Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Communication Server 1000E R7.5 with Avaya Aura® Session Manager R6.1 and Avaya Aura® Session Border Controller to support BT Global Services NOAS SIP Trunk - Issue 1.1

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between an Avaya SIP enabled enterprise solution and the BT Global Services NOAS SIP Trunk Service. The Avaya solution consists of an Avaya Aura® Session Manager and an Avaya Communication Server 1000E connected to an Avaya Aura® Session Border Controller. BT is a member of the Global 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 necessary steps to configure Session Initiation Protocol (SIP) trunking between an Avaya SIP enabled enterprise solution and the BT Global Services NOAS SIP Trunk Service. The Avaya solution consists of an Avaya Aura® Session Manager, an Avaya Communication Server 1000E and an Avaya Aura® Session Border Controller (AASBC) connected to the BT SIP Trunk Service. Customers using this Avaya SIP enabled enterprise solution with the BT SIP Trunk Service are able to place and receive PSTN calls via a dedicated Internet connection using the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks. The approach normally results in lower cost and a more flexible implementation for the enterprise customers.

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, Communication Server 1000E and the AASBC. The enterprise site was configured to use the SIP Trunk Service provided by BT, with all PSTN traffic transiting via the BT SIP Trunk Service.

2.1. Interoperability Compliance Testing

The interoperability test included the following:

- Incoming calls to the enterprise site from the PSTN were routed to the DID numbers assigned by BT. Incoming PSTN calls were terminated on Digital, Unistim, SIP and Analog telephones at the enterprise side.
- Outgoing calls from the enterprise site were completed via BT to PSTN telephones. Outgoing calls from the enterprise to the PSTN were made from Digital, Unistim, SIP and Analog telephones.
- Calls were made using G.729A, and G.711A codec's.
- Fax calls to/from a group 3 fax machine to a PSTN connected fax machine using T.38 transmission.
- DTMF transmission using RFC 2833 with successful IVR menu progression.
- 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 of SIP OPTIONS messages sent by BT requiring Avaya response and sent by Avaya requiring BT response.

2.2. Test Results

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

- No inbound toll free numbers were tested, however routing of inbound DID numbers and the relevant number translation was successfully tested.
- Routing to emergency numbers (such as 112) was not tested.
- G729 annex b (silence suppression) is not supported by BT SIP Trunk Service and thus was not tested.
- Early media is only supported for UEXT type phones on Communication Server 1000E.
- PSTN called party hanging up an active call did not cause the call to drop. The Communication Server 1000E caller must hang up first, or wait for the PSTN T2ISUP timer to expire.
- Unsupervised transfer of incoming or outgoing PSTN calls to PSTN called parties is not permitted. The same restriction exists for supervised transfers of an existing PSTN call to a PSTN called party. This is due to configuration restrictions imposed by the local PSTN the NOAS SIP Trunk service was connected to.
- Call hold has a time limit of 15 minutes. If this limit is exceeded the call drops. This is due to the NOAS SIP Session timer refresh not refreshing the session. BT has produced a system patch to address this problem. The patch has not been independently verified by the compliance test process.
- Calls to/from SMC 3456 soft clients using unsupported codecs failed, most likely because the call server was unable to determine the phone capabilities and the SMC 3456 not correctly handling the calls.
- The BT SIP Trunk Service did not handle accumulation of SIP 5xx messages correctly, causing Call Admission Control (CAC) issues with PSTN calls on one occasion, with the effect of disabling the SIP trunks. A workaround was to manually clear the CAC counters.
- Avaya one-X® Communicator three-party-conferences did not work if one or more of the parties was a PSTN user. The affected user received no speech from the conference bridge. This was not observed on non-NOAS SIP trunks.

2.3. Support

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

Avaya customers may obtain documentation and support for Avaya products by visiting http://support.avaya.com. Selecting the **Support Contact Options** link followed by **Maintenance Support** provides the worldwide support directory for Avaya Global Services. Specific numbers are provided for both customers and partners based on the specific type of support or consultation services needed. Some services may require specific Avaya service support agreements. Alternatively, in the United States, (866) GO-AVAYA (866-462-8292) provides access to overall sales and service support menus.

3. Reference Configuration

Figure 1 illustrates the tested configuration. The test configuration shows an Avaya enterprise site connected to the BT SIP Trunk Service. Located at the enterprise site are a Session Manager and a Communication Server 1000E. Endpoints are Avaya 1140e series IP telephones (one with SIP firmware), Avaya 1220 IP telephones, Avaya 3904 series Digital telephones, a one-X Communicator soft phone, an SMC 3456 Soft Client, an Analog Telephone and a Fax Machine. For security purposes, any public IP addresses or PSTN routable phone numbers used in the compliance test are not shown in these Application Notes.

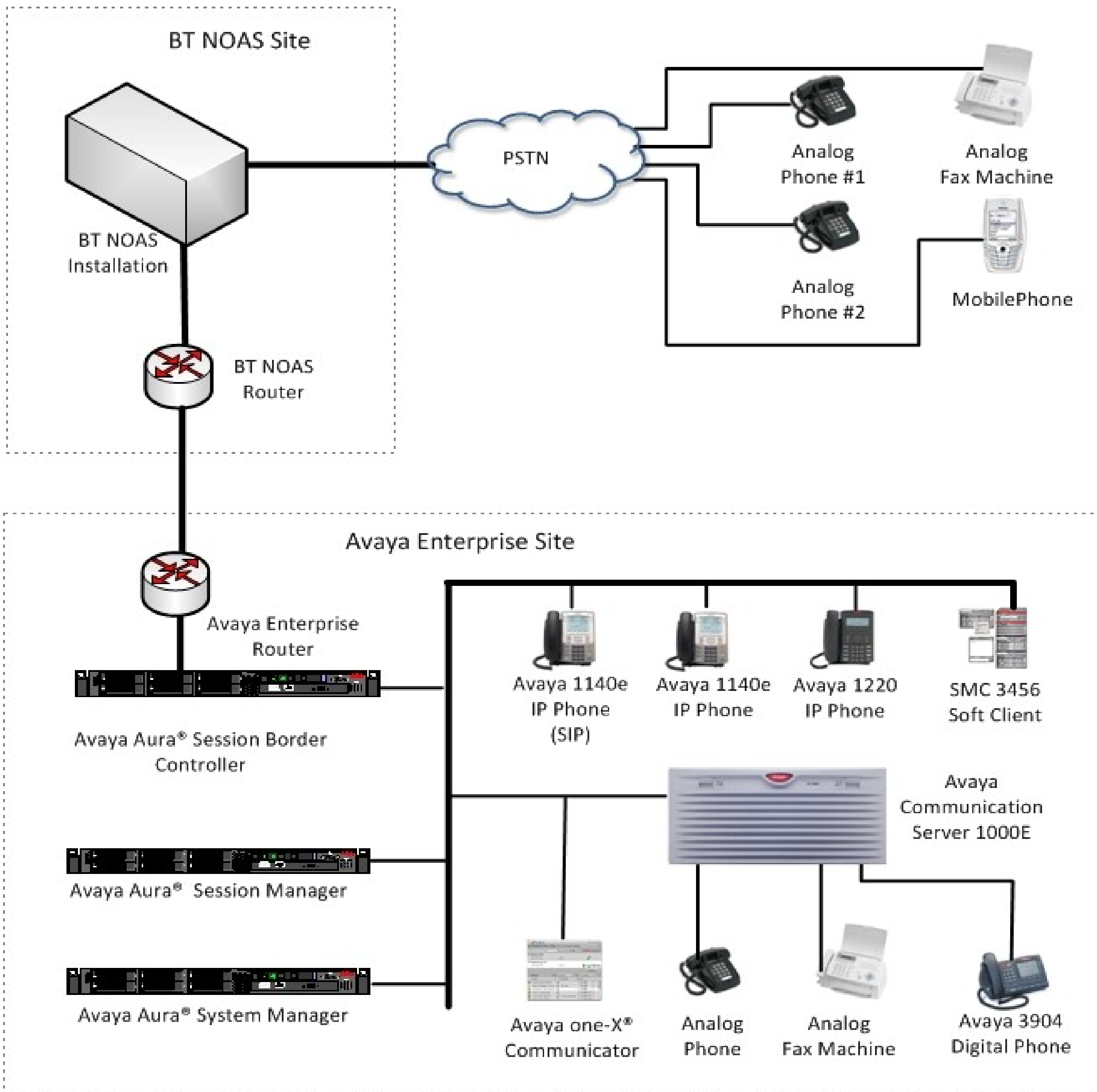


Figure 1: BT NOAS and Avaya Enterprise Test Configuration Network Diagram

4. Equipment and Software Validated

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

Equipment	Software
Avaya Communication Server 1000E	Avaya Communication Server 1000E R7.5 007.50Q/ 7.50.17 (PSWV 100 with latest Patches and Deplist)
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 DSP2 Version: DSP2 AB03
Avaya S8800 Server	Avaya Aura® Session Manager R6.1 (6.1.3.0.613006)
Avaya S8800 Server	Avaya Aura® System Manager R6.1 (6.1.7.1.1260)
Avaya S8800 Server	Avaya Aura® Session Border Controller (E362P4)
Avaya 1140e Unistim Phone	5.0
Avaya 1140e SIP Phone	4.00.03.00
Avaya 1220 Unistim Phone	5.0
Avaya 3904 Digital Phone	AA94
Avaya SMC3456 Soft Client	Version 2.6
Avaya one-X® Communicator	CS6.10.10
Analog Phone	N/A
BT SIP Trunk Service	2.1.0.8

5. Configure Avaya Communication Server 1000E

This section describes the steps required to configure Communication Server 1000E for SIP Trunking and also the basic configuration for telephones (analog, SIP and IP phones). SIP trunks are established between Communication Server 1000E and Session Manager. SIP trunks are also established between Session Manager and the AASBC private interface. The AASBC public interface connects to the BT Global Services NOAS SIP trunks. Incoming PSTN calls from the BT Global Services NOAS SIP Trunk Service traverse the AASBC and are directed to the Session Manager, which directs the calls to Communication Server 1000E (see **Figure 1**).

The AASBC media manager has been configured to ensure RTP packets are managed correctly from the AASBC public interface to the private interface and vice versa. When 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. When Communication Server 1000E selects a SIP trunk for outgoing PSTN calls, SIP signaling is directed to the Session Manager. The Session Manager directs the outbound SIP messages to the AASBC private interface. The AASBC public interface manages outgoing SIP sessions onwards to the BT Global Services NOAS SIP trunks.

Specific Communication Server 1000E configuration was performed using Element Manager and the system terminal interface. The general installation of the Avaya Communication Server 1000E, System Manager, Session Manager and AASBC is presumed to have been previously completed and is not discussed here. Configuration details provided in these application notes draw attention to changes from default system configurations.

5.1. Confirm System Features

The keycode installed on the Call Server controls the maximum values for these attributes. If a required feature is not enabled or there is insufficient capacity, contact an authorized Avaya sales representative for adding additional capacity. Use the Communication Server 1000E system terminal and manually load overlay 22 to print the System Limits (the required command is SLT), and verify that the number of SIP Access Ports reported by the system is sufficient for the combination of trunks to the BT network, and any other SIP trunks needed. See the following screenshot for a typical System Limits printout. The value of **SIP ACCESS PORTS** defines the maximum number of SIP trunks for the Communication Server 1000E.

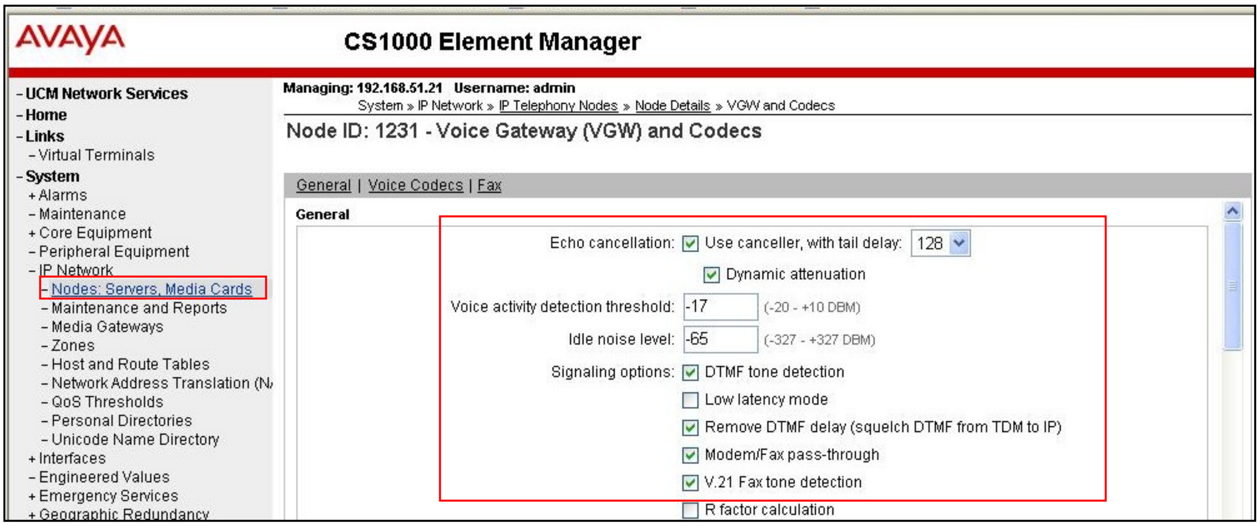
```
System type is - Communication Server 1000E/CP PM
CP PM - Pentium M 1.4 GHz

IPMGs Registered:               4
IPMGs Unregistered:             0
IPMGs Configured/unregistered:  2

TRADITIONAL TELEPHONES   120    LEFT   110    USED    10
DECT USERS                16    LEFT    16    USED     0
IP USERS               10000    LEFT  9954    USED    46
BASIC IP USERS            16    LEFT    13    USED     3
TEMPORARY IP USERS         8    LEFT     8    USED     0
DECT VISITOR USER         16    LEFT    16    USED     0
ACD AGENTS               192    LEFT   185    USED     7
MOBILE EXTENSIONS          8    LEFT     7    USED     1
TELEPHONY SERVICES        16    LEFT    13    USED     3
CONVERGED MOBILE USERS     8    LEFT     8    USED     0
AVAYA SIP LINES           16    LEFT    12    USED     4
THIRD PARTY SIP LINES     16    LEFT    16    USED     0
PCA                       20    LEFT    18    USED     2
ITG ISDN TRUNKS            0    LEFT     0    USED     0
H.323 ACCESS PORTS       524    LEFT   524    USED     0
AST                     6652    LEFT  6640    USED    12
SIP CONVERGED DESKTOPS    16    LEFT    16    USED     0
SIP CTI TR87              16    LEFT     8    USED     8
SIP ACCESS PORTS         524    LEFT   518    USED     6
RAN CON                   90    LEFT    90    USED     0
MUS CON                  120    LEFT   120    USED     0
```

Load overlay 21, and confirm the customer is set up to use **ISDN** trunks (see below).

