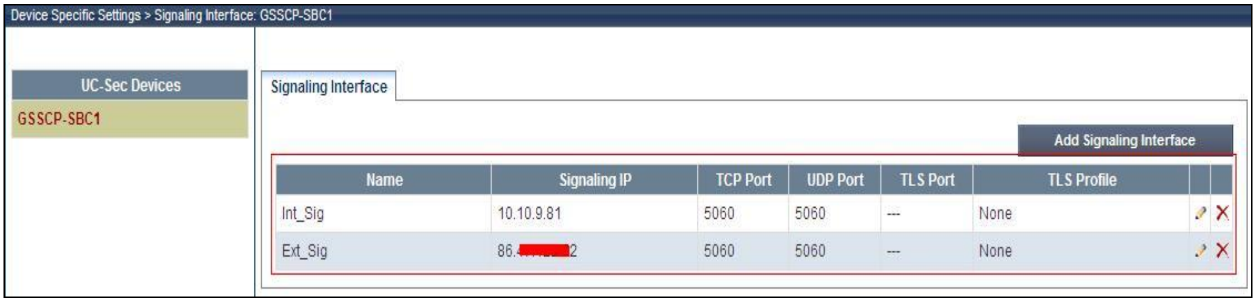
- Select **Add Media Interface**
- **Name**: **Int_Media**
- **Media IP**: **10.10.9.81** (Internal Address for calls toward Session Manager)
- **Port Range**: **35000-50000**
- Click **Finish**
- Select **Add Media Interface**
- **Name**: **Ext_Media**
- **Media IP**: **86.xx.xx.xx** (External Address for calls toward Frontier trunk, hidden for security purposes)
- **Port Range**: **35000-50000**
- Click **Finish**
- Select **Add Media Interface**

The screen below is a result of the details configured above.

7.3.3. The **Signalling Interfaces** feature allows the IP Address and ports to be set for transporting Media over the SIP trunk. From the left-hand menu select **Device Specific Settings → Signalling Interface.**

- Select **Add Signaling Interface**
- **Name**: **Int_Sig**
- **Signaling IP**: **10.10.9.81** (Internal Address for calls toward Session Manager)
- **TCP Port**: **5060**
- **UDP Port**: **5060**
- Click **Finish**
- Select **Add Signaling Interface**
- **Name**: **Ext_Sig**
- **Signaling IP: 86.xx.xx.xx** (External Address for calls toward Frontier trunk, hidden for security purposes)
- **TCP Port**: **5060**
- **UDP Port**: **5060**
- Click **Finish**

The screen below is a result of the details configured above.

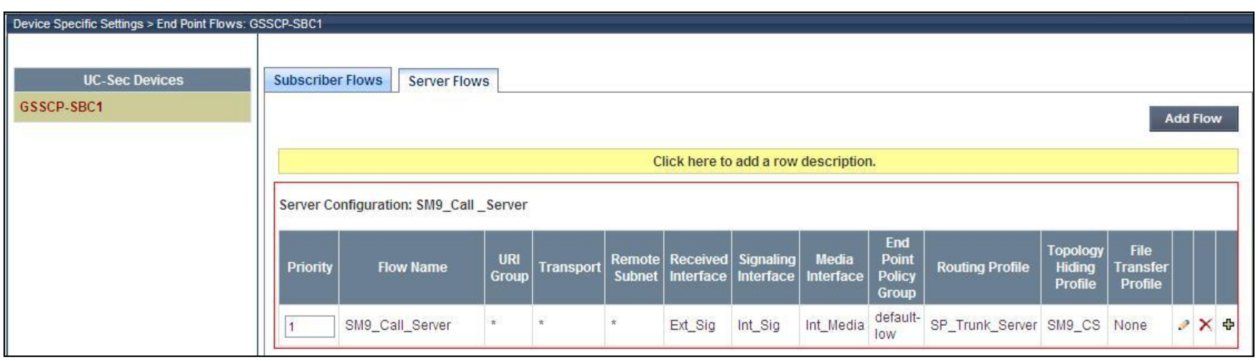


7.3.4. The **End Point Flows** allow the Interfaces**,** Policies and Profiles administered to be used to transport the SIP traffic. From the left-hand menu select **Device Specific Settings → Endpoint Flows.**

