Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Communication Server 1000E R7.5 with Avaya Aura® Session Manager 6.1 and Acme Packet Net-Net 4500 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 the BT Global Services NOAS SIP Trunk Service and an Avaya SIP enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager and Avaya Communication Server 1000E. BT is a member of the DevConnect Service Provider program.

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

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between the BT SIP Trunk Service and an Avaya SIP enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager and Avaya Communication Server 1000E connected to the BT SIP Trunk Service via an Acme Packet Net-Net 4500 Session Border Controller (SBC). Customers using this Avaya SIP-enabled enterprise solution with the BT SIP Trunk Service are able to place and receive PSTN calls via a dedicated Internet connection and the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks. This approach normally results in lower cost for the enterprise.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using an Avaya SIP telephony solution consisting of Session Manager and Communication Server 1000E. The enterprise site was configured to use the SIP Trunk Service provided by BT, with all SIP traffic connecting to the BT SIP Trunk Service via an Acme Packet 4500 SBC.

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 codecs.
- Fax calls to/from a group 3 fax machine to a PSTN connected fax machine using the T.38 transmission mode.
- 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 and response 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:

- The Calling Line Identity (CLI) presented to a PSTN called party is set to a pre-configured trunk number if the CLI is withheld at the enterprise side.
- 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 tested.
- G729 annex b (silence suppression) is not supported by BT SIP Trunk Service and thus was not tested.
- G711mu is not supported by BT SIP Trunk Service and thus was not tested.
- Early media is only supported for UEXT type phones on Communication Server 1000.
- PSTN called party hangup during an active call did not cause the call to drop. The Communication Server 1000E caller must hangup 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; this is a PSTN imposed restriction. The same restriction exists for supervised transfers of an existing PSTN call to a PSTN called party.
- Call hold has a time limit of less than 16 minutes. If this time limit is exceeded, the call drops. This is a PSTN imposed restriction.
- Calls to/from SMC 3456 soft clients using unsupported codecs failed, most likely because the call server was unable to determine the set capabilities and the SMC 3456 not correctly handling the calls.
- The BT SIP Trunk Service did not handle some SIP 5xx messages correctly, causing Call Admission Control (CAC) issues on PSTN calls, with the effect of reducing the pool of available SIP trunks. A workaround was to manually clear the CAC counters. This will be resolved with a software patch to the BT SIP Trunking Service.
- T.38 outgoing Fax calls (either single or multiple page, G.711 setup) only transmitted as clear channel Fax calls. T.38 outgoing Fax does not work with NOAS.
- T.38 outgoing Fax calls (either single or multiple pages, G.729 setup) fail. T.38 outgoing Fax does not work with NOAS.

2.3. Support

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

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 Communication Server 1000E. Endpoints are Avaya 1140e series IP telephones (one with SIP firmware), Avaya 3904 series Digital telephones, 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.