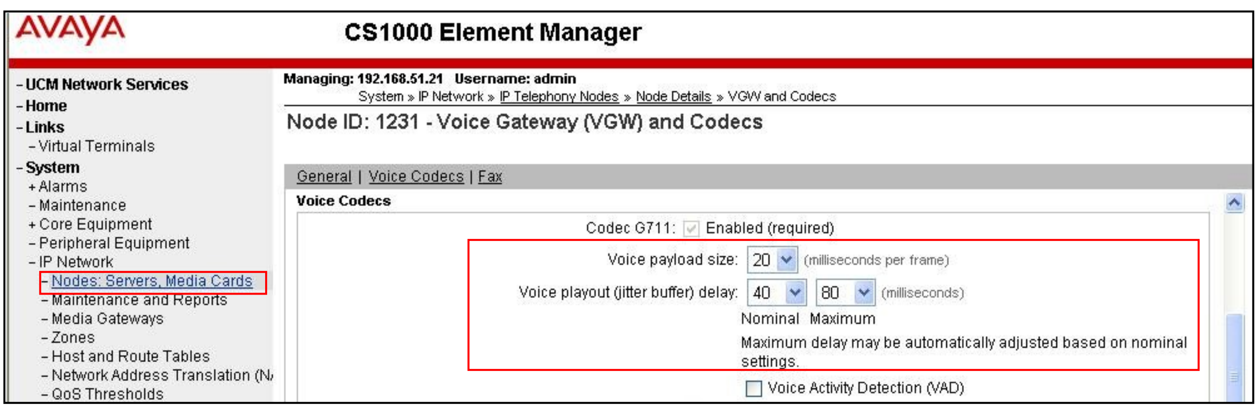
```
REQ: prt
TYPE: net
TYPE NET_DATA
CUST 0

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

5.2. Configure Codec's for Voice and FAX operation

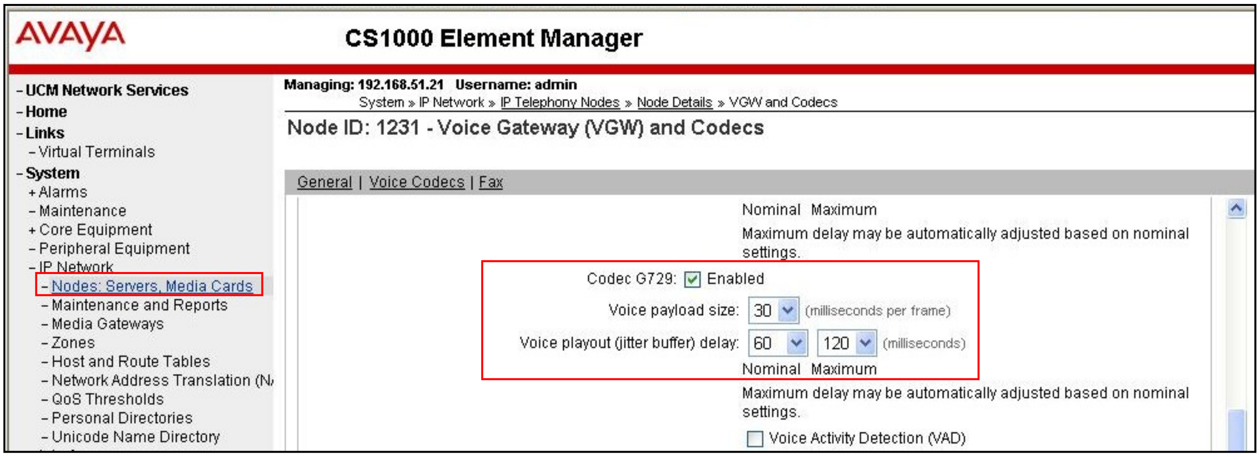
The BT Global Services NOAS SIP Trunk Service supports G.711A and G.729A voice codecs and T.38 FAX transmissions. Using the Communication Server 1000E element manager sidebar, select **System → IP Networks → Nodes: Servers, Media Cards**. Navigate to the **IP Network → IP Telephony Nodes → Node Details → VGW and Codecs** property page and configure the Communication Server 1000E General codec settings as in the following screenshots. The values highlighted were used during testing. The following screenshot shows the necessary **General** settings.



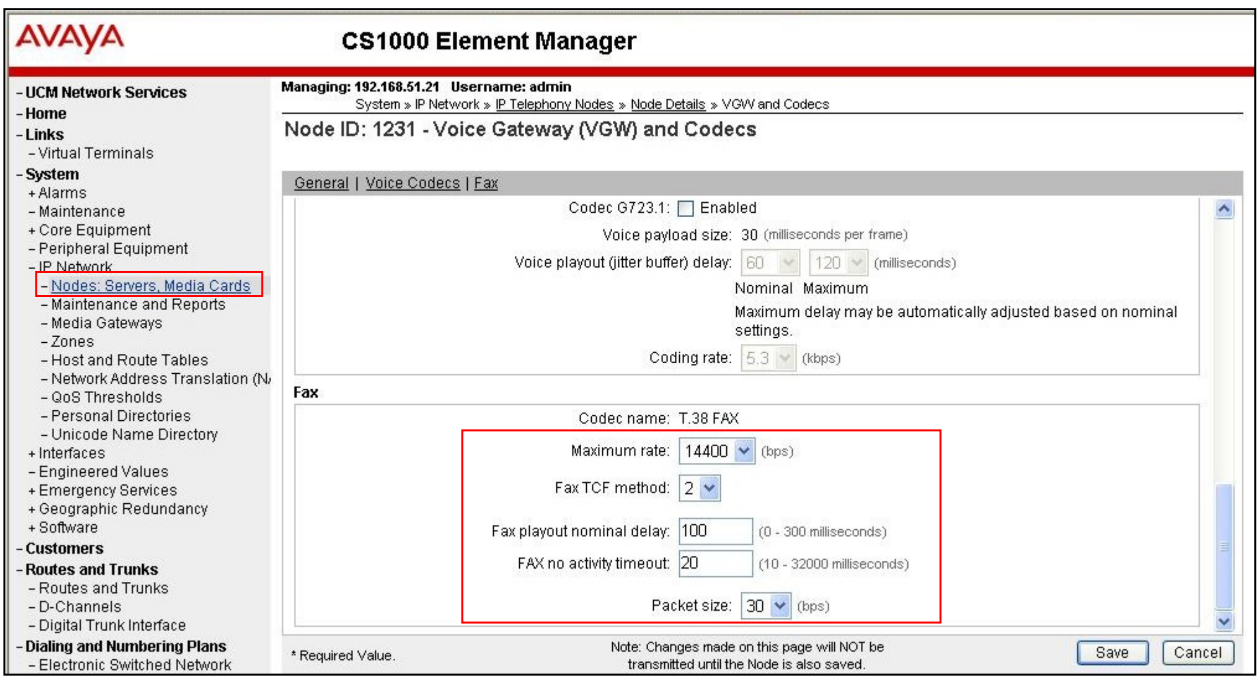
Move down to the **Voice Codecs** section and configure the **G.711** codec settings. The following screenshot shows the G.711 codec settings used for calls.



Next, scroll down to the **G.729** codec section and configure the low bandwidth codec settings.

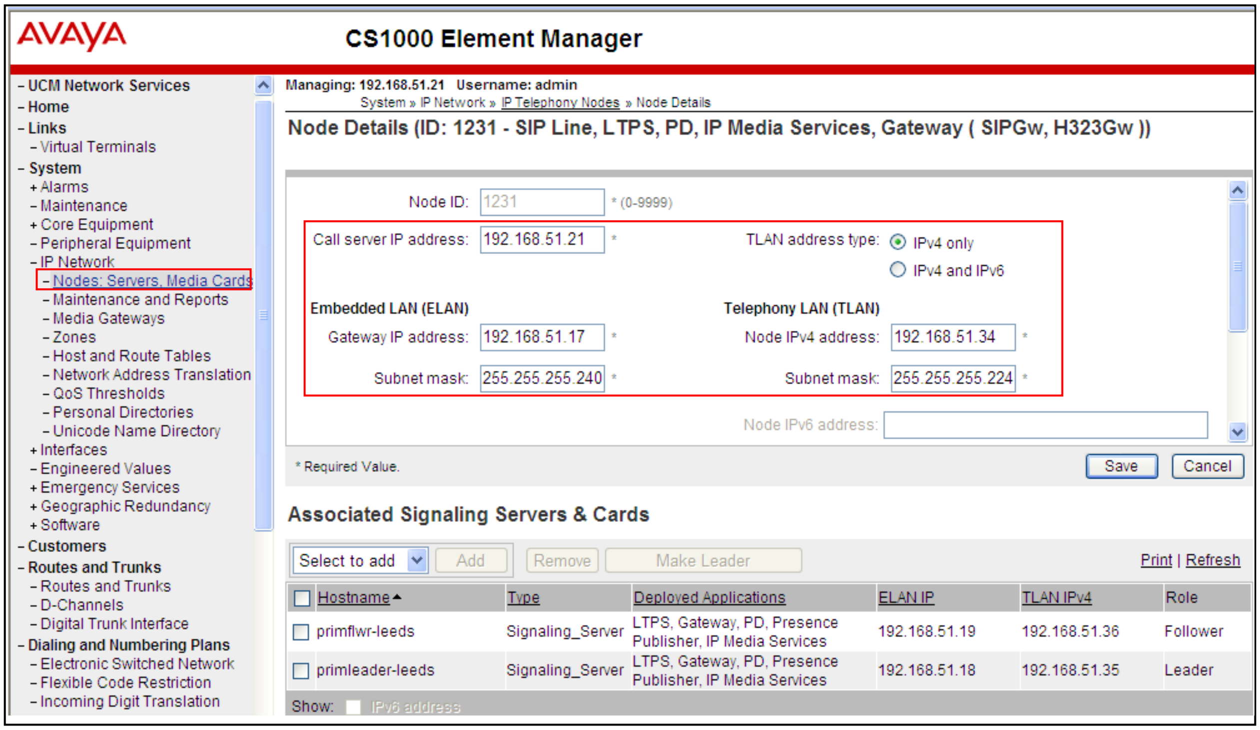


Finally, configure the Fax settings as in the highlighted section of the next screenshot. Click on the **Save** button when finished.

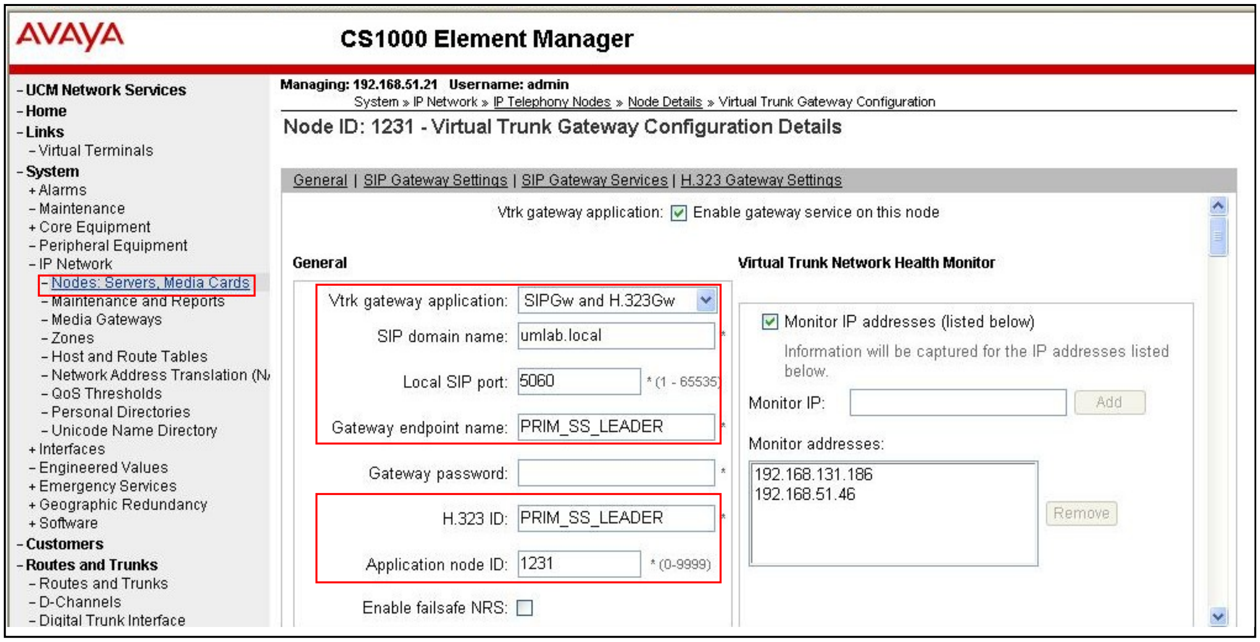


5.3. Virtual Trunk Gateway Configuration

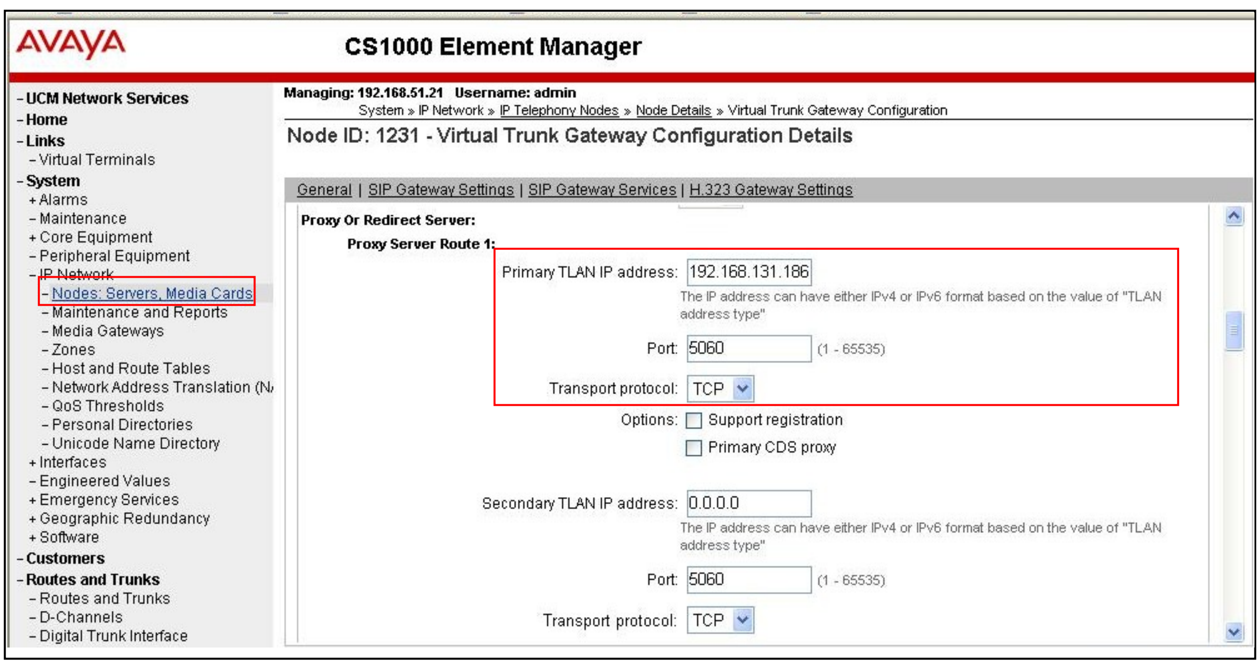
Use Communication Server 1000E Element Manager to configure the system node properties. Navigate to the **System → IP Networks → IP Telephony Nodes → Node Details** and verify the highlighted section is completed with the correct IP addresses and subnet masks. The **Call Server IP address** is normally the same as the server ELAN IP address for a Co-resident installation and the **Node IPv4 address** is a virtual IP address which will be used for all telephony signaling.



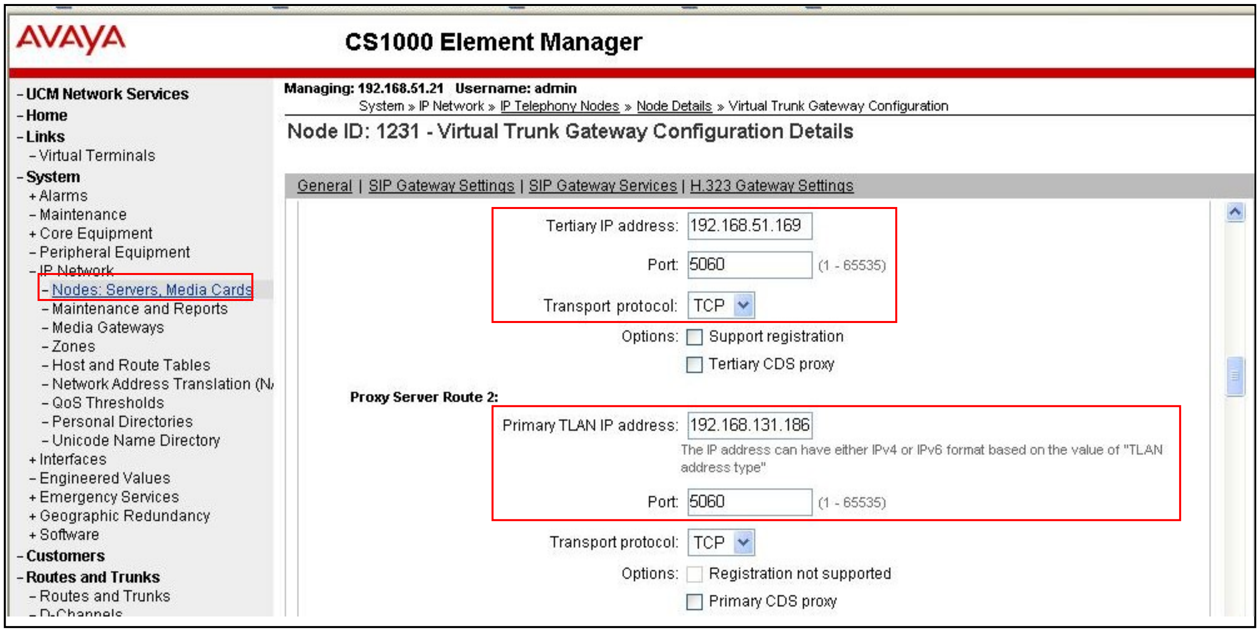
The next screenshot shows the SIP Virtual Trunk Gateway configuration. Navigate to **System → IP Networks → IP Telephony Nodes → Node Details → Virtual Trunk Gateway Configuration** and in the **General** section, fill in the highlighted areas with the relevant settings.



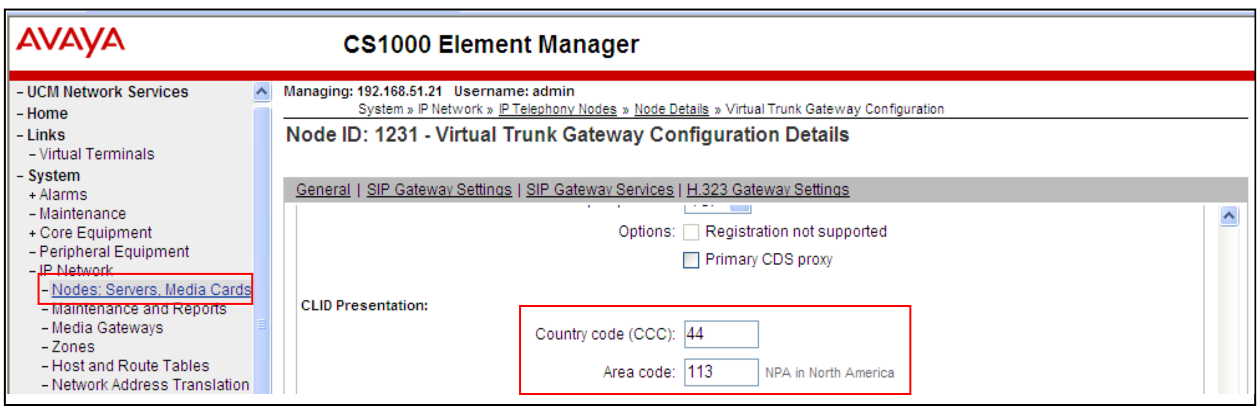
Scroll down to the **Proxy or Redirect Server** area and fill in the values for **Proxy Server Route 1:** , the Primary **TLAN IP address**, **Port** and **Transport protocol** values are required. This is the Session Manager SIP Signaling Interface IP address connection information.



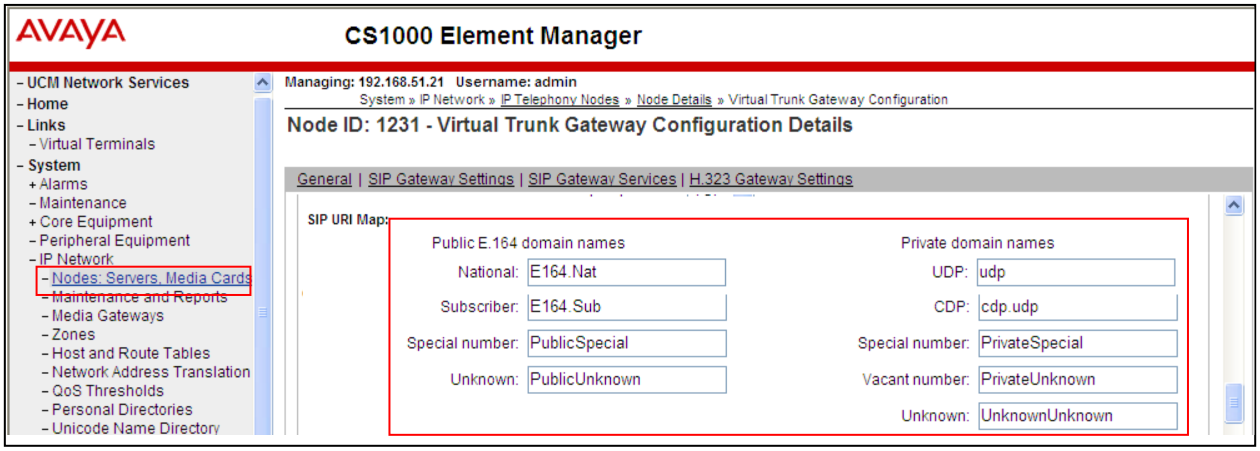
Move down the page and fill in **Tertiary IP address**, **Port** and **Transport protocol** (see the next screenshot). Fill in the **Proxy Server Route 2: Primary TLAN IP address**, **Port** and **Transport protocol**. In this case, the same values as **Proxy Server Route 2** were used.



Scroll down to the CLID Presentation section and fill in the **Country code (CCC)** and **Area code** values.



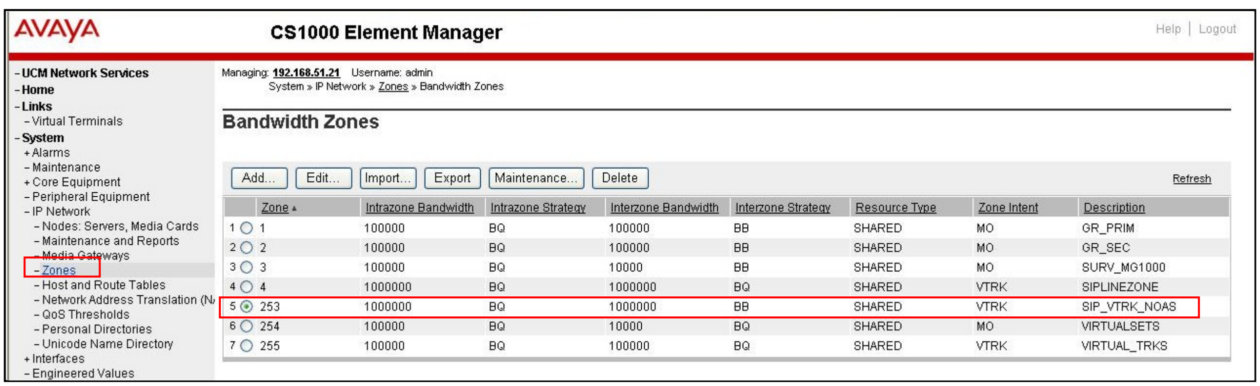
Move to the **SIP URI Maps**: section and fill in the values (see next screenshot).



Scroll down to the bottom of the page and click on the **Save** button (not shown).

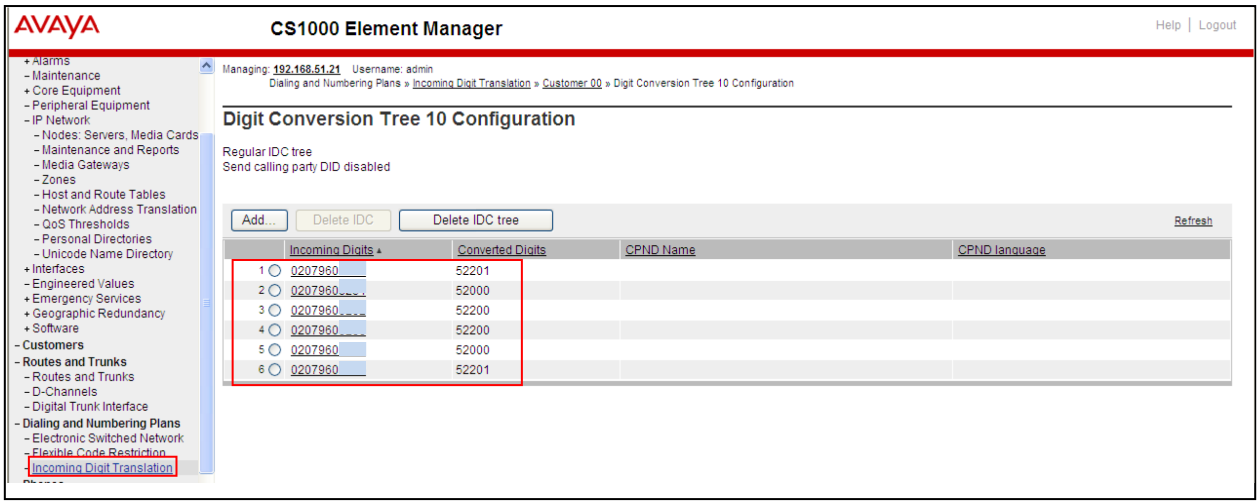
5.4. Configure Bandwidth Zones

Bandwidth Zones are used for alternate call routing between IP stations and for Bandwidth Management. SIP trunks require a unique zone, not shared with other resources and best practice dictates that IP telephones and Media Gateways are all placed in separate zones. Use Element Manager to define bandwidth zones as in the following highlighted example. Use Element Manager and navigate to **System → IP Network → Zones → Bandwidth Zones** and add new zones as required.



5.5. Configure Incoming Digit Conversion Table

A limited number of Direct Dial Inwards (DDI) numbers were available from the service provider; an IDC table was configured to translate incoming PSTN DDI numbers to five digit local telephone extension numbers. Use Element Manager and navigate to **Dialing and Numbering Plans → Incoming Digit Translation**. In the Digit Conversion Tree Configuration screen (not shown), enter the incoming PSTN telephone numbers and the mapped local telephone numbers. The last four digits of the actual PSTN DDI number are obscured for security reasons. The following screenshot shows **Digit Conversion Tree 10 Configuration**, where the incoming PSTN numbers are converted to local extension numbers. These were altered during testing to map to various SIP, Analog, Digital or Unistim telephones depending on the particular test case being executed.



5.6. Configure SIP Trunks

Communication Server 1000E virtual trunks will be used for all inbound and outbound PSTN calls from/to the BT SIP Trunk Service. Five separate steps are required to configure Communication Server 1000E virtual trunks:

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

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