- Select the **Server Flows** Tab

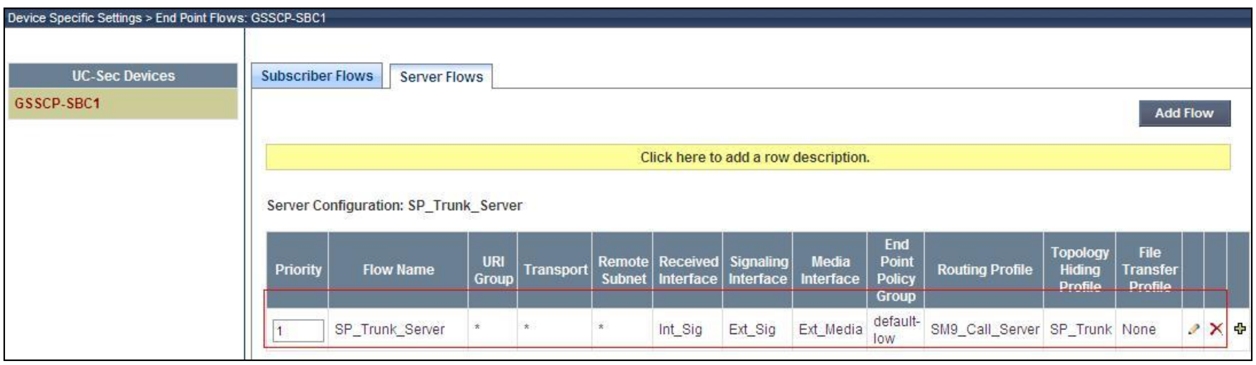
To add the settings for call flow to Session Manager. Click on select **Add Flow.**

- **Name**: **SM9_Call_Server**
- **Server Configuration**: **SM9_Call_Server**
- **URI Group: ***
- **Transport**: *****
- **Remote Subnet**: *****
- **Received Interface**: **Ext_Sig**
- **Signaling Interface**: **Int_Sig**
- **Media Interface**: **Int_Media**
- **End Point Policy Group**: **default-low**
- **Routing Profile**: **SP_Trunk_Server**
- **Topology Hiding Profile**: **SM9_CS**
- **File Transfer Profile**: **None**
- Click **Finish** (not shown)



To add the settings for call flow to Frontier select **Add Flow.**

- **Name**: **SP_Trunk_Server**
- **Server Configuration**: **SP_Trunk_Server**
- **URI Group**: *****
- **Transport**: *****
- **Remote Subnet**: *****
- **Received Interface**: **Int_Sig**
- **Signaling Interface**: **Ext_Sig**
- **Media Interface**: **Ext_Media**
- **End Point Policy Group**: **default-low**
- **Routing Profile**: **SM9_Call_Server**
- **Topology Hiding Profile**: **SP_Trunk**
- **File Transfer Profile**: **None**
- Click **Finish**