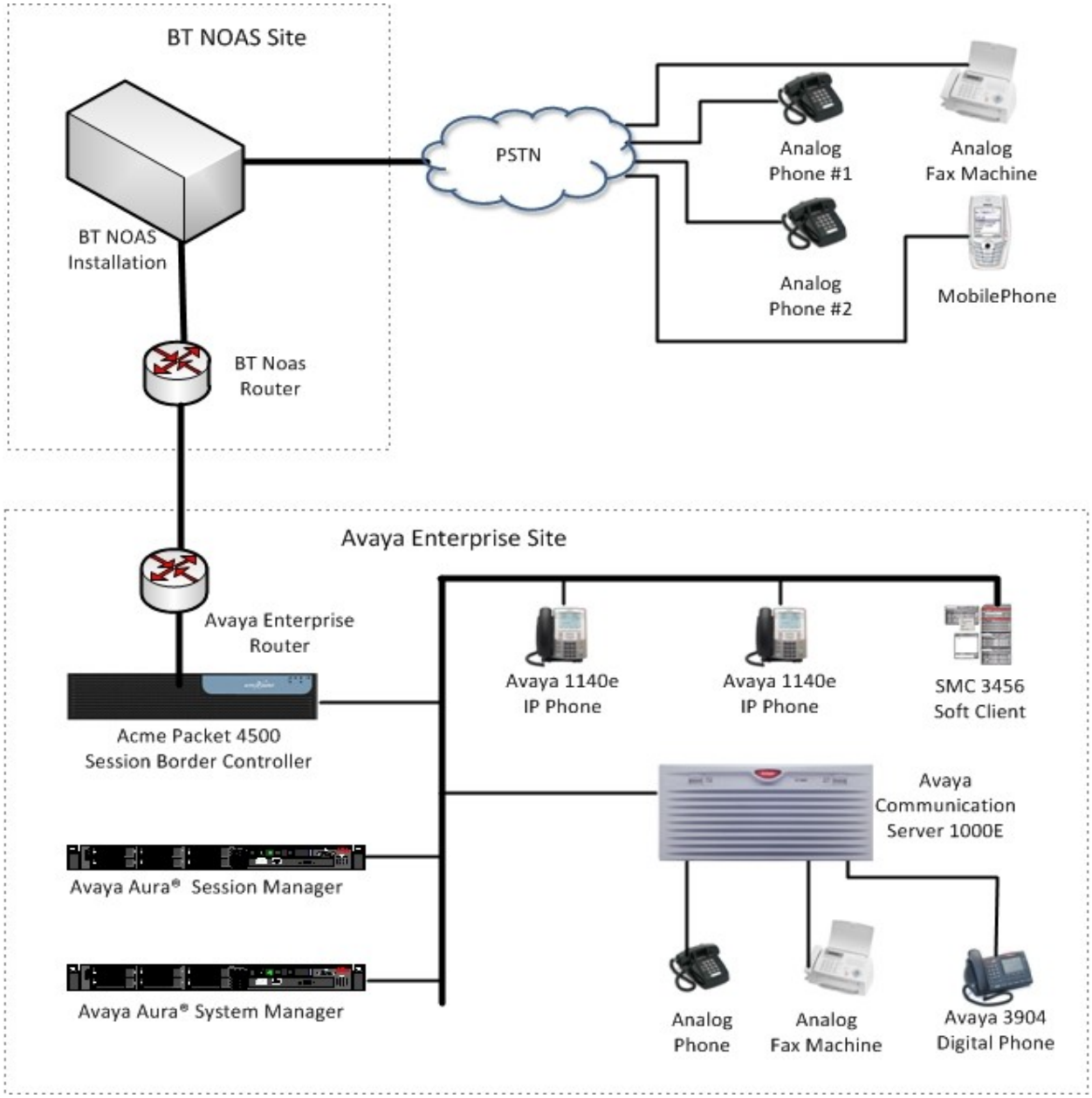


Figure 1: BT Test Configuration

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 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 6.1 (6.1.0.0.610023)
Avaya S8800 Server	Avaya Aura® System Manager 6.1 (6.1.4.0 Build Number 6.1.0.4.5072)
Avaya 1140e Unistim Phone	5.0
Avaya 1140e SIP Phone	4.00.03.00
Analog Phone	N/A
BT SIP Trunk Service	2.1.0.8
Acme Packet Net-Net 4500 Session Border Controller	version 6.4

5. Configure Avaya Communication Server 1000E

This section describes the steps required to configure Communication Server 1000E for SIP Trunking and also the necessary configuration for terminals (analog, SIP and IP phones). SIP trunks are established between Communication Server 1000E and Session Manager. These SIP trunks carry SIP Signaling associated with BT SIP Trunk Service. For incoming calls, the Session Manager receives SIP messages from the Acme Packet 4500 SBC, through which the BT Global Services NOAS SIP Trunk service directs incoming SIP messages to Communication Server 1000E (see **Figure 1**). The Acme Packet 4500 SBC media manager has been activated to ensure RTP packets are routed correctly from the Acme public interface to the private interface and vice versa. Once a SIP message arrives at Communication Server 1000E, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed. All outgoing calls to the PSTN are processed within Communication Server 1000E and may be first subject to outbound features such as route selection, digit manipulation and class of service restrictions. Once Communication Server 1000E selects a SIP trunk, the SIP signaling is routed to the Session Manager. The Session Manager directs the outbound SIP messages to the Acme Packet 4500 SBC and on to the BT network. Specific Communication Server 1000E configuration was performed using Element Manager and the system terminal interface. The general installation of the Avaya Communication Server 1000E and System Manager and Session Manager is presumed to have been previously completed and is not discussed here.