```
Overlay 17
ADAN     DCH 50
  CTYP DCIP
  DES  VIR_TRK
  USR  ISLD
  ISLM 4000
  SSRC 1800
  OTBF 32
  NASA YES
  IFC  SL1
  CNEG 1
  RLS  ID  5
  RCAP ND2
  MBGA NO
  H323
    OVLR NO
    OVLS NO
```

Next, configure the SIP trunk Route Data Block (RDB) using the Communication Server 1000E system terminal and overlay 16. Load **Overlay 16**, enter **RDB** at the prompt, press return and commence configuration. The value for **DCH** is the same as previously entered in overlay 17. The value for **NODE** should match the node value in **Section 5.3**. The value for **ZONE** should match that used in **Section 5.4** for **SIP_VTRK_NOAS**. The remaining highlighted values are important for correct SIP trunk operation.

```
Overlay 16
TYPE: rdb
CUST 00
ROUT 100
TYPE RDB
CUST 00
ROUT 100
DES  VIR_TRK
TKTP TIE
NPID_TBL_NUM   0
ESN  NO
RPA  NO
CNVT NO
SAT  NO
RCLS EXT
VTRK YES
ZONE 00253
PCID SIP
CRID NO
NODE 1231
DTRK NO
ISDN YES
    MODE ISLD
    DCH  50
    IFC  SL1
    PNI  00001
    NCNA YES
    NCRD YES
    TRO  NO
    FALT NO
    CTYP UKWN
    INAC NO
    ISAR NO
    DAPC NO
MBXR NO
MBXOT NPA
MBXT 0
PTYP ATT
CNDP UKWN
AUTO NO
DNIS NO
DCDR NO
ICOG IAO
SRCH LIN
TRMB YES
STEP
```

```
ACOD 1600
TCPP NO
PII NO
AUXP NO
TARG
CLEN 1
BILN NO
OABS
INST
IDC  YES
DCNO 10
NDNO 10 *
DEXT NO
DNAM NO
SIGO STD
STYP SDAT
MFC  NO
ICIS YES
OGIS YES
TIMR ICF  1920
     OGF  1920
     EOD  13952
     LCT  256
     DSI  34944
     NRD  10112
     DDL  70
     ODT  4096
     RGV  640
     GTO  896
     GTI  896
     SFB  3
     PRPS  800
     NBS  2048
     NBL  4096
     IENB  5
     TFD  0
     VSS  0
     VGD  6
     EESD  1024
SST  5 0
DTD  NO
SCDT NO
2 DT NO
NEDC ORG
FEDC ORG
```

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

Next, configure virtual trunk members using the Communication Server 1000E system terminal and overlay 14. Configure sufficient trunk members to carry both incoming and outgoing PSTN calls. The following example shows a single SIP trunk member configuration. Load **Overlay 14** at the system terminal and type **new X**, where X is the required number of trunks. Continue entering data until the overlay exits. The **RTMB** value is a combination of the **ROUT** value entered in the previous step and the first trunk member (usually 1). The remaining highlighted values are important for correct SIP trunk operation.

```
Overlay 14
TN   160 0 0 0
DATE
PAGE
DES  VIR_TRK
TN   160 0 00 00  VIRTUAL
TYPE IPTI
CDEN 8D
CUST 0
XTRK VTRK
ZONE 00253
TIMP 600
BIMP 600
AUTO_BIMP NO
NMUS NO
TRK  ANLG
NCOS 0
RTMB 100 1
CHID 1
TGAR 1
STRI/STRO WNK WNK
SUPN YES
AST  NO
IAPG 0
CLS  TLD DTN CND ECD WTA LPR APN THFD XREP SPCD MSBT
     P10 NTC
TKID
AACR NO
```

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

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

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

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

5.7. Configure Analog, Digital and IP Telephones

A variety of telephone types were used during the testing, the following is the configuration for the Avaya 1140e Unistim IP telephone. Load **Overlay 20** at the system terminal and enter the following values. A unique five digit number is entered for the **KEY 00** and **KEY 01** value. The value for **CFG_ZONE** is the value used in **Section 5.4** for **VIRTUALSETS**.

```
Overlay 20 IP Telephone configuration
DES  1140
TN   096 0 01 16  VIRTUAL
TYPE 1140
CDEN 8D
CTYP XDLC
CUST 0
NUID
NHTN
CFG_ZONE 00254
CUR_ZONE 00254
ERL  0
ECL  0
FDN  0
TGAR 0
LDN  NO
NCOS 0
SGRP 0
RNPG 1
SCI  0
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 52000 0     MARP
        CPND
          CPND_LANG ROMAN
            NAME IP1140
            XPLN 10
            DISPLAY_FMT FIRST,LAST
     01 MCR 52000 0
        CPND
          CPND_LANG ROMAN
            NAME IP1140
            XPLN 10
            DISPLAY_FMT FIRST,LAST
     02
     03 BSY
     04 DSP
     05
     06
     07
     08
     09
     10
     11
     12
     13
     14
     15
     16
     17 TRN
     18 AO6
     19 CFW 16
     20 RGA
     21 PRK
     22 RNP
     23
     24 PRS
     25 CHG
     26 CPN
```

Digital telephones are configured using the **Overlay 20**; the following is a sample 3904 digital set configuration. Again, a unique number is entered for the **KEY 00** and **KEY 01** value.

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

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

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

MLNG ENG
DNDR 0
KEY  00 MCR 52001 0     MARP
        CPND
          CPND_LANG ROMAN
            NAME Digital Set
            XPLN 10
            DISPLAY_FMT FIRST,LAST
     01 MCR 52001 0
        CPND
          CPND_LANG ROMAN
            NAME Digital Set
            XPLN 10
            DISPLAY_FMT FIRST,LAST
     02 DSP
     03 MSB
     04
     05
     06
     07
     08
     09
     10
     11
     12
     13
     14
     15
     16
     17 TRN
     18 AO6
     19 CFW 16
     20 RGA
     21 PRK
     22 RNP
     23
     24 PRS
     25 CHG
     26 CPN
     27 CLT
     28 RLT
     29
     30
     31
```