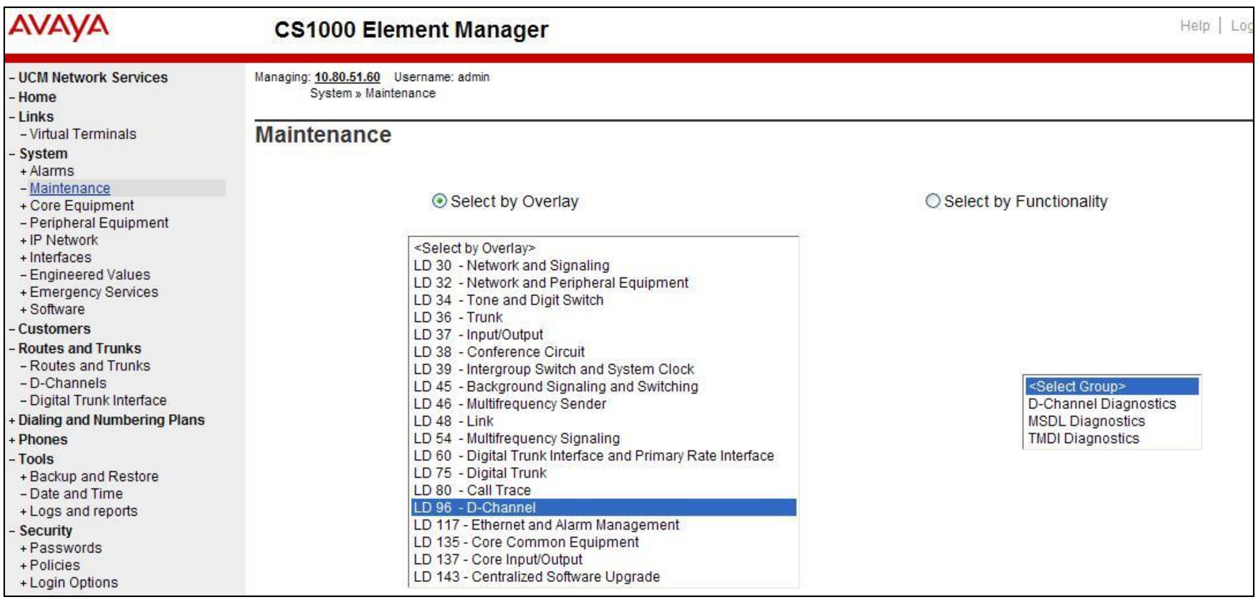
8. Service Provider Configuration

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

9. Verification Steps

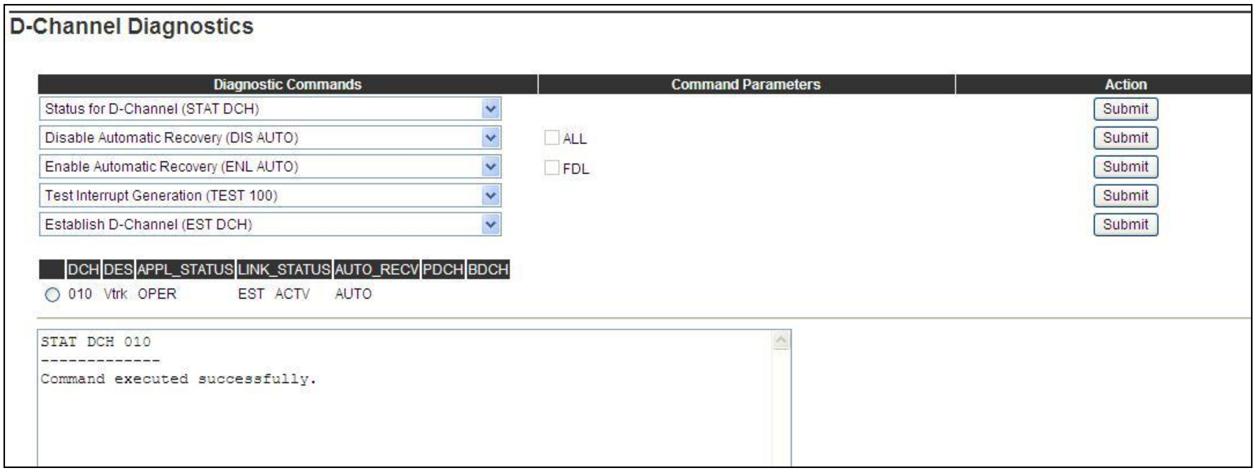
9.1. Verify Avaya Communication Server 1000E Operational Status

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



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

- **Appl_Status** Verify status is **OPER**
- **Link_Status** Verify status is **EST ACTV**



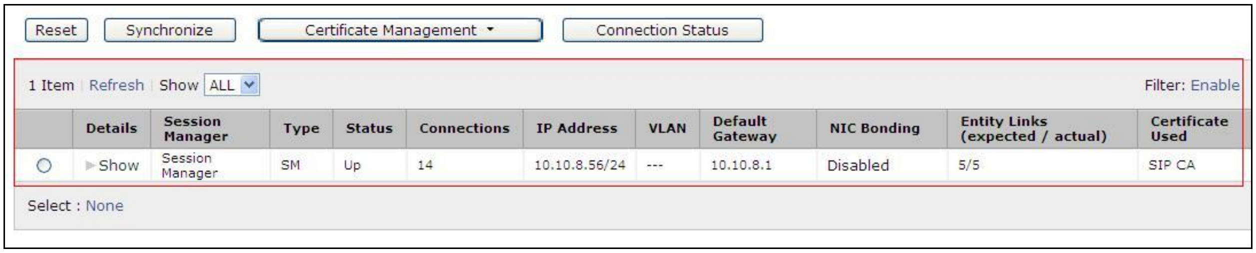
9.2. Verify Avaya Aura® Session Manager Operational Status

9.2.1. Verify Avaya Aura® Session Manager is Operational

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

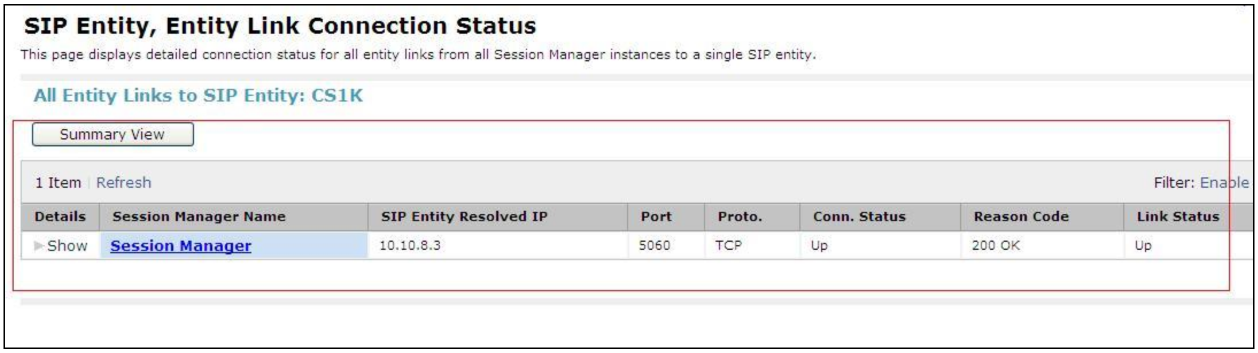
- Tests Pass
- Security Module
- Service State

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



9.2.2. Verify SIP Entity Link Status

Navigate to **Elements → Session Manager → System Status → SIP Entity Monitoring** (not shown) to view more detailed status information for one of the SIP Entity Links. Select the SIP Entity for Communication Server 1000Efrom the **All Monitored SIP Entities** table (not shown) to open the **SIP Entity, Entity Link Connection Status** page. In the **All Entity Links to SIP Entity: CS1000 Rel7.5** table, verify the **Conn. Status** for the link is **Up** as shown below.