5.1. Confirm System Features

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

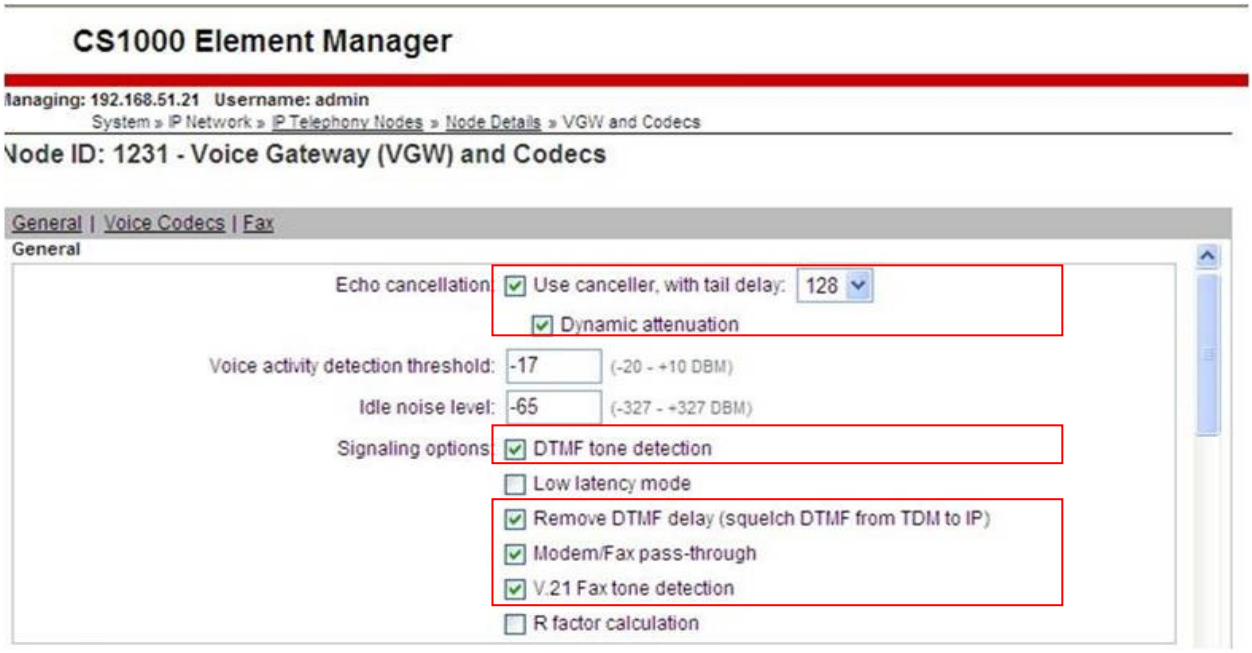
```
System type is - Communication Server 1000E/CPPM Linux
CPPM - Pentium M 1.4 GHz

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

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

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

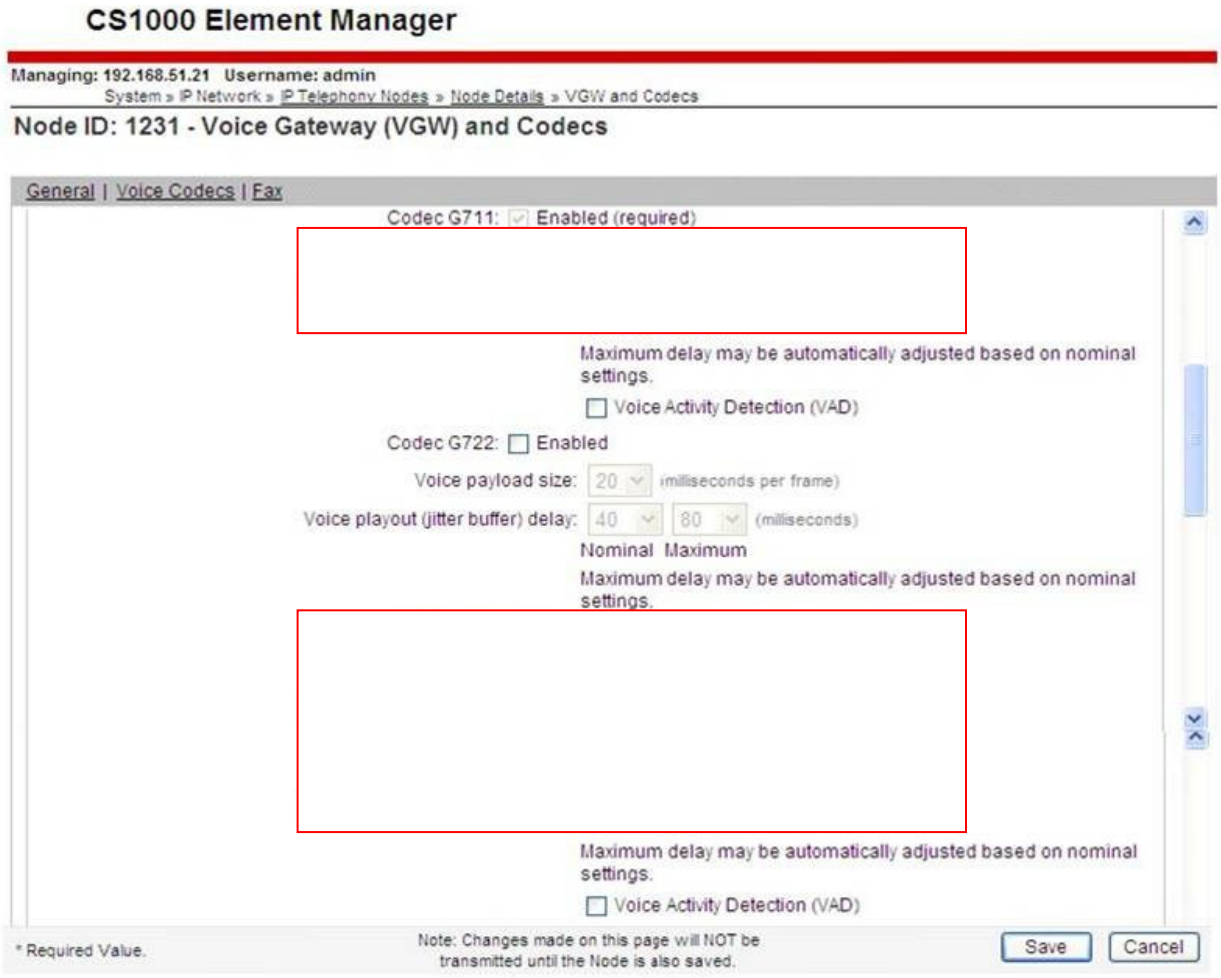
```
REQ: prt
TYPE: net
TYPE NET_DATA
CUST 0