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

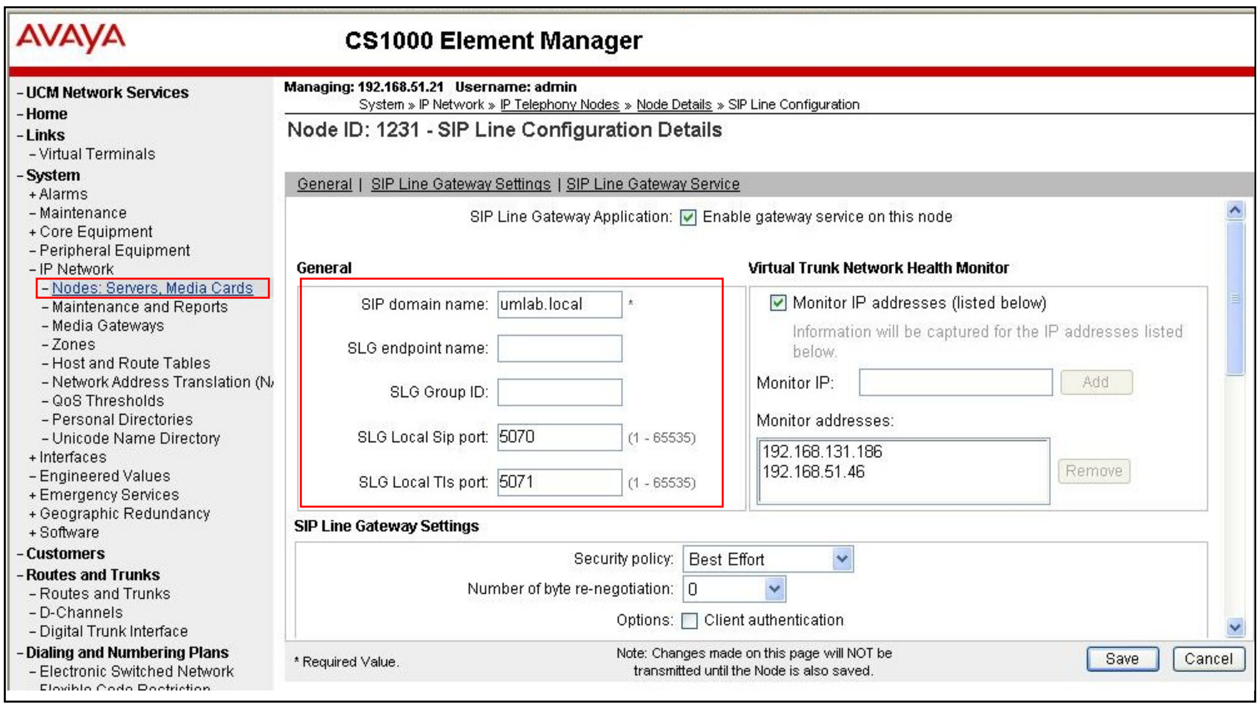
```
Overlay 20 – Analog Telephone Configuration
DES  500
TN   100 0 00 03
TYPE 500
CDEN 4D
CUST 0
MRT

ERL 00000
WRLS NO
DN   52002
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

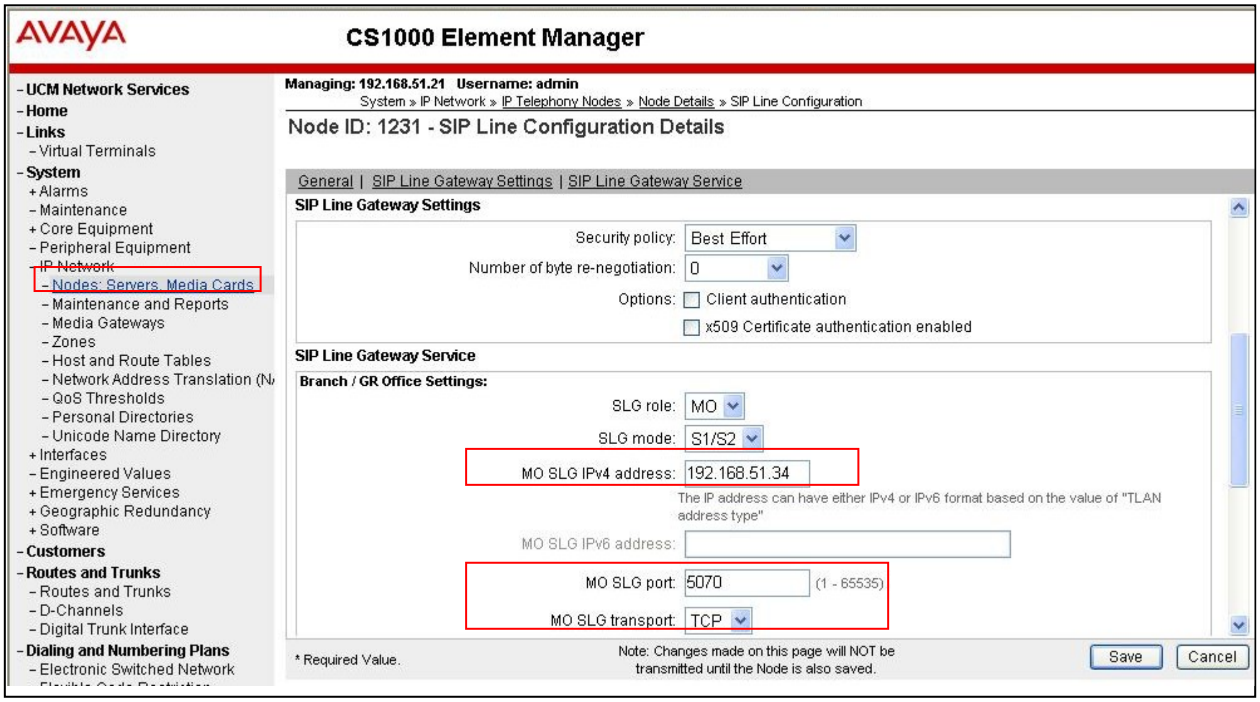
SIP terminal operation requires the Communication Server node to be configured as a SIP Line Gateway (SLG) before SIP telephones can be configured. Prior to configuring the SIP Line node properties, the SIP Line service must be enabled in the customer data block. Use the Communication Server 1000E system terminal and overlay 15 to activate SIP Line services, as in the following example where **SIPL_ON** is set to **YES**. The numerical value entered for the **UAPR** setting will be pre-appended to all SIP Line phones, and is used internally to track SIP phones.

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

Use Element Manager and navigate to **System → IP Network → IP Telephony Nodes → Node Details → SIP Line Configuration**. In the **General** section, configure the **SIP domain name**, **SLG Local SIP port** and **SLG Local Tls port**. The **SIP domain Name** must match that configured in **Section 6.5.1**.



Scroll down to the **Branch / GR Office Settings** area. The IP address for **MO SLG IPv4 address** is the system **NODE Ipv4 address**, previously configured in **Section 5.3**. The **MO SLG port** and **MO SLG transport** values will be 5070 and TCP. Click on the **Save** button when finished.



5.9. Configure SIP Line Telephones

When SIP Line service configuration is completed, use the Communication Server 1000E system terminal and overlay 20 to add a Universal Extension (UEXT). See the following example of a SIP Line extension. The value for **UXTY** must be **SIPL**. This example is for an Avaya SIP telephone, so the value for **SIPN** is 1. The **SIPU** value is the username, **SCPW** is the logon password and these values are required to register the SIP telephone to the SLG. The value for **CFG_ZONE** is the value set for **SIPLINEZONE** in **Section 5.4**. A unique telephone number is entered for value **KEY 00**. The value for **KEY 01** is comprised of the **UAPR** value (set to 78 previously in **Section 5.8**) and the telephone number used in **KEY 00**.