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

10. Conclusion

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

11. References

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

[1] Avaya Aura® Session Manager Overview, Doc ID 03-603323, available at http://support.avaya.com.

[2] Installing and Configuring Avaya Aura® Session Manager, available at http://support.avaya.com.

[3] Avaya Aura® Session Manager Case Studies, available at http://support.avaya.com

[4] Maintaining and Troubleshooting Avaya Aura® Session Manager, Doc ID 03-603325, available at http://support.avaya.com.

[5] Administering Avaya Aura® Session Manager, Doc ID 03-603324, available at http://support.avaya.com

[6] IP Peer Networking Installation and Commissioning, Release 7.5, Document Number NN43001-313, available at http://support.avaya.com

[7] Unified Communications Management Common Services Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-116, available at http://support.avaya.com

[8] Network Routing Service Fundamentals, Release 7.5, Document Number NN43001-130, Issue 03.02, available at http://support.avaya.com

[9] Co-resident Call Server and Signaling Server Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-509, available at http://support.avaya.com

[10] Signaling Server and IP Line Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-125, available at http://support.avaya.com

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

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

Appendix A
Avaya Communication Server 1000E Software

Communication Server 1000E call server patches and plug ins

```
17/01/12 13:16:37
TID: 46379

VERSION 4121

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

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

RELEASE 7
ISSUE 50 Q  +
IDLE_SET_DISPLAY NORTEL
DepList 1: core Issue: 01(created: 2012-01-10 16:47:54 (est))

MDP>LAST SUCCESSFUL MDP REFRESH :2012-01-17 13:01:58(Local Time)
MDP>USING DEPLIST ZIP FILE DOWNLOADED :2012-01-11 11:07:13(est)
SYSTEM HAS NO USER SELECTED PEPS IN-SERVICE


LOADWARE VERSION: PSWV 100+

INSTALLED LOADWARE PEPS : 1
PAT#  CR #            PATCH REF #     NAME            DATE        FILENAME
00    wi00832543      ISS1:1OF1       DSP1AB04        24/05/2011  DSP1AB04.LW


ENABLED PLUGINS : 1

PLUGIN    STATUS      PRS/CR_NUM    MPLR_NUM      DESCRIPTION
-------------------------------------------------------------
501       ENABLED     Q02138637     MPLR30070     Enables blind transfer to a SIP endpoint even
if SIP UPDATE is not supported by the far end
```

Communication Server 1000E call server deplists

```
VERSION 4121
RELEASE 7
ISSUE 50 Q +
DepList 1: core Issue: 01 (created: 2012-01-10 16:47:54 (est))

IN-SERVICE PEPS
PAT# CR #            PATCH REF #     NAME      DATE        FILENAME       SPECINS
000  wi00832106      ISS1:1OF1       p30550_1  17/01/2012  p30550_1.cpl   NO
001  wi00835294      ISS1:1OF1       p30565_1  17/01/2012  p30565_1.cpl   NO
002  wi00897176      ISS1:1OF1       p30418_1  17/01/2012  p30418_1.cpl   NO
003  wi00925218      ISS1:1OF1       p30675_1  17/01/2012  p30675_1.cpl   NO
004  wi00839821      ISS1:1OF1       p30619_1  17/01/2012  p30619_1.cpl   NO
005  wi00957141      ISS1:1OF1       p31579_1  17/01/2012  p31579_1.cpl   NO
006  wi00842409      ISS1:1OF1       p30621_1  17/01/2012  p30621_1.cpl   NO
007  wi00838073      ISS1:1OF1       p30588_1  17/01/2012  p30588_1.cpl   NO
008  wi00937114      ISS1:1OF1       p31310_1  17/01/2012  p31310_1.cpl   NO
009  wi00841980      ISS1:1OF1       p30618_1  17/01/2012  p30618_1.cpl   NO
010  wi00836981      ISS1:1OF1       p30613_1  17/01/2012  p30613_1.cpl   NO
011  wi00839255      ISS1:1OF1       p30591_1  17/01/2012  p30591_1.cpl   NO
012  wi00843623      ISS1:1OF1       p30731_1  17/01/2012  p30731_1.cpl   YES
013  WI00843571      ISS1:1OF1       p30627_1  17/01/2012  p30627_1.cpl   NO
014  wi00871739      ISS1:1OF1       p30856_1  17/01/2012  p30856_1.cpl   NO
```