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

5.2. Configure Codecs for Voice and FAX operation

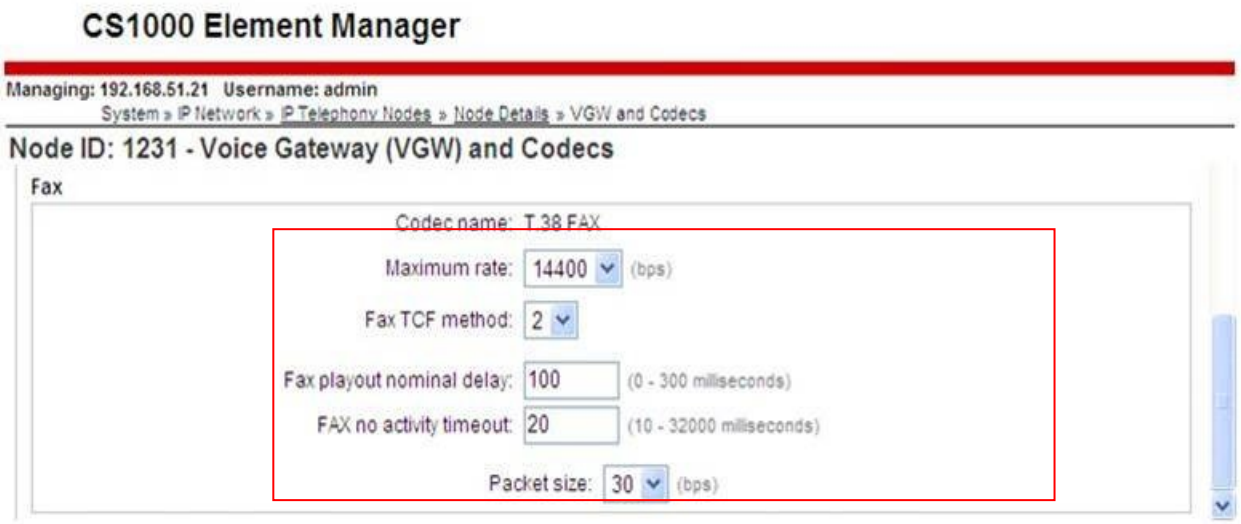
The BT Global Services NOAS SIP Trunk service supports G.711A and G.729A voice codecs and T.38 FAX transmissions. Using the Communication Server 1000E element manager sidebar, navigate to the **IP Network → IP Telephony Nodes → Node Details → VGW and Codecs** property page and configure the Communication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