```
Overlay 20 – SIP Telephone Configuration
DES  SIPD
TN   096 0 01 15  VIRTUAL
TYPE UEXT
CDEN 8D
CTYP XDLC
CUST 0
UXTY SIPL
MCCL YES
SIPN 1
SIP3 0
FMCL 0
TLSV 0
SIPU 52003
NDID 5
SUPR NO
SUBR DFLT MWI RGA CWI MSB
UXID
NUID
NHTN
CFG_ZONE 00004
CUR_ZONE 00004
ERL  0
ECL  0
VSIT NO
FDN
TGAR 0
LDN  NO
NCOS 0
SGRP 0
RNPG 0
SCI  0
SSU
XLST
SCPW 52003
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 52003 0     MARP
        CPND
          CPND_LANG ROMAN
            NAME Sigma 1140
            XPLN 11
            DISPLAY_FMT FIRST,LAST*
     01 HOT U 7852003 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
```

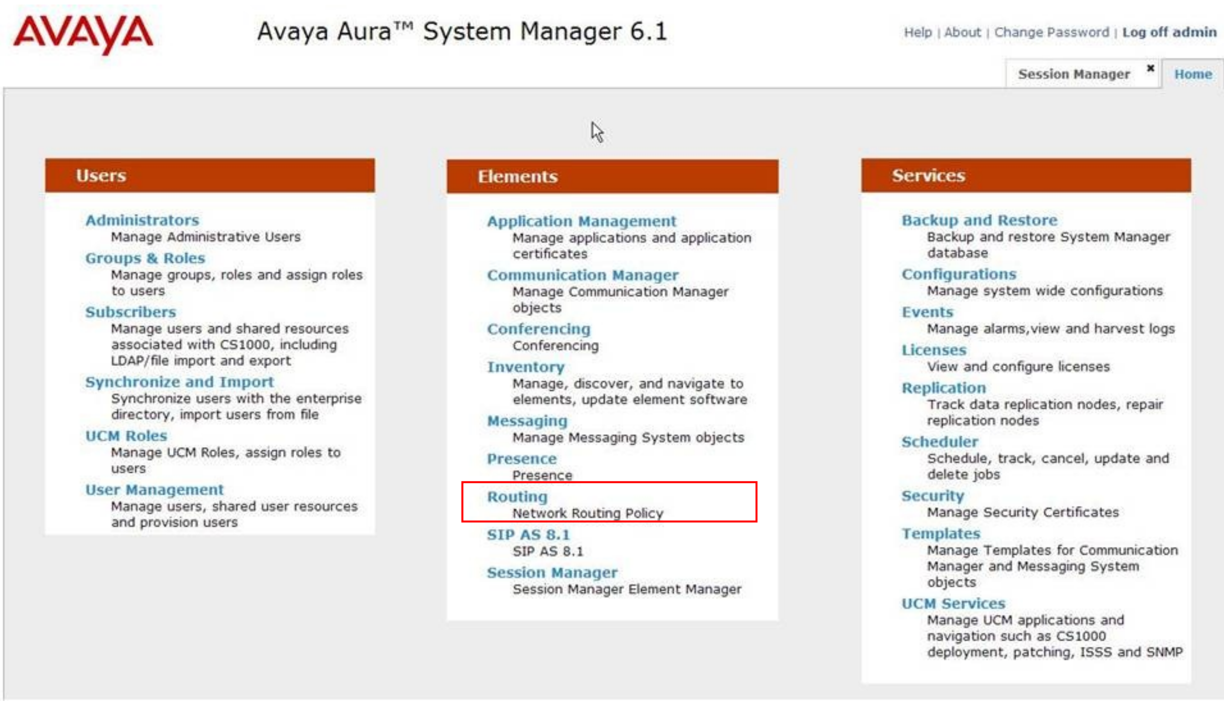
6. Configuring Avaya Aura® Session Manager

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 System Manager
- Administer SIP domain
- Administer Locations
- Administer Adaptations
- Administer SIP Entities
- Administer Entity Links
- Administer Routing Policies
- Administer Dial Patterns
- Administer Avaya Communication Server 1000E as Managed Element

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** screen will be presented with menu options shown below.

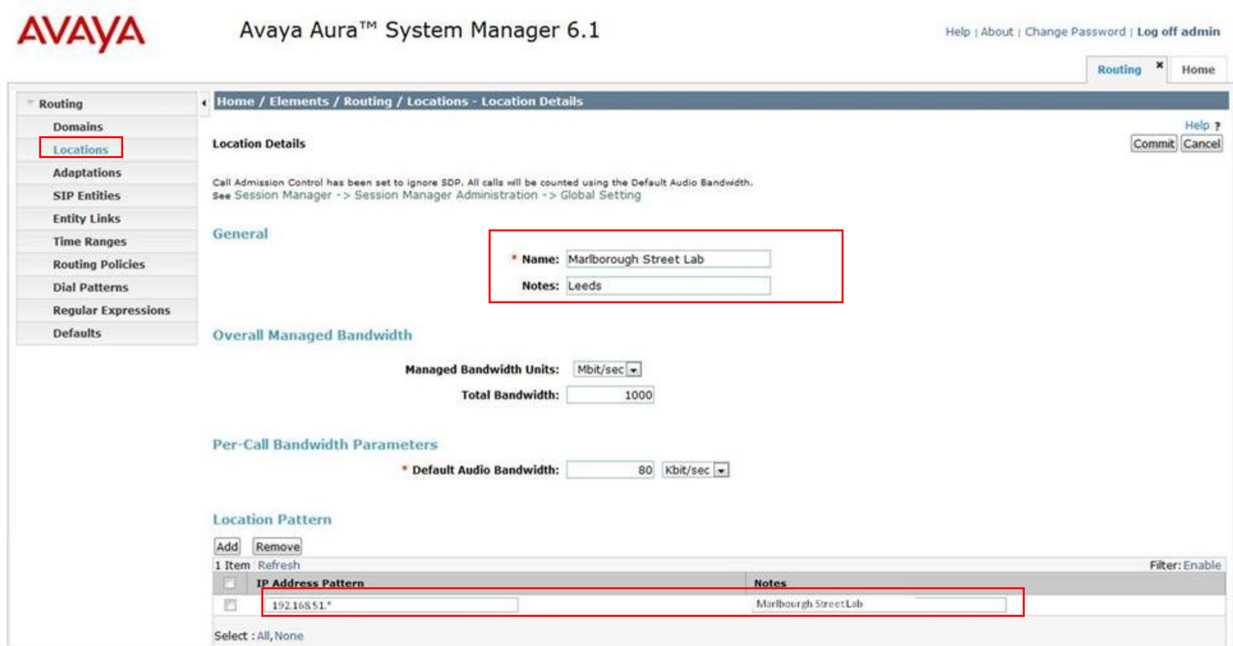


6.2. Administer SIP Domain

To add the SIP domain that will be used with Session Manager, select **Routing** from the **Elements** menu and in the resulting screen select **Domains** under **Routing** from left-hand menu. Click the **New** button (not shown) to create a new SIP domain entry. In the **Name** field enter the domain name (e.g., **umlab.local**) and optionally a description for the domain 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 the enterprise SIP entities. Under **Routing** 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, The character '*' is used to specify any number of allowed characters at the end of the string. Below is the location configuration used for the simulated Enterprise site.

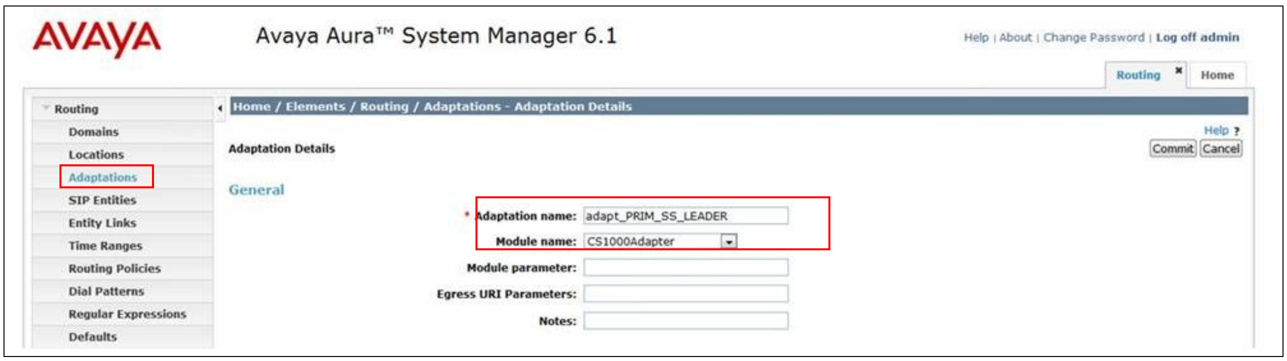


6.4. Administer Adaptations

To ensure that the E.164 numbering format is used between the enterprise and BT SIP Trunk Service, an adaptation module is used to perform some digit manipulation. This adaptation is applied to the Communication Server 1000E SIP entity. To add an adaptation, under **Routing** select **Adaptations** from the left-hand menu and then click on the **New** button (not shown).

Under **Adaption Details → General**:

- In the **Adaptation name** field enter an informative name.
- In the **Module name** field click on the down arrow and then select the <**click to add module**> entry from the drop down list and type **CS1000Adapter** in the resulting New Module Name field



Scroll down the page and under **Digit Conversion for Incoming Calls to SM**, click the **Add** button and specify the digit manipulation to be performed as follows:

- Enter the leading digits that will be matched in the Matching Pattern field.
- In the **Min** and **Max** fields set the minimum and maximum digits allowed in the digit string to be matched.
- In the **Delete Digits** field enter the number of leading digits to be removed.
- In the **Insert Digits** field specify the digits to be prefixed to the digit string.
- In the **Address to modify** field specify the digits to manipulate by the adaptation. In this configuration the dialed number is the target so destination has been selected.

This will ensure any destination numbers received from Communication Server 1000E are converted to the E.164 numbering format before being processed by Session Manager. The following screenshot shows the settings used.

Digit Conversion for Incoming Calls to SM

Add Remove

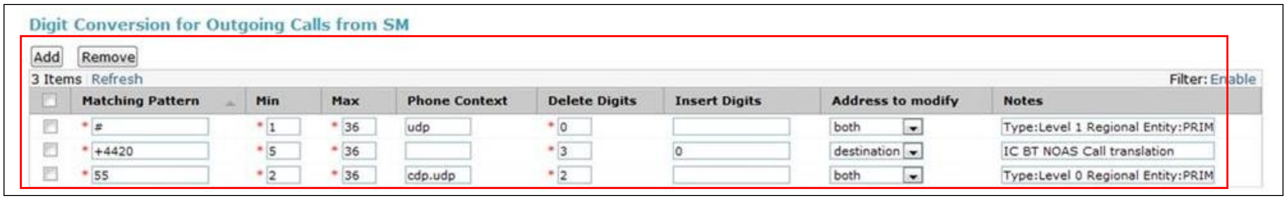
12 Items Refresh Filter: Enable

Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
003	3	36	PrivateSpecia	2	+	destination	Ireland IDD Code
0113	4	36	PrivateSpecia	1	+44	destination	Leeds Area STD Code
0121	4	36	PrivateSpecia	1	+44	destination	Birmingham Area STD Code
0131	4	36	PrivateSpecia	1	+44	destination	Edinburgh Area STD Code
01903	5	36	PrivateSpecia	1	+44	destination	Worthing Area STD Code
0191	4	36	PrivateSpecia	1	+44	destination	Tyneside Area STD Code
020	3	36	PrivateSpecia	1	+44	destination	London Area STD Code
05	2	36		0	+	both	Type:E164 Local, special rule
07	2	36	PrivateSpecia	1	+44	destination	UK Mobile Services
x	1	36	cdp.udp	0	55	both	Type:Level 0 Regional, special rule
x	1	36	PrivateSpecia	0	56	both	Type:Special, general rule
x	1	36	+1	0	+1	both	Type:E164 National, special rule

Under **Digit Conversion for Outgoing Calls from Session Manager** click the **Add** button and specify the digit manipulation to be performed as follows:

- Enter the leading digits that will be matched in the **Matching Pattern** field.
- In the **Min** and **Max** fields set the minimum and maximum digits allowed in the digit string to be matched.
- In the **Delete Digits** field enter the number of leading digits to be removed.
- In the **Insert Digits** field specify the digits to be prefixed to the digit string.
- In the **Address to modify** field specify the digits to manipulate by the adaptation. In this configuration the dialed number is the target so destination has been selected.

This will ensure any destination numbers will have the + symbol and international dialing code removed before being presented to Communication Server 1000E. See the following screenshot for the settings used.