015	wi00852365	ISS1:1OF1	p30707_1	17/01/2012	p30707_1.cpl	NO
016	wi00852389	ISS1:1OF1	p30641_1	17/01/2012	p30641_1.cpl	NO
017	wi00839134	ISS1:1OF1	p30698_1	17/01/2012	p30698_1.cpl	YES
018	wi00856702	ISS1:1OF1	p30573_1	17/01/2012	p30573_1.cpl	NO
019	wi00857566	ISS1:1OF1	p30766_1	17/01/2012	p30766_1.cpl	NO
020	wi00850521	ISS1:1OF1	p30709_1	17/01/2012	p30709_1.cpl	YES
021	wi00903381	ISS1:1OF1	p30421_1	17/01/2012	p30421_1.cpl	NO
022	wi00863876	ISS1:1OF1	p30787_1	17/01/2012	p30787_1.cpl	NO
023	WI00853473	ISS1:1OF1	p30625_1	17/01/2012	p30625_1.cpl	NO
024	wi00854130	ISS1:1OF1	p30443_1	17/01/2012	p30443_1.cpl	NO
025	wi00875425	ISS1:1OF1	p30943_1	17/01/2012	p30943_1.cpl	NO
026	wi00927678	ISS1:1OF1	p31399_1	17/01/2012	p31399_1.cpl	NO
027	wi00875701	ISS1:1OF1	p30942_1	17/01/2012	p30942_1.cpl	NO
028	wi00853031	ISS1:1OF1	p30531_1	17/01/2012	p30531_1.cpl	NO
029	wi00877367	ISS1:1OF1	p30534_1	17/01/2012	p30534_1.cpl	NO
030	wi00871969	ISS1:1OF1	p30768_1	17/01/2012	p30768_1.cpl	NO
031	wi00886321	ISS1:1OF1	p31009_1	17/01/2012	p31009_1.cpl	NO
032	WI00836334	ISS1:1OF1	p30481_1	17/01/2012	p30481_1.cpl	NO
033	wi00836182	ISS1:1OF1	p30450_1	17/01/2012	p30450_1.cpl	NO
034	wi00858335	ISS1:1OF1	p30819_1	17/01/2012	p30819_1.cpl	NO
035	wi00860279	ISS1:1OF1	p30789_1	17/01/2012	p30789_1.cpl	NO
036	wi00953900	ISS1:1OF1	p31494_1	17/01/2012	p31494_1.cpl	NO
037	wi00854415	ISS1:1OF1	p30593_1	17/01/2012	p30593_1.cpl	NO
038	WI00836292	ISS1:1OF1	p30554_1	17/01/2012	p30554_1.cpl	NO
039	WI00839794	ISS1:1OF1	p28647_1	17/01/2012	p28647_1.cpl	NO
040	wi00824257	ISS1:1OF1	p30447_1	17/01/2012	p30447_1.cpl	NO
041	wi00827950	ISS2:1OF1	p30471_2	17/01/2012	p30471_2.cpl	NO
042	wi00949273	ISS1:1OF1	p31411_1	17/01/2012	p31411_1.cpl	NO
043	WI00854150	ISS1:1OF1	p30468_1	17/01/2012	p30468_1.cpl	NO
044	wi00873382	ISS1:1OF1	p30832_1	17/01/2012	p30832_1.cpl	NO
045	wi00853178	ISS1:1OF1	p30719_1	17/01/2012	p30719_1.cpl	NO
046	wi00869695	ISS1:1OF1	p30654_1	17/01/2012	p30654_1.cpl	NO
047	wi00834382	ISS1:1OF1	p30548_1	17/01/2012	p30548_1.cpl	NO
048	wi00951427	ISS1:1OF1	p31478_1	17/01/2012	p31478_1.cpl	NO
049	wi00946558	ISS1:1OF1	p31358_1	17/01/2012	p31358_1.cpl	NO
050	wi00903369	ISS1:1OF1	p31165_1	17/01/2012	p31165_1.cpl	NO
051	wi00927321	ISS1:1OF1	p31286_1	17/01/2012	p31286_1.cpl	YES
052	wi00923899	ISS1:1OF1	p31270_1	17/01/2012	p31270_1.cpl	NO
053	wi00949627	ISS1:1OF1	p31462_1	17/01/2012	p31462_1.cpl	NO
054	wi00962557	ISS1:1OF1	p31581_1	17/01/2012	p31581_1.cpl	NO
055	wi00865477	ISS1:1OF1	p30894_1	17/01/2012	p30894_1.cpl	YES
056	wi00962211	ISS1:1OF1	p31580_1	17/01/2012	p31580_1.cpl	NO
057	wi00883604	ISS1:1OF1	p30973_1	17/01/2012	p30973_1.cpl	NO
058	wi00898327	ISS1:1OF1	p31136_1	17/01/2012	p31136_1.cpl	NO
059	wi00856410	ISS1:1OF1	p30749_1	17/01/2012	p30749_1.cpl	NO
060	wi00932948	ISS1:1OF1	p31077_1	17/01/2012	p31077_1.cpl	NO
061	wi00905600	ISS1:1OF1	p31201_1	17/01/2012	p31201_1.cpl	NO
062	wi00865477	ISS1:1OF1	p30897_1	17/01/2012	p30897_1.cpl	YES
063	wi00879526	ISS1:1OF1	p31007_1	17/01/2012	p31007_1.cpl	NO
064	wi00962955	ISS1:1OF1	p31585_1	17/01/2012	p31585_1.cpl	NO
065	wi00865477	ISS1:1OF1	p30890_1	17/01/2012	p30890_1.cpl	YES
066	wi00907707	ISS1:1OF1	p31228_1	17/01/2012	p31228_1.cpl	NO
067	wi00857362	ISS1:1OF1	p30782_1	17/01/2012	p30782_1.cpl	NO
068	wi00877442	ISS1:1OF1	p30844_1	17/01/2012	p30844_1.cpl	NO
069	wi00894443	ISS1:1OF1	p31093_1	17/01/2012	p31093_1.cpl	NO
070	wi00942734	ISS1:1OF1	p31409_1	17/01/2012	p31409_1.cpl	NO
071	wi00841273	ISS1:1OF1	p30713_1	17/01/2012	p30713_1.cpl	NO
072	WI00900213	ISS1:1OF1	p30656_1	17/01/2012	p30656_1.cpl	NO
073	wi00948931	ISS1:1OF1	p31407_1	17/01/2012	p31407_1.cpl	NO
074	wi00891626	ISS1:1OF1	p31051_1	17/01/2012	p31051_1.cpl	YES
075	wi00929140	ISS1:1OF1	p31284_1	17/01/2012	p31284_1.cpl	NO
076	wi00925208	ISS1:1OF1	p30986_1	17/01/2012	p30986_1.cpl	NO
077	wi00958776	ISS1:1OF1	p31542_1	17/01/2012	p31542_1.cpl	YES
078	wi00880836	ISS1:1OF1	p30976_1	17/01/2012	p30976_1.cpl	NO
079	WI00927300	ISS1:1OF1	p30999_1	17/01/2012	p30999_1.cpl	NO
080	wi00943172	ISS1:1OF1	p31402_1	17/01/2012	p31402_1.cpl	NO
081	wi00826075	ISS1:1OF1	p30452_1	17/01/2012	p30452_1.cpl	NO
082	wi00881777	ISS1:1OF1	p25747_1	17/01/2012	p25747_1.cpl	NO
083	wi00948274	ISS1:1OF1	p31365_1	17/01/2012	p31365_1.cpl	NO
084	wi00908933	ISS1:1OF1	p31239_1	17/01/2012	p31239_1.cpl	NO