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

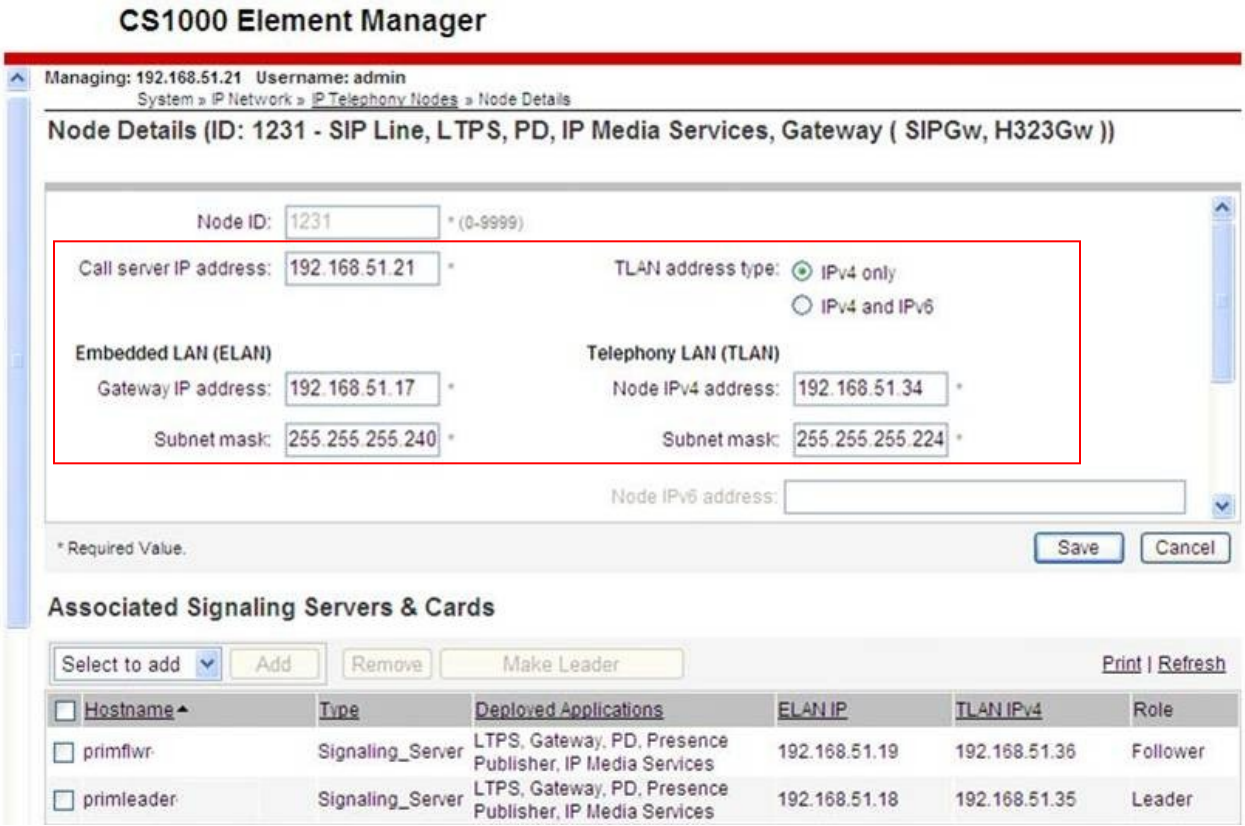


Finally, configure the Fax settings as in the highlighted section of the next screenshot.