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 (see the following screenshot) and then click on the **New** button (not shown). The following will need to be entered for each SIP Entity.

Under **SIP Entity Details → General**:

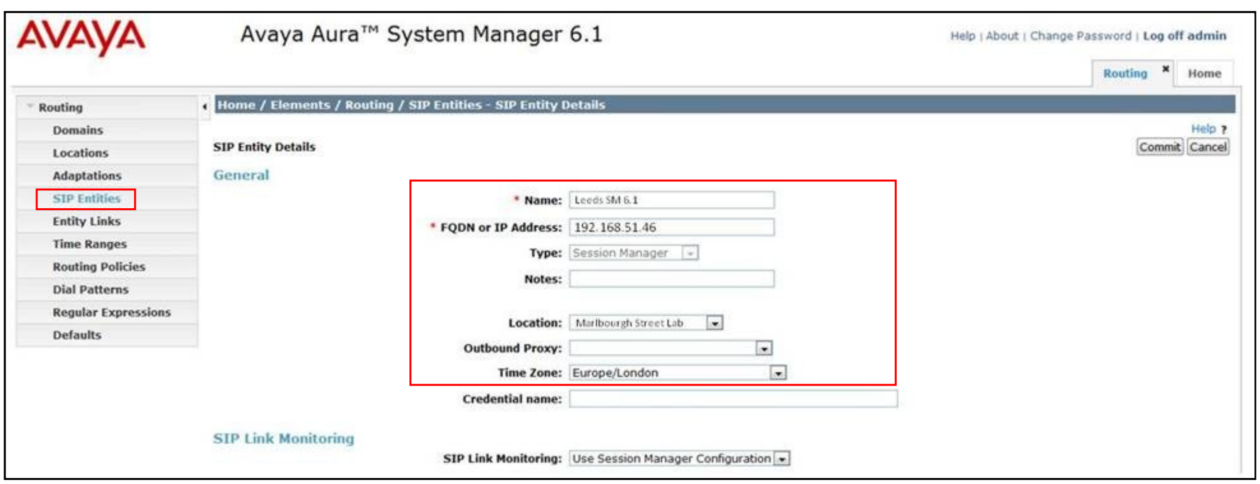
- In the **Name** field enter an informative name.
- In the **FQDN or IP Address** field enter the IP address of Session Manager or the signaling interface on the connecting system.
- In the **Type** field use **Session Manager** for a Session Manager SIP entity, **Other** for a Communication Server 1000E 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 enterprise site configuration there are three SIP Entities configured.

- Avaya Aura® Session Manager SIP Entity
- Communication Server 1000E SIP Entity
- Avaya Aura® Session Border Controller SIP Entity

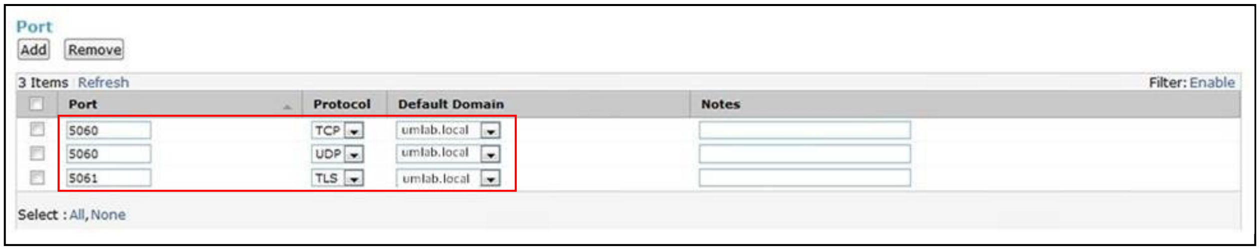
6.5.1. Avaya Aura® Session Manager SIP Entity

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



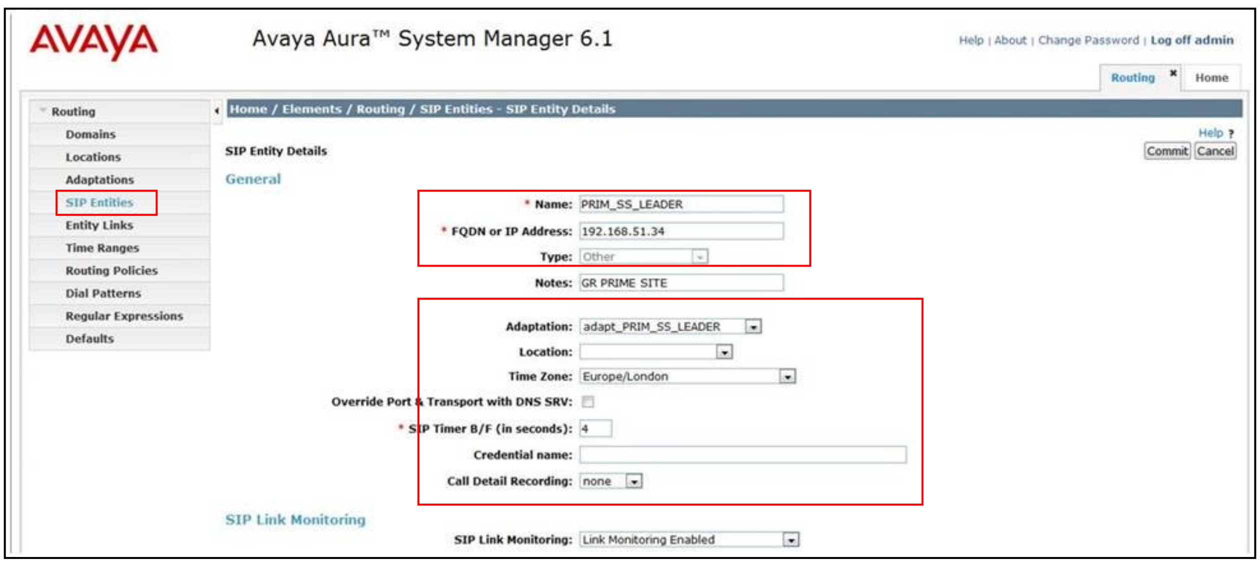
The Session Manager must be configured with the port numbers of the protocols that will be used by the other SIP entities. To configure these scroll to the bottom of the page and under Port, click Add, then edit the fields in the resulting new row.

- 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 **umlab.local** as the default domain.



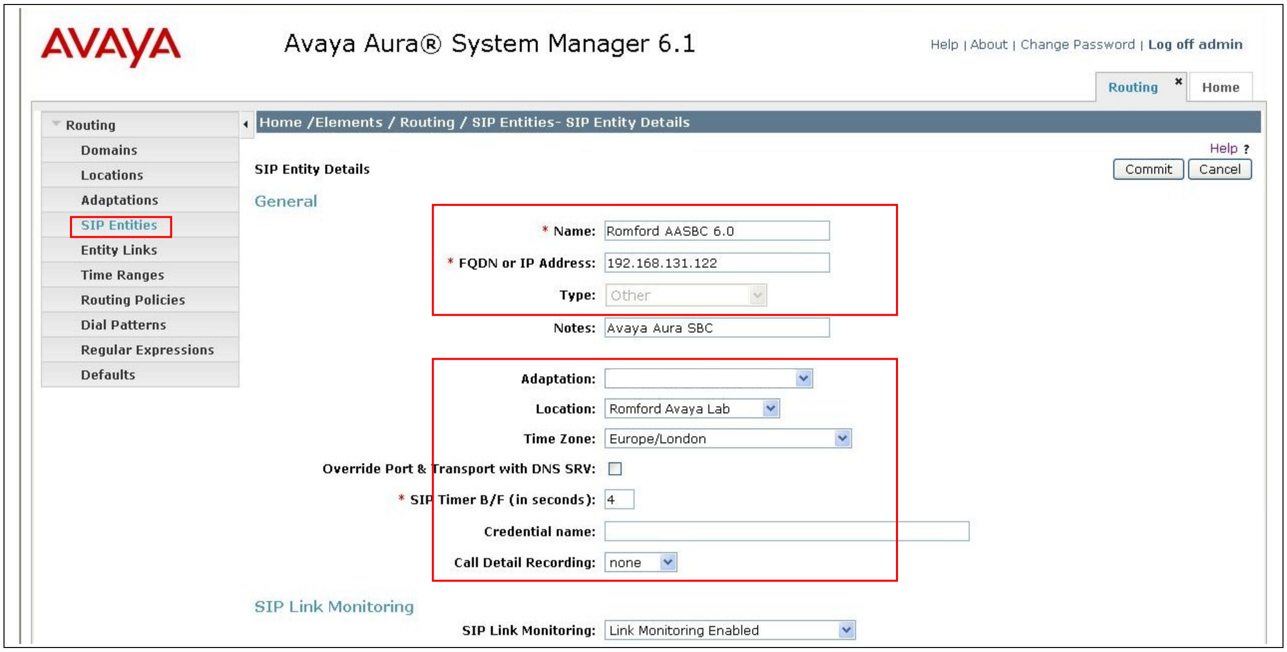
6.5.2. Avaya Communication Server 1000E SIP Entity

The following screenshot shows the SIP entity for Communication Server 1000E. The **Type** is set to **Other**. The **FQDN or IP Address** field is set to the Communication Server 1000E node IP address. For the **Adaptation** field, select the adaptation module previously defined for dial plan digit manipulation in **section 6.4**.



6.5.3. Avaya Aura® Session Border Controller SIP Entity

The following screen shows the SIP Entity for the AASBC. The **FQDN or IP Address** field is set to the IP address of the AASBC private network interface.

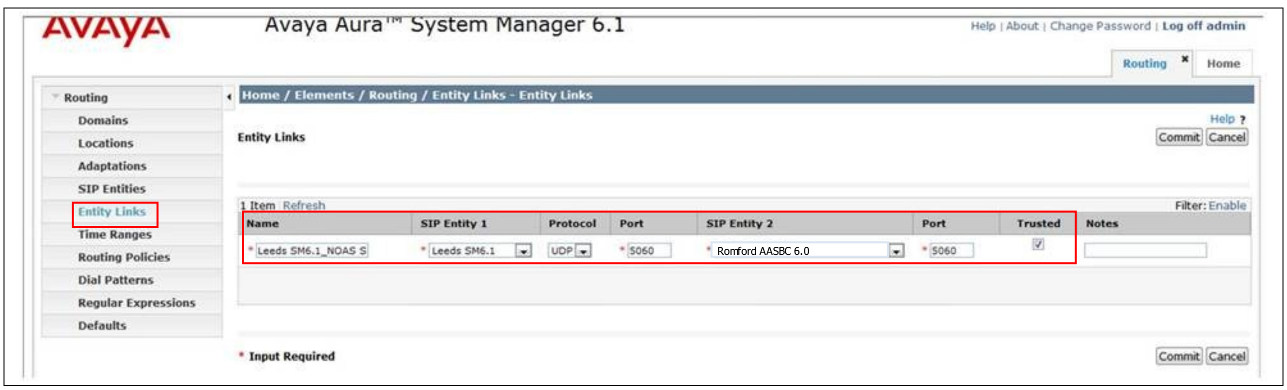


6.6. Administer Entity Links

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 **Protocol** field enter the transport protocol to be used to send SIP requests.
- 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 from which the other system expects to receive SIP requests.
- Select the **Trusted** tick box to make the other system trusted.

Click **Commit** to save changes. The following screen shows the Entity Link used in the compliance test configuration between Session Manager and AASBC.

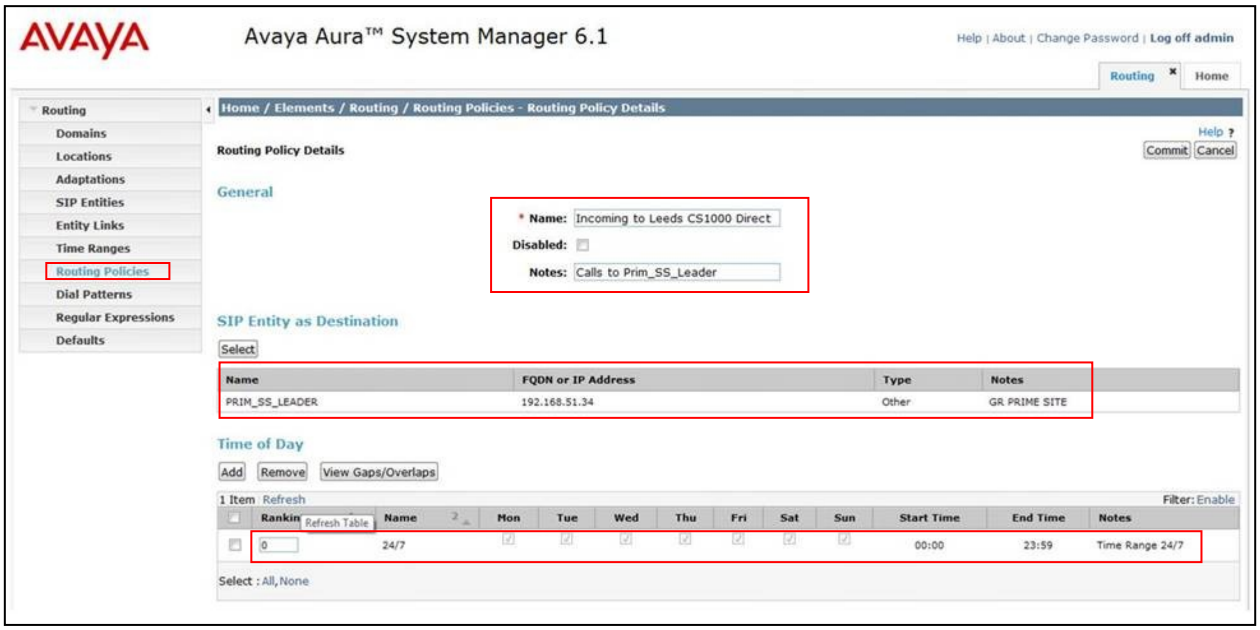


6.7. Administer Routing Policies

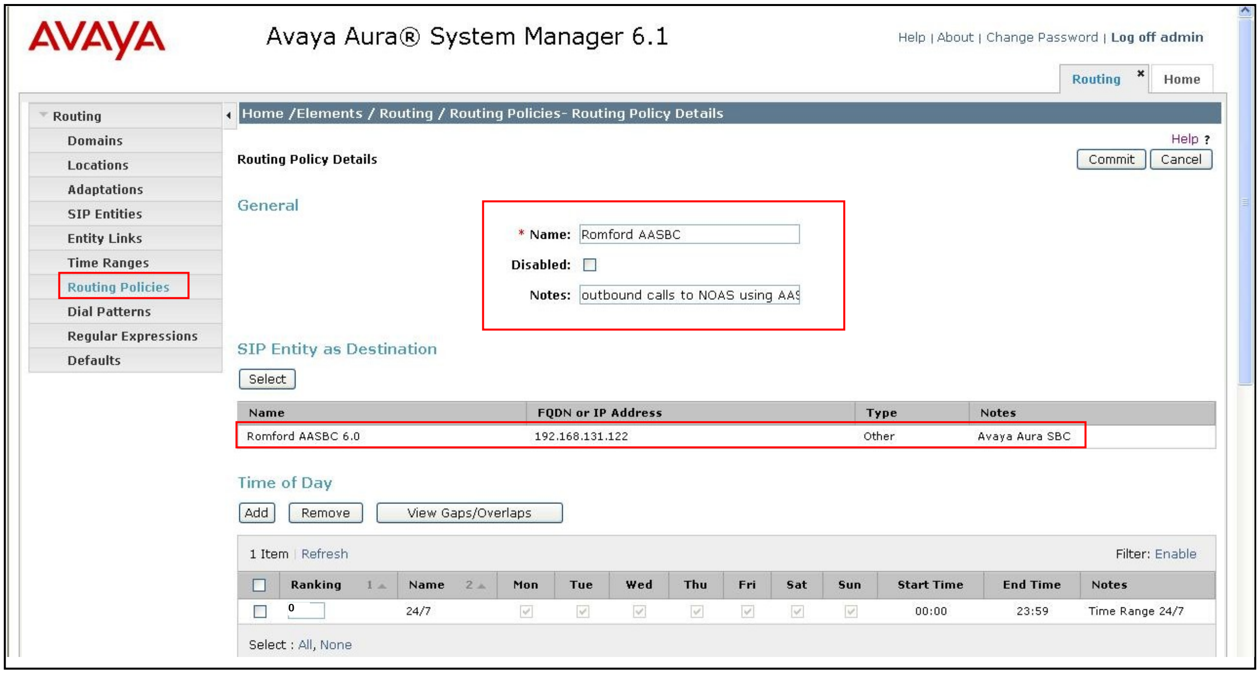
Routing policies must be created to direct how calls will be routed to a system. To add a routing policy, select **Routing Policies** on the left panel menu (see next screenshot) and then click on the **New** button (not shown).

- 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 **SIP Entity as Destination** value is set to **PRIM_SS_LEADER**, as entered in **Section 6.5.2**. The **Time of Day** is set to 24 hour by 7 day operation.



The following screen shows the routing policy for the AASBC. The **SIP Entity as Destination** value is set to **Romford AASBC 6.0**, as entered in **Section 6.5.3**. The **Time of Day** is set to 24 hour by 7 day operation.



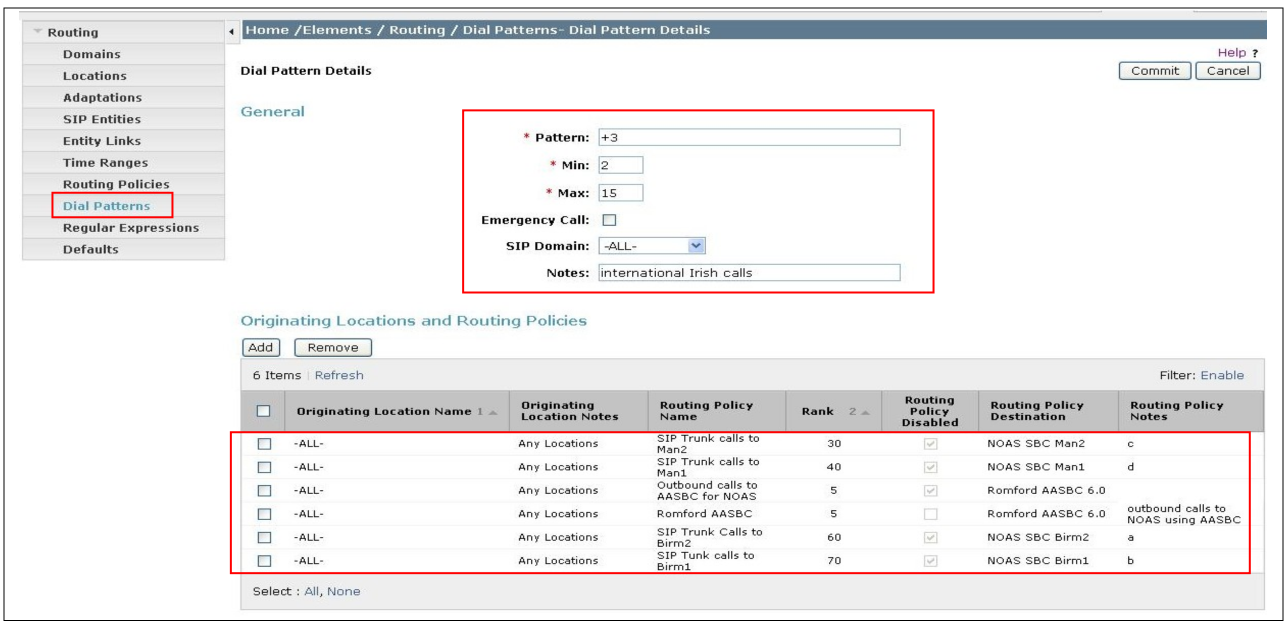
6.8. Administer Dial Patterns

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 (see below) and then click on the **New** button (not shown).

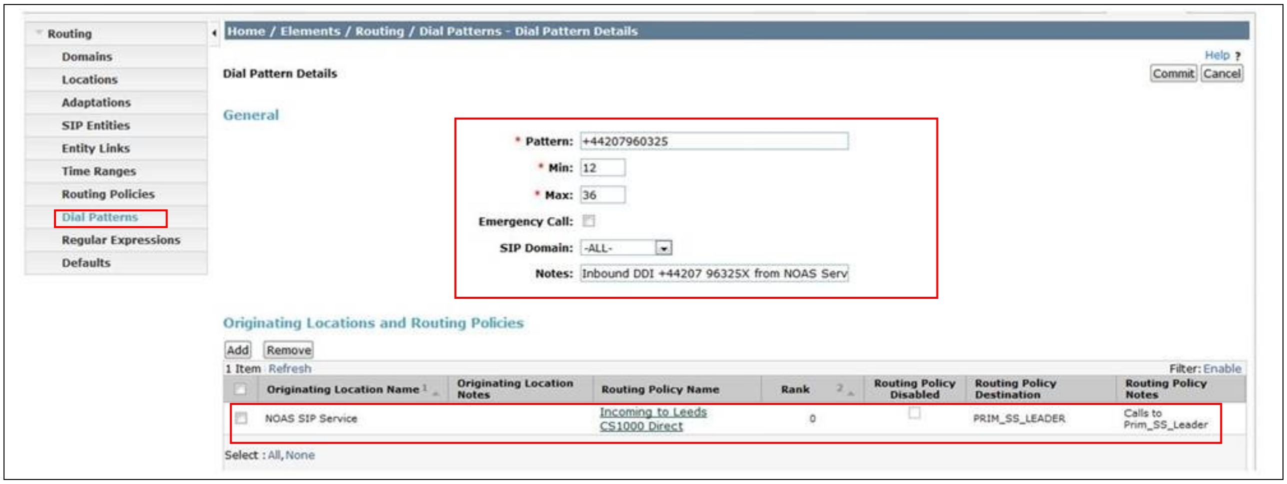
Under **Dial Pattern Details → General**:

- In the **Pattern** field enter a dialed number or prefix to be matched
- In the **Min** field enter the minimum length of the dialed number
- In the **Max** field enter the maximum length of the dialed number
- In the **SIP Domain** field select the domain configured in **Section 6.2**

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 6.7**. Click **Select** button to save. The following screen shows an example dial pattern configured for BT SIP Trunk Service. Note the ranking for each routing policy as applied in **Section 6.7**. The routing policy with the lowest rank will be selected first, if this route is unavailable or does not respond then the routing policy with the next lowest rank will be selected and so on. This allows for redundant routing within Session Manager.



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



7. Configure Avaya Aura® Session Border Controller

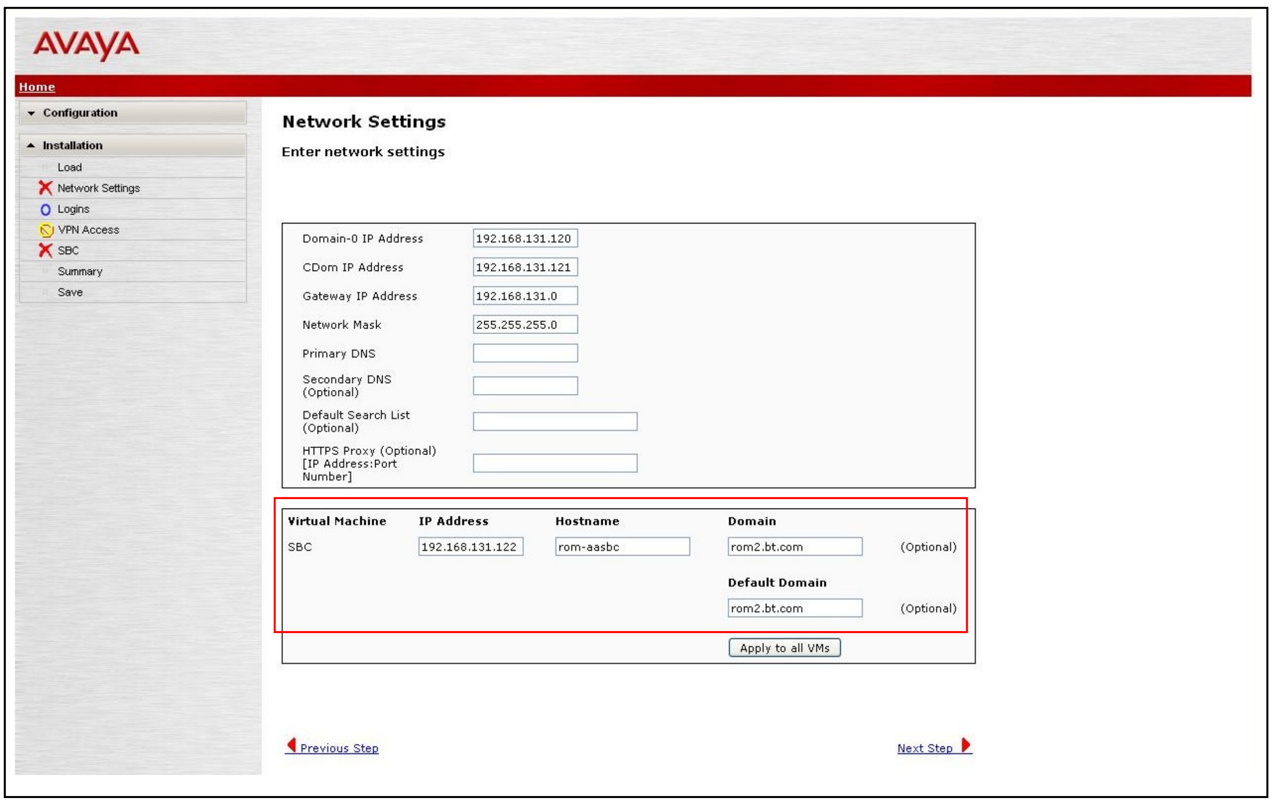
This section describes the configuration of the AASBC. This configuration is done in two parts. The first part is done during the AASBC installation via the installation wizard. These Application Notes will not cover the AASBC installation in its entirety but will include the use of the installation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

7.1. Installation Wizard

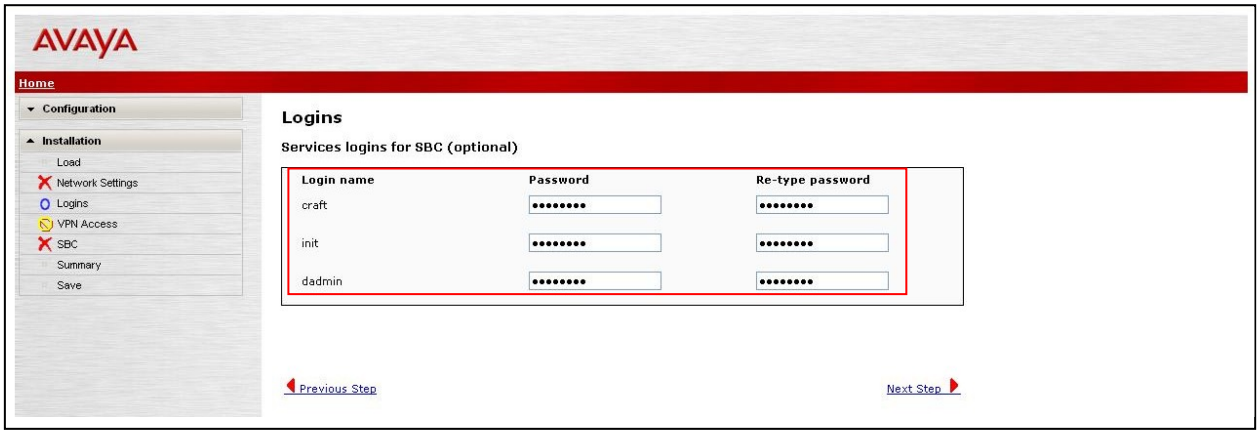
During the installation of the AASBC template, the installation wizard will prompt the installer for information that will be used to create the initial configuration of the AASBC. The first screen of the installation wizard is the Network Settings screen. Fill in the fields as described below and shown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