085	wi00865477	ISS1:1OF1	p30892_1	17/01/2012	p30892_1.cpl	YES
086	wi00867905	ISS1:1OF1	p30640_1	17/01/2012	p30640_1.cpl	NO
087	wi00961267	ISS1:1OF1	p30288_1	17/01/2012	p30288_1.cpl	NO
088	wi00930864	ISS1:1OF1	p31325_1	17/01/2012	p31325_1.cpl	NO
089	wi00898200	ISS1:1of1	p31274_1	17/01/2012	p31274_1.cpl	NO
090	wi00946876	ISS1:1OF1	p31430_1	17/01/2012	p31430_1.cpl	NO
091	wi00936714	ISS1:1OF1	p31379_1	17/01/2012	p31379_1.cpl	NO
092	wi00951925	ISS1:1OF1	p31486_1	17/01/2012	p31486_1.cpl	NO
093	wi00921340	ISS1:1OF1	p31266_1	17/01/2012	p31266_1.cpl	NO
094	wi00956885	ISS1:1OF1	p31489_1	17/01/2012	p31489_1.cpl	NO
095	wi00959854	ISS1:1OF1	p31556_1	17/01/2012	p31556_1.cpl	NO
096	wi00946282	ISS1:1OF1	p31204_1	17/01/2012	p31204_1.cpl	NO
097	wi00840590	ISS1:1OF1	p30767_1	17/01/2012	p30767_1.cpl	NO
098	wi00897082	ISS1:1OF1	p31124_1	17/01/2012	p31124_1.cpl	NO
099	wi00896394	ISS1:1OF1	p30807_1	17/01/2012	p30807_1.cpl	NO
100	wi00909476	ISS1:1OF1	p31340_1	17/01/2012	p31340_1.cpl	NO
101	wi00887744	ISS2:1OF1	p31026_2	17/01/2012	p31026_2.cpl	NO
102	wi00865477	ISS1:1OF1	p30896_1	17/01/2012	p30896_1.cpl	YES
103	wi00957252	ISS1:1OF1	p31530_1	17/01/2012	p31530_1.cpl	NO
104	wi00859123	ISS1:1OF1	p30648_1	17/01/2012	p30648_1.cpl	NO
105	wi00895181	ISS1:1OF1	p31106_1	17/01/2012	p31106_1.cpl	NO
106	wi00938555	ISS1:1OF1	p30881_1	17/01/2012	p30881_1.cpl	YES
107	wi00941500	ISS1:1OF1	p31394_1	17/01/2012	p31394_1.cpl	NO
108	wi00931028	ISS1:1OF1	p31354_1	17/01/2012	p31354_1.cpl	YES
109	wi00907697	ISS1:1OF1	p31227_1	17/01/2012	p31227_1.cpl	NO
110	wi00905660	ISS1:1OF1	p27968_1	17/01/2012	p27968_1.cpl	NO
111	wi00900096	ISS1:1OF1	p31006_1	17/01/2012	p31006_1.cpl	NO
112	wi00900766	ISS1:1OF1	p31159_1	17/01/2012	p31159_1.cpl	NO
113	wi00865477	ISS1:1OF1	p30898_1	17/01/2012	p30898_1.cpl	YES
114	wi00906022	ISS1:1OF1	p31202_1	17/01/2012	p31202_1.cpl	NO
115	wi00856991	ISS1:1OF1	p17588_1	17/01/2012	p17588_1.cpl	NO
116	wi00880386	ISS1:1OF1	p30977_1	17/01/2012	p30977_1.cpl	NO
117	wi00688381	ISS1:1OF1	p30104_1	17/01/2012	p30104_1.cpl	NO
118	wi00908598	ISS1:1OF1	p31235_1	17/01/2012	p31235_1.cpl	NO
119	wi00890475	p30952	p31048_1	17/01/2012	p31048_1.cpl	NO
120	wi00868729	ISS1:1OF1	p31163_1	17/01/2012	p31163_1.cpl	NO
121	wi00952381	ISS1:1OF1	p31410_1	17/01/2012	p31410_1.cpl	NO
122	wi00859499	ISS1:1OF1	p30694_1	17/01/2012	p30694_1.cpl	NO
123	wi00895090	ISS1:1OF1	p31105_1	17/01/2012	p31105_1.cpl	NO
124	wi00869243	ISS1:1OF1	p30848_1	17/01/2012	p30848_1.cpl	NO
125	wi00937119	ISS1:1OF1	p28005_1	17/01/2012	p28005_1.cpl	NO
126	wi00899584	ISS1:1OF1	p30809_1	17/01/2012	p30809_1.cpl	NO
127	wi00932204	ISS2:1OF1	p31305_2	17/01/2012	p31305_2.cpl	NO
128	wi00951837	ISS1:1OF1	p31485_1	17/01/2012	p31485_1.cpl	NO
129	wi00865477	ISS1:1OF1	p30893_1	17/01/2012	p30893_1.cpl	YES
130	wi00946477	ISS1:1OF1	p31426_1	17/01/2012	p31426_1.cpl	NO
131	wi00946681	ISS1:1OF1	p31428_1	17/01/2012	p31428_1.cpl	NO
132	wi00855423	ISS1:1OF1	p31328_1	17/01/2012	p31328_1.cpl	YES
133	wi00900668	ISS1:1OF1	p30456_1	17/01/2012	p30456_1.cpl	NO
134	wi00862574	iss1:1of1	p30870_1	17/01/2012	p30870_1.cpl	NO
135	wi00894243	ISS1:1OF1	p31087_1	17/01/2012	p31087_1.cpl	NO
136	wi00959820	ISS1:1OF1	p31562_1	17/01/2012	p31562_1.cpl	NO
137	WI00889786	ISS1:1OF1	p30750_1	17/01/2012	p30750_1.cpl	NO
138	wi00943748	ISS1:1OF1	p31516_1	17/01/2012	p31516_1.cpl	NO
139	wi00950592	ISS1:1OF1	p31499_1	17/01/2012	p31499_1.cpl	NO
140	WI00928455	ISS1:1OF1	p31297_1	17/01/2012	p31297_1.cpl	NO
141	wi00896680	ISS1:1OF1	p30357_1	17/01/2012	p30357_1.cpl	NO
142	wi00925141	ISS1:1OF1	p30802_1	17/01/2012	p30802_1.cpl	NO
143	wi00865477	ISS1:1OF1	p30891_1	17/01/2012	p30891_1.cpl	YES
144	wi00884699	ISS1:1OF1	p31000_1	17/01/2012	p31000_1.cpl	YES
145	wi00932958	ISS1:1OF1	p31115_1	17/01/2012	p31115_1.cpl	NO
146	wi00921295	ISS1:1OF1	p31265_1	17/01/2012	p31265_1.cpl	NO
147	wi00906163	ISS1:1OF1	p31205_1	17/01/2012	p31205_1.cpl	NO
148	wi00903437	ISS1:1OF1	p31167_1	17/01/2012	p31167_1.cpl	NO
149	wi00960133	ISS2:1OF1	p31557_2	17/01/2012	p31557_2.cpl	NO
150	wi00879322	ISS1:1OF1	p30954_1	17/01/2012	p30954_1.cpl	NO
151	wi00896420	ISS1:1OF1	p30867_1	17/01/2012	p30867_1.cpl	NO
152	wi00903085	ISS1:1OF1	p31164_1	17/01/2012	p31164_1.cpl	NO
153	wi00877592	ISS1:1OF1	p30880_1	17/01/2012	p30880_1.cpl	NO
154	wi00958682	ISS1:1OF1	p31540_1	17/01/2012	p31540_1.cpl	NO

```
155  wi00882293      ISS1:1OF1       p31010_1  17/01/2012  p31010_1.cpl   NO
156  wi00905297      ISS1:1OF1       p31195_1  17/01/2012  p31195_1.cpl   NO
157  wi00833910      ISS2:1OF1       p30492_2  17/01/2012  p30492_2.cpl   NO
158  wi00865477      ISS1:1OF1       p30895_1  17/01/2012  p30895_1.cpl   YES
159  wi00897096      ISS1:1OF1       p30676_1  17/01/2012  p30676_1.cpl   NO
160  wi00945533      ISS1:1OF1       p31421_1  17/01/2012  p31421_1.cpl   YES
MDP>LAST SUCCESSFUL MDP REFRESH :2012-01-17 13:01:58(Local Time)
MDP>USING DEPLIST ZIP FILE DOWNLOADED :2012-01-11 11:07:13(est)
```