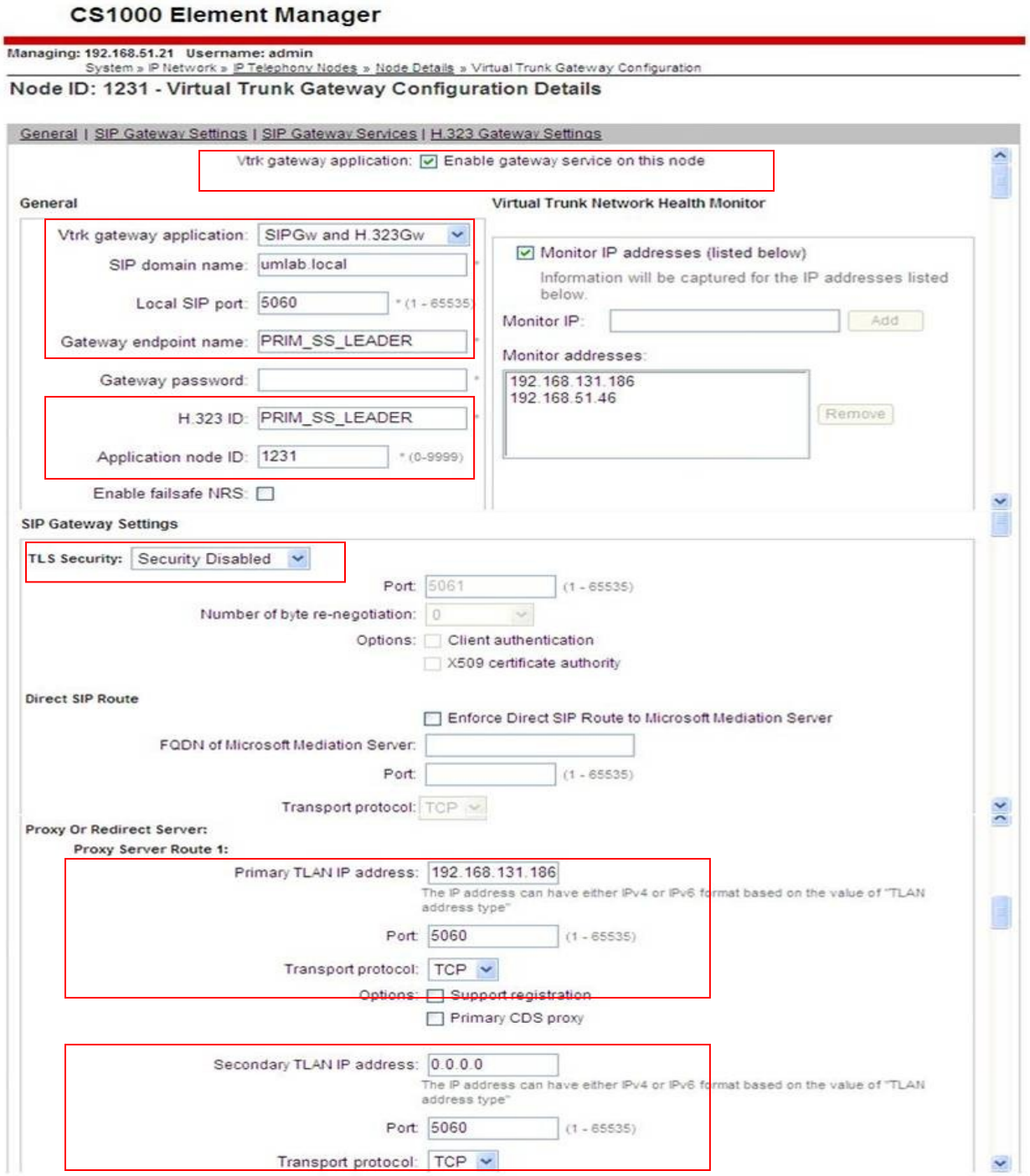


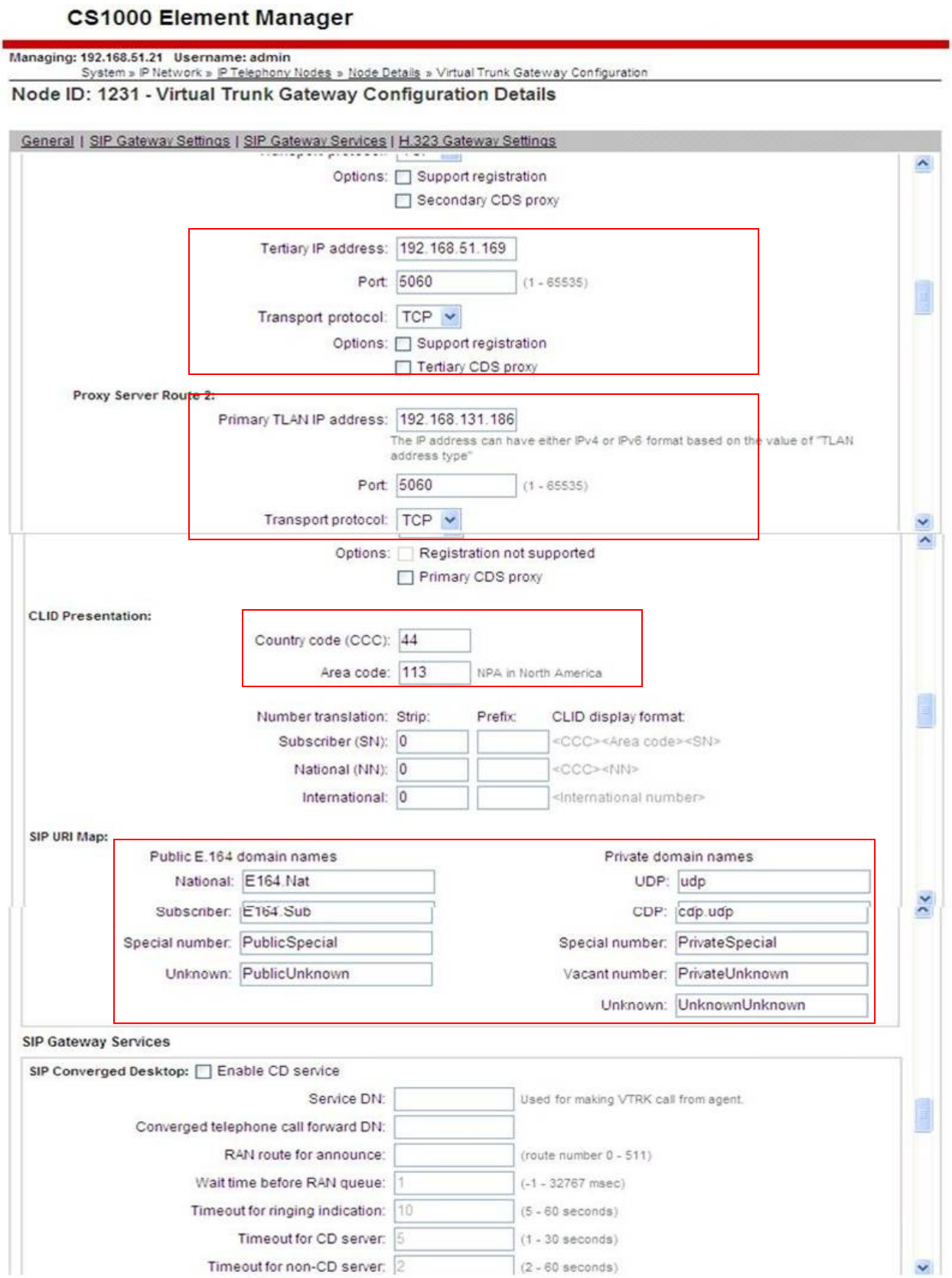
5.3. Virtual Trunk Gateway Configuration