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

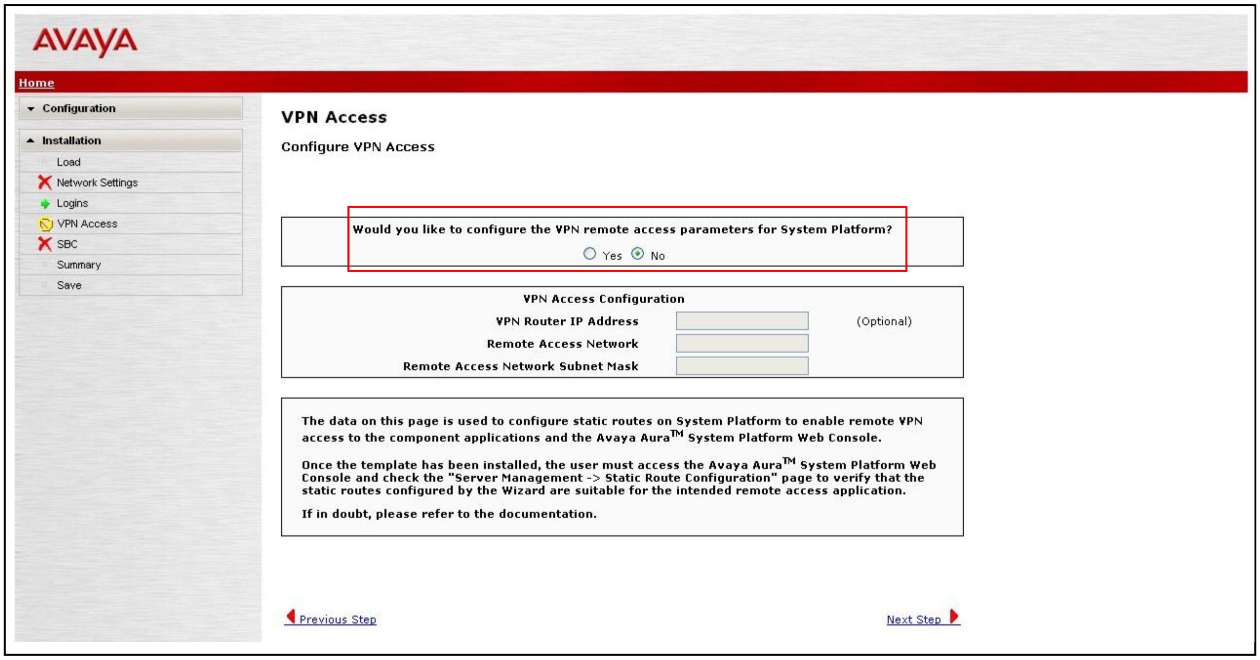
Click **Next Step** to continue.



From the Logins screen specify passwords for the services logins to the AASBC. Click **Next Step** to continue.



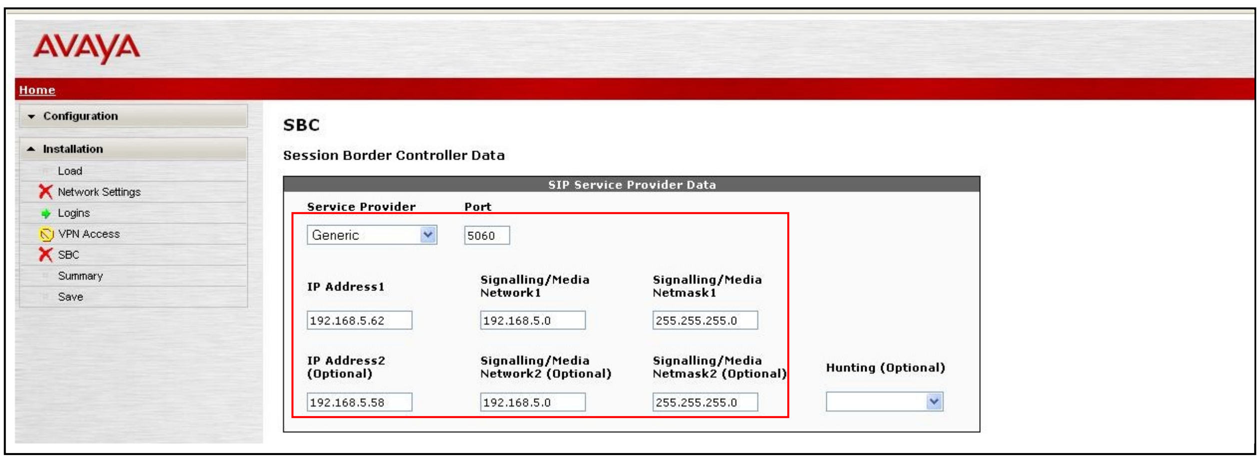
VPN remote access to the AASBC was not part of the compliance test. Thus, on the VPN Access screen, select **No** to the question, **Would you like to configure the VPN remote access parameters for System Platform?,** click **Next Step** to continue.



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

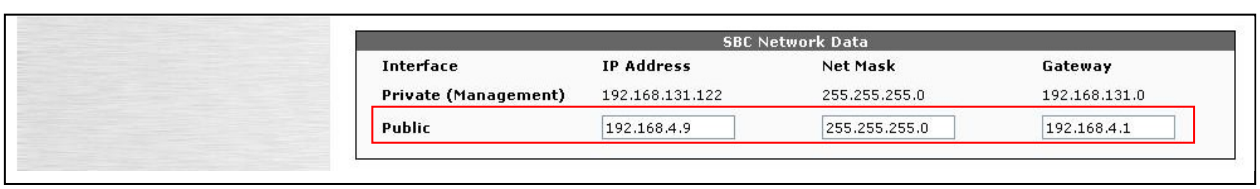
- In the **Service Provider** select the name of the service provider to which the AASBC will connect. This will allow the wizard to select a configuration file customized for this service provider. At the time of the compliance test, a customized configuration file did not exist for BT. Therefore, **Generic** was chosen
- In the **Port** field enter the port number that BT uses to listen for SIP traffic
- In the **IP Address1** and **IP Address2** fields enter the first two BT provided IP addresses for the SIP Trunk Service. The remaining IP addresses will be added after the AASBC template is installed **(Section 7.3)**
- In the **Signaling/Media Network1** field enter the BT provided subnet where media traffic will originate. An additional subnet can be provided for **Signaling/Media Network2**
- In the **Media Netmask** field enter the netmask corresponding to the Media Network

Scroll down to continue.



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

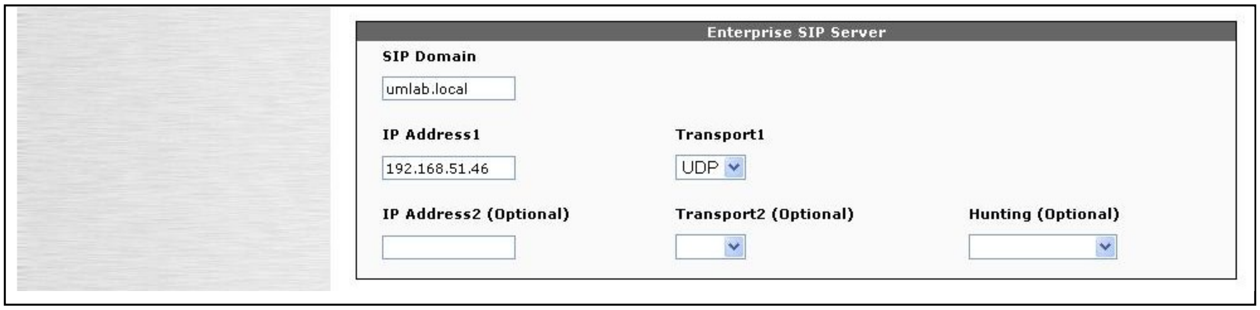
- In the **Public IP Address** field enter the IP address of the public side of the AASBC
- In the **Public Net Mask** field enter the netmask associated with the public network to which the AASBC connects
- In the **Public Gateway** field enter the default gateway of the public network



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

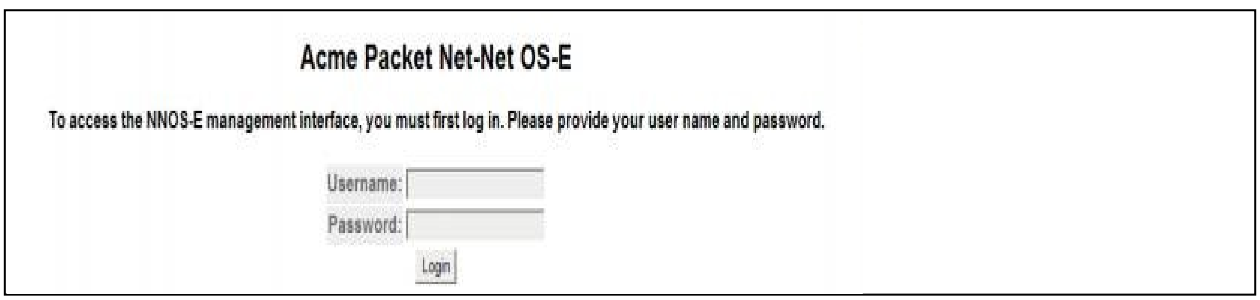
- In the **IP Address1** field enter the IP address of the Enterprise SIP Server to which the AASBC will connect. In the case of the compliance test, this is the IP address of the Session Manager SIP signaling interface
- In the **Transport1** field select the transport protocol to be used for SIP traffic between the AASBC and Session Manager
- In the **SIP Domain** field enter the enterprise SIP domain

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



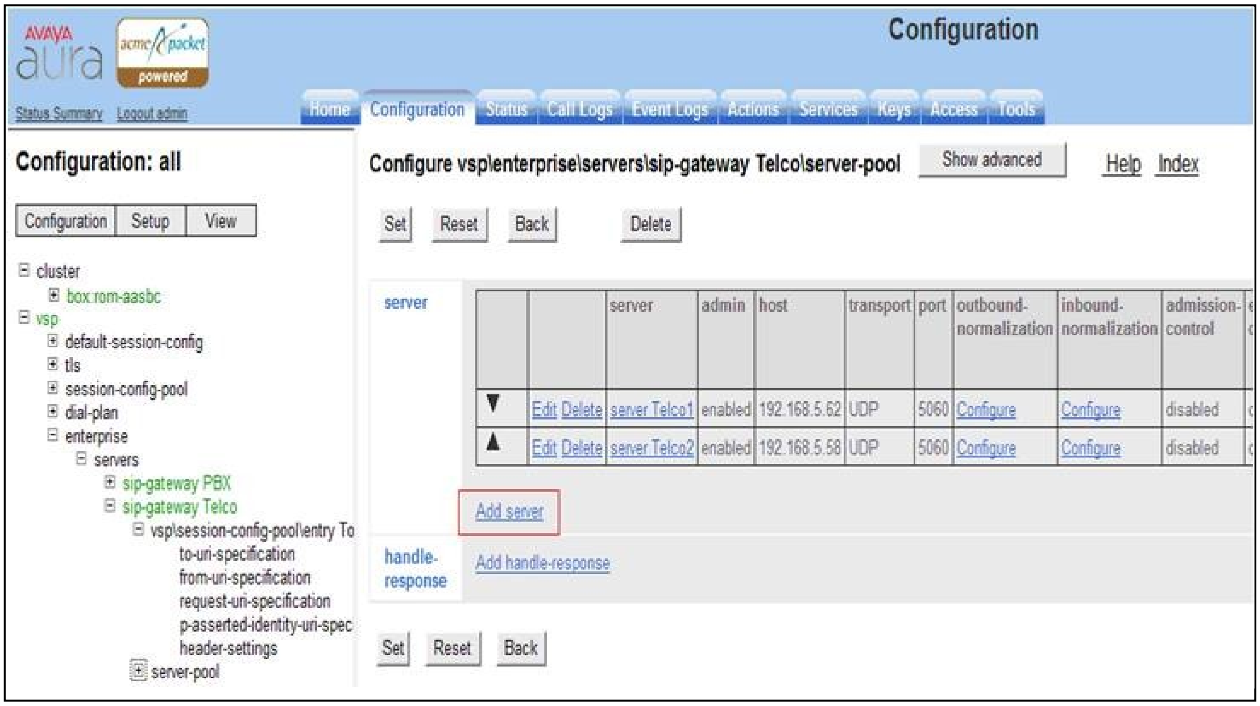
7.2. Access Avaya Aura® Session Border Controller

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

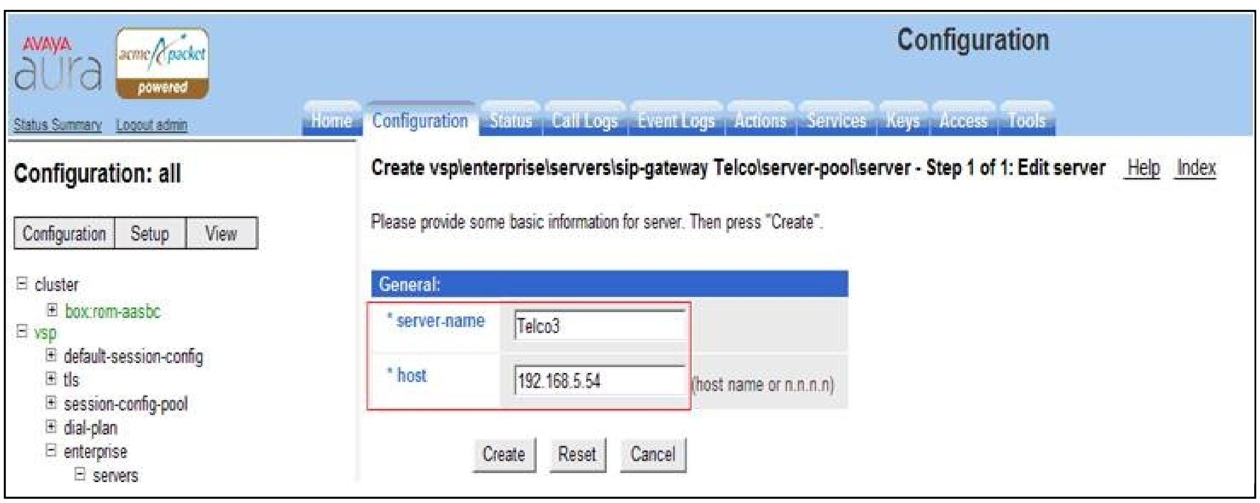


7.3. Add Additional Service Provider IP Addresses

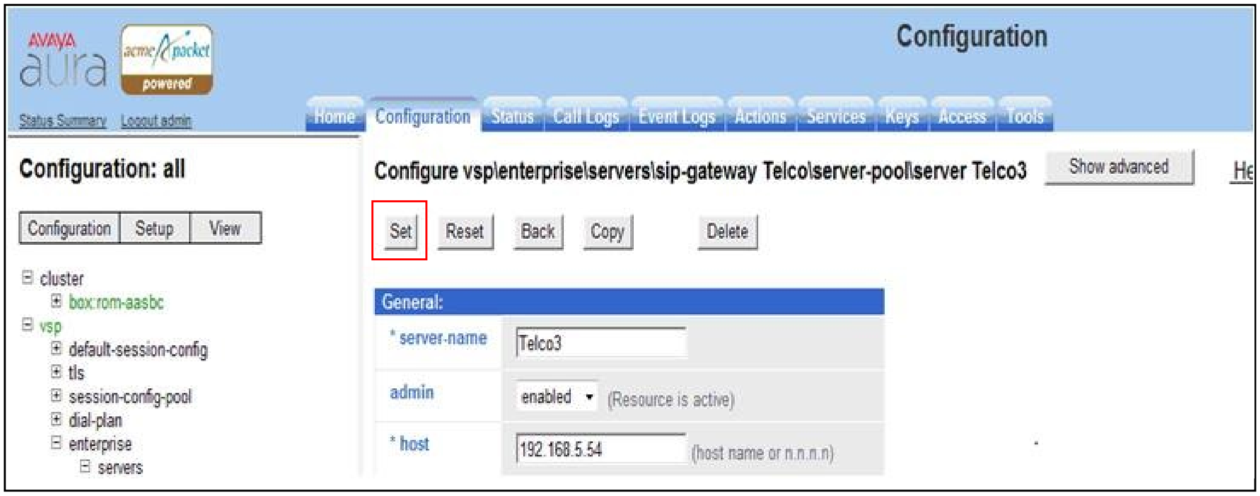
To add the additional IP addresses for the remaining BT SBCs that were not configured during the AASBC installation click on the **Configuration** tab and browse to **vsp → enterprise → servers → sip-gateway Telco → server-pool.** A list of the IP addresses already configured in the server pool is displayed in the right hand pane. Click the **Add server** link.



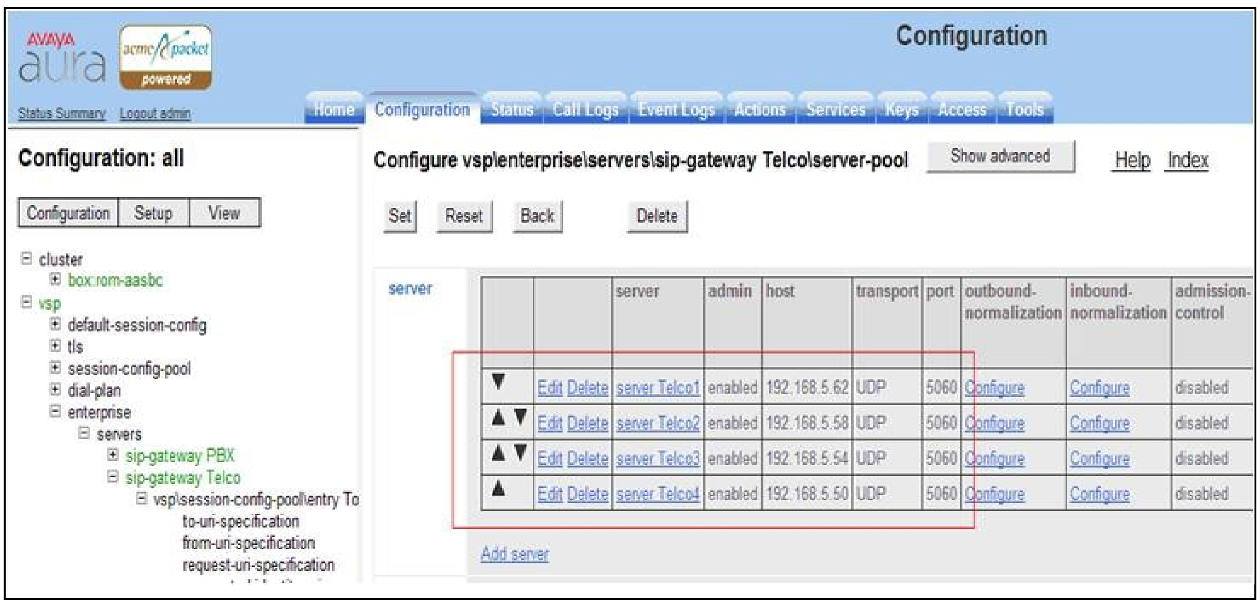
In the resulting page enter a name for the server in the server-name field and an IP address in the host field. Click **Create** to continue.



In the resulting page verify the details entered and click the **Set** button.

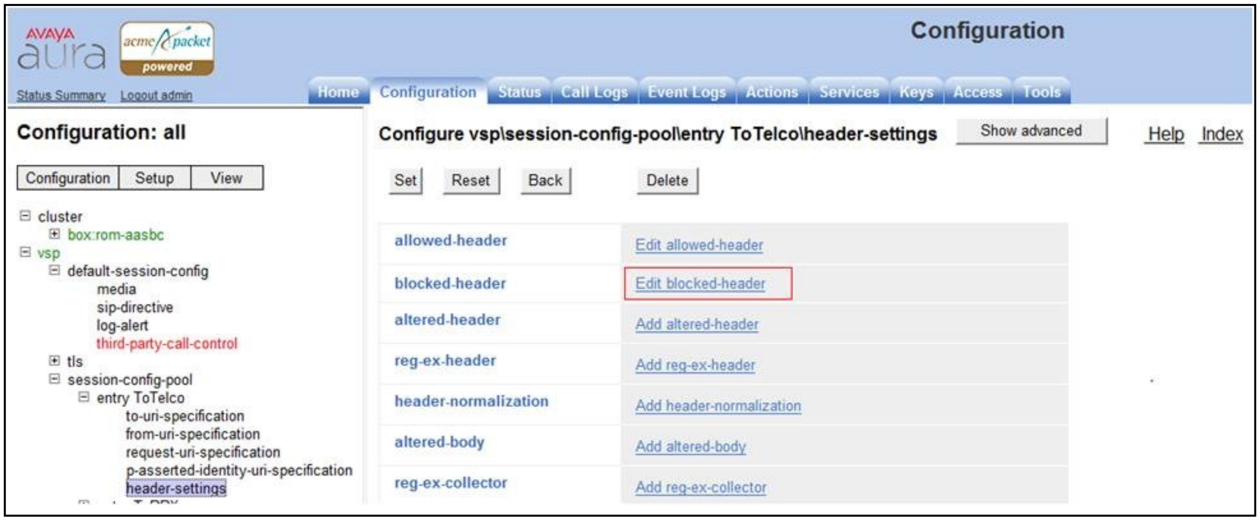


Repeat these steps for each additional IP address that needs to be added to the AASBC server pool. The screen below shows the server pool that was configured for the compliance test.

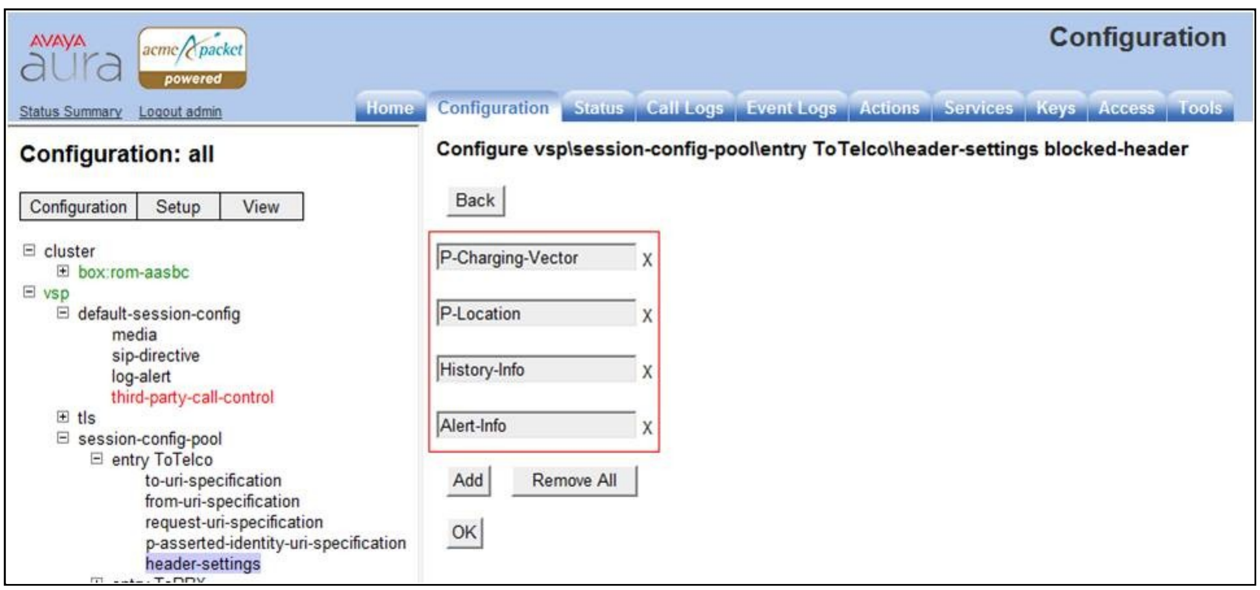


7.4. Stripping SIP Headers

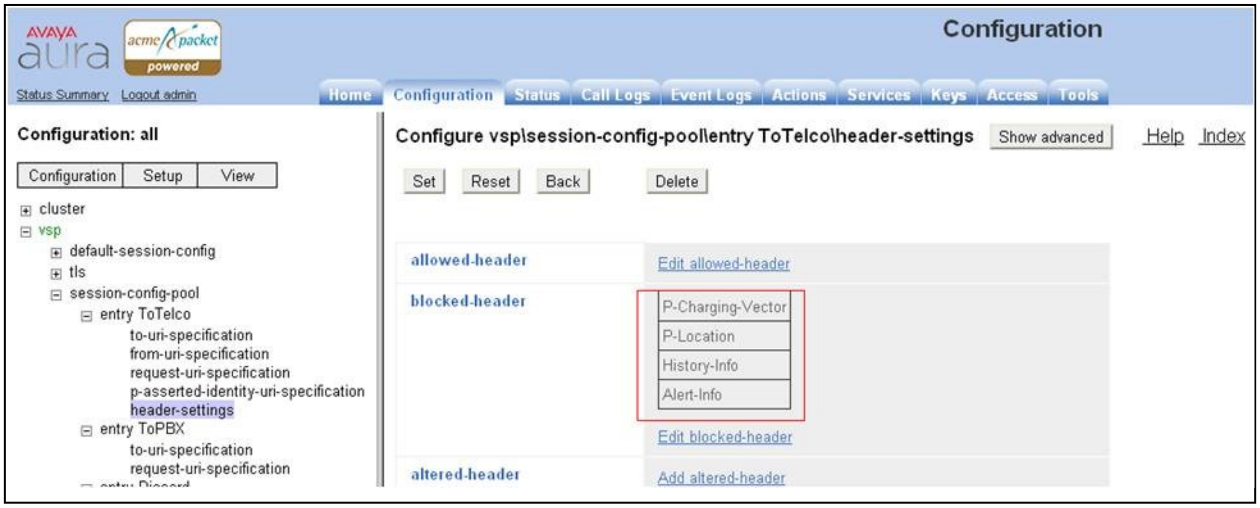
The AASBC can be used to strip SIP headers to prevent particular headers from being sent to the public SIP Service Provider. To strip a SIP header navigate to **vsp → session-config-pool → entry ToTelco → header-settings** and click on the **Edit blocked-header** link.



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

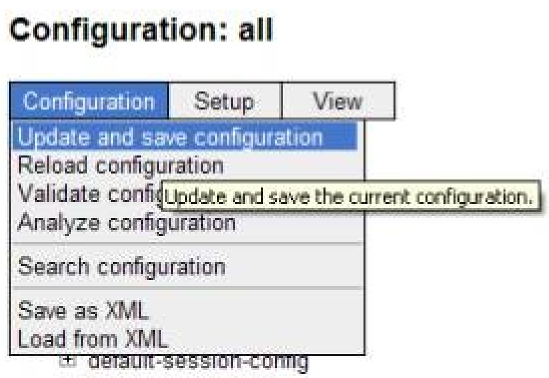


The following screen shows the headers being stripped during testing.



7.5. Save the Configuration

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



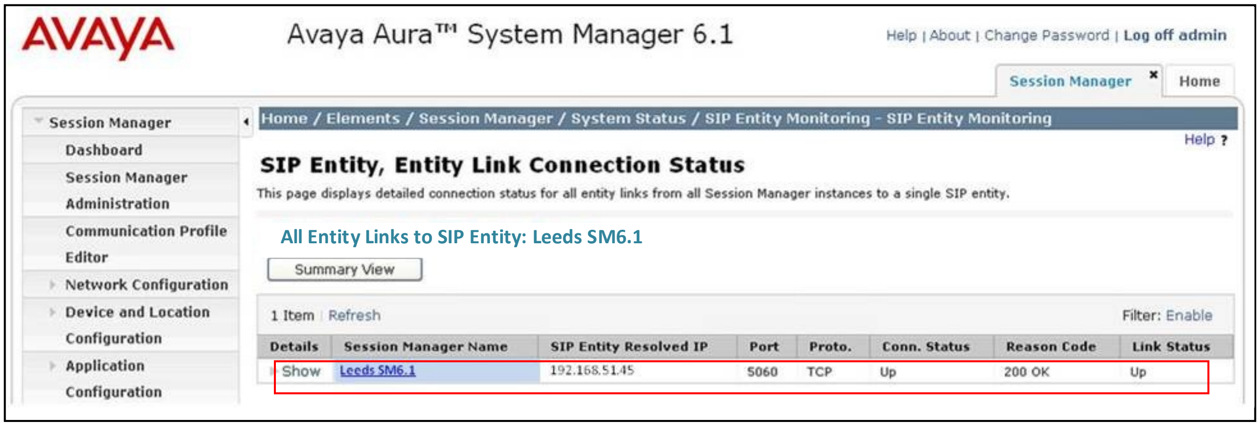
8. Service Provider Configuration

The configuration of the BT equipment used to support the BT SIP Trunk Service is outside of the scope for these application notes and will not be covered. To obtain further information on BT equipment and system configuration please contact an authorized BT representative using the contact details provided in **Section 2.3**.

9. Verification Steps

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

1. From System Manager **Home** screen (see **Section 6.1**), click on **Session Manager** under **Elements**, then 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. See the following screenshot for an example.



2. From the Communication Server 1000Esystem terminal; load overlay 32 and run the command ‘stat vtrm <cust> <x>’ where ‘cust’ is the customer number (usually 0) and ‘x’ is a previously configured SIP trunk route. Confirm all channels on the trunk group display **IDLE REGISTERED**.