Communication Server 1000E signaling server service updates

```
Product Release: 7.50.17.00
In system patches: 1
PATCH#  NAME       IN_SERVICE   DATE      SPECINS  TYPE   RPM
0       p30253_1   Yes          17/01/12  NO       FRU    cs1000-pi-control-1.00.00.00-00.noarch

Product Release: 7.50.17.00
In System service updates: 19
PATCH#  IN_SERVICE   DATE       SPECINS   REMOVABLE   NAME
4       Yes          18/04/11   NO        YES         cs1000-dbcom-7.50.17-02.i386.000
9       Yes          17/01/12   NO        YES         cs1000-patchWeb-7.50.17.16-2.i386.000
10      Yes          17/01/12   NO        yes         cs1000-sps-7.50.17.16-01.i386.000
11      Yes          17/01/12   NO        YES         cs1000-baseWeb-7.50.17.16-1.i386.001
12      Yes          17/01/12   NO        YES         cs1000-shared-pbx-7.50.17.16-1.i386.000
13      Yes          17/01/12   NO        YES         cs1000-kcv-7.50.17.16-1.i386.000
14      Yes          17/01/12   NO        YES         cs1000-dmWeb-7.50.17.16-1.i386.000
15      Yes          17/01/12   NO        YES         cs1000-ipsec-7.50.17.16-1.i386.000
16      Yes          17/01/12   NO        YES         cs1000-ftrpkg-7.50.17.16-5.i386.000
17      Yes          17/01/12   NO        YES         cs1000-tps-7.50.17.16-8.i386.000
18      Yes          17/01/12   NO        YES         cs1000-csmWeb-7.50.17.16-2.i386.000
19      Yes          17/01/12   NO        YES         ipsec-tools-0.6.5-14.el5.3_avaya_1.i386.000
20      Yes          17/01/12   NO        YES         spiritAgent-6.1-1.0.0.108.208.i386.000
21      Yes          17/01/12   NO        YES         cs1000-EmCentralLogic-7.50.17.16-1.i386.000
22      Yes          17/01/12   NO        YES         cs1000-Jboss-Quantum-7.50.17.16-8.i386.000
23      Yes          17/01/12   NO        YES         cs1000-bcc-7.50.17.16-31.i386.000
24      Yes          17/01/12   NO        YES         cs1000-emWeb_6-0-7.50.17.16-9.i386.000
25      Yes          17/01/12   NO        YES         cs1000-linuxbase-7.50.17.16-5.i386.000
26      Yes          17/01/12   NO        YES         cs1000-vtrk-7.50.17.16-26.i386.000
```