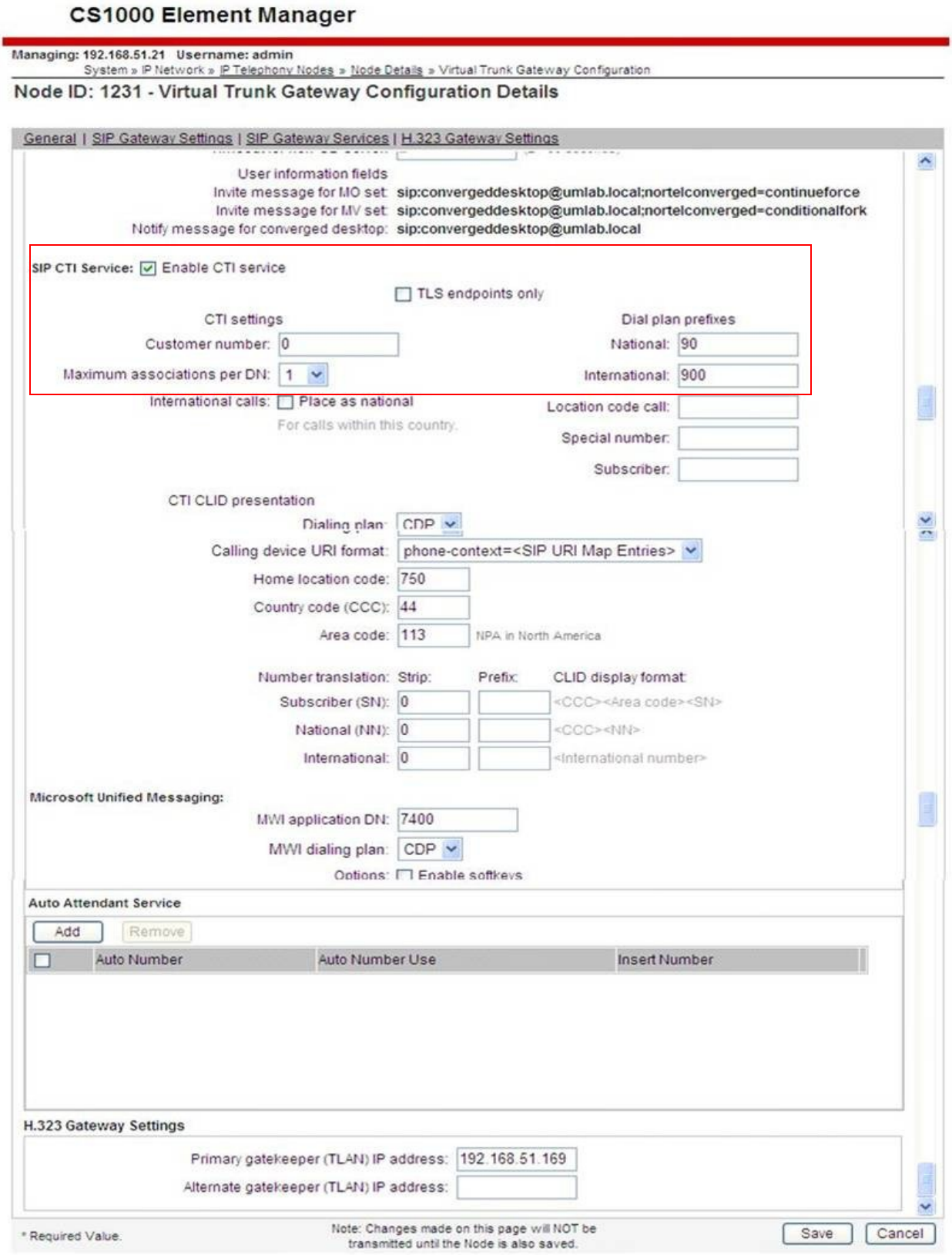
Use Communication Server 1000E Element Manager to configure the system node properties. Navigate to the **System → IP Networks → IP Telephony Nodes → Node Details** and verify the highlighted section is completed with the correct IP addresses and subnet masks.