```
stst vtrm 0 100

*************************************
STATUS OF VTRL IP TRUNK ROUTE AND MBRS
*************************************



=====================================
CUST ROUTE PROTOCOL  CALL_DIRCTN
0    100     SIP       IN AND OUT

DCH 50  SSRC TOTAL 2048  SSRC USED 77  SSRC AVAILABLE 1971

MBR STATUS

IDLE UNREGISTERED 0
IDLE REGISTERED 15
BUSY 0
MBSY 0
DSBL UNREGISTERED 0
DSBL REGISTERED 0
LCKO 0
```

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 remains 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.

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Communication Server 1000E, Avaya Aura® Session Manager and Avaya Aura® Session Border Controller to the BT SIP Trunk Service. BT SIP Trunk Service is a SIP-based Voice over IP solution providing businesses with a flexible, cost-saving alternative to traditional hardwired telephony trunks.

11. 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 6.0.3, February 2011.

[2] *Administering Avaya Aura® System Platform*, Release 6.0.3, February 2011.

[3] *Avaya Communication Server 1000E Installation and Commissioning*, Release 7.5, November 2011, Document Number NN43041-310, 05.06.

[4] *Feature Listing Reference Avaya Communication Server 1000,* Release 7.5, November 2010, Document Number NN43001-111, 05.01.

[5] *Installing and Upgrading Avaya Aura® System* Manager, Release 6.1, April 2011, Document Number 03-603473.

[7] *Administering Avaya Aura® Session Manager,* Release 6.1, March 2011, Document Number 03-603324.

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

Appendix A – Avaya Communication Server 1000 Software

Avaya Communication Server 1000E call server patches and plug_ins

```
18/08/11 10:33:16
TID: 008808096

VERSION 4021

System type is - Communication Server 1000E/CP PM

CP PM - Pentium M 1.4 GHz

IPMGs Registered:              4
IPMGs Unregistered:            0
IPMGs Configured/unregistered:  2


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

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


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

Avaya Communication Server 1000E call server deplists

```
VERSION 4021
RELEASE 7
ISSUE 50 Q +
DepList 1: core Issue: 02 (created: 2010-11-30 15:12:45 (est))

IN-SERVICE PEPS
PAT# CR #           PATCH REF #     NAME      DATE        FILENAME       SPECINS
000  wi00832106     ISS1:1OF1       p30550_1  14/12/2010  p30550_1.cpm   NO
001  wi00835093     ISS1:1OF1       p30553_1  14/12/2010  p30553_1.cpm   YES
002  wi00832626     ISS2:1OF1       p30560_2  14/12/2010  p30560_2.cpm   NO
MDP>LAST SUCCESSFUL MDP REFRESH :2010-12-06 15:33:54(Local Time)
MDP>USING DEPLIST ZIP FILE DOWNLOADED :2010-12-01 08:31:36(est)
```

Avaya Communication Server 1000E signaling server service updates

```
Product Release: 7.50.17.00
In system patches: 0
In System service updates: 8
PATCH#  IN_SERVICE   DATE       SPECINS   REMOVABLE   NAME
0       Yes          07/02/11   NO        YES         cs1000-baseWeb-7.50.17.01-1.i386.000
1       Yes          07/02/11   NO        YES         cs1000-linuxbase-7.50.17.04-00.i386.000
2       Yes          07/02/11   NO        YES         cs1000-sps-7.50.17-01.i386.000
3       Yes          07/02/11   NO        YES         cs1000-shared-pbx-7.50.17-01.i386.000
4       Yes          07/02/11   NO        YES         cs1000-bcc-7.50.17.03-00.i386.000
5       Yes          07/02/11   NO        YES         cs1000-Jboss-Quantum-7.50.17.01-1.i386.000
6       Yes          07/02/11   NO        YES         cs1000-vtrk-7.50.17-11.i386.000
7       Yes          07/02/11   NO        YES         cs1000-dmWeb-7.50.17.04-00.i386.001
[admin@primleader-leeds ~]$ spstat
There is no SP in loaded status. The last applied SP: Service_Pack_Linux_7.50_17_20110118.ntl. It
is a STANDARD SP. Has been applied by user nortel on Mon Feb  7 14:59:01 2011.
```

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]
   lhmonitor                    7.50.17
   baseAppUtils                 7.50.17
   dfoTools                     7.50.17
   nnnm                         7.50.17
   cppmUtil                     7.50.17
   oam-logging                  7.50.17
   dmWeb                        n/a         [patched]
   baseWeb                      n/a         [patched]
   ipsec                        7.50.17
   Snmp-Daemon-TrapLib          7.50.17
   ISECSH                       7.50.17
   patchWeb                     7.50.17
   EmCentralLogic               7.50.17
Application configuration: SS_EM
Packages: SS EM
Configuration version:     7.50.17-00
   dbcom                        7.50.17
   cslogin                      7.50.17
   sigServerShare               7.50.17     [patched]
   csv                          7.50.17
   tps                          7.50.17
   vtrk                         7.50.17     [patched]
   pd                           7.50.17
   sps                          7.50.17     [patched]
   ncs                          7.50.17
   gk                           7.50.17
   EmConfig                     7.50.17
   emWeb_6-0                    7.50.17
   emWebLocal_6-0               7.50.17
   csmWeb                       7.50.17
   bcc                          7.50.17     [patched]
   ftrpkg                       7.50.17
   cs1000WebService_6-0         7.50.17
   managedElementWebService     7.50.17
   mscAnnc                      7.50.17
   mscAttn                      7.50.17
   mscConf                      7.50.17
   mscMusc                      7.50.17
   mscTone                      7.50.17
```

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.