Communication Server 1000E system software

```
Product Release: 7.50.17.00
Base Applications
   base                         7.50.17     [patched]
   NTAFS                        7.50.17
   sm                           7.50.17
   cs1000-Auth                  7.50.17
   Jboss-Quantum                7.50.17     [patched]
   lhmonitor                    7.50.17
   baseAppUtils                 7.50.17     [patched]
   dfoTools                     7.50.17
   nnnm                         7.50.17
   cppmUtil                     7.50.17
   oam-logging                  7.50.17     [patched]
   dmWeb                        n/a         [patched]
   baseWeb                      n/a         [patched]
   ipsec                        n/a         [patched]
   Snmp-Daemon-TrapLib          7.50.17
   ISECSH                       7.50.17
   patchWeb                     n/a         [patched]
   EmCentralLogic               n/a         [patched]
Application configuration: CS+SS+EM
Packages:
CS+SS+EM
Configuration version:     7.50.17-00
   cs                           7.50.17
   dbcom                        7.50.17     [patched]
   cslogin                      7.50.17
```

```
    sigServerShare              7.50.17     [patched]
    csv                         7.50.17
    tps                         7.50.17.16  [patched]
    vtrk                        7.50.17.16  [patched]
    pd                          7.50.17
    sps                         7.50.17.16  [patched]
    ncs                         7.50.17
    gk                          7.50.17
    EmConfig                    7.50.17
    emWeb_6-0                   7.50.17     [patched]
    emWebLocal_6-0              7.50.17
    csmWeb                      7.50.17     [patched]
    bcc                         7.50.17     [patched]
    ftrpkg                      7.50.17     [patched]
    cs1000WebService_6-0        7.50.17
    managedElementWebService    7.50.17
    mscAnnc                     7.50.17
    mscAttn                     7.50.17
    mscConf                     7.50.17
    mscMusc                     7.50.17
    mscTone                     7.50.17
```

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.