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







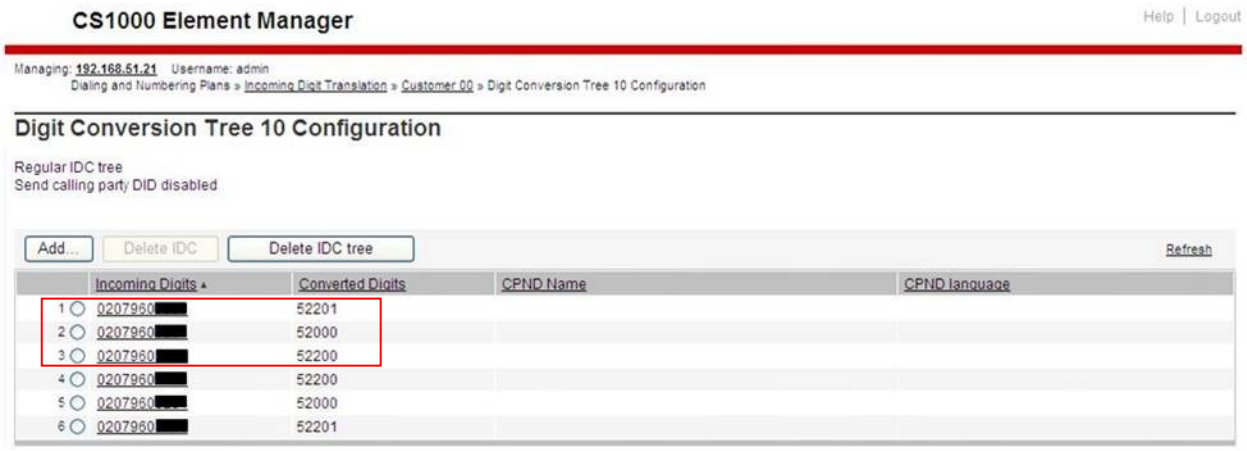
5.4. Configure Bandwidth Zones

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.

	Zone	Intrazone Bandwidth	Intrazone Strategy	Interzone Bandwidth	Interzone Strategy	Resource Type	Zone Intent	Description
1	1	100000	BQ	100000	BQ	SHARED	MO	GR_PRIM
2	2	100000	BQ	100000	BB	SHARED	MO	GR_SEC
3	3	100000	BQ	10000	BB	SHARED	MO	SURV_MG1000
4	4	1000000	BQ	1000000	BQ	SHARED	VTRK	SIPLINEZONE
5	253	1000000	BQ	1000000	BB	SHARED	VTRK	SIP_VTRK_NOAS
6	254	100000	BQ	10000	BQ	SHARED	MO	VIRTUALSETS
7	255	100000	BQ	100000	BQ	SHARED	VTRK	VIRTUAL_TRKS

5.5. Configure Incoming Digit Conversion Table

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



	Incoming Digits	Converted Digits	CPND Name	CPND language
1	0207960[redacted]	52201		
2	0207960[redacted]	52000		
3	0207960[redacted]	52200		
4	0207960[redacted]	52200		
5	0207960[redacted]	52000		
6	0207960[redacted]	52201		

5.6. Configure SIP Trunks

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

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

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

```
Overlay 17
ADAN     DCH 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 same value used in **Section 5.4** for **VIRTUALSETS**.

```
Overlay 20 IP Telephone configuration
DES  1140
TN   096 0 01 16  VIRTUAL
TYPE 1140
CDEN 8D
CTYP XDLC
CUST 0
NUID
NHTN
CFG_ZONE 00254
CUR_ZONE 00254
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 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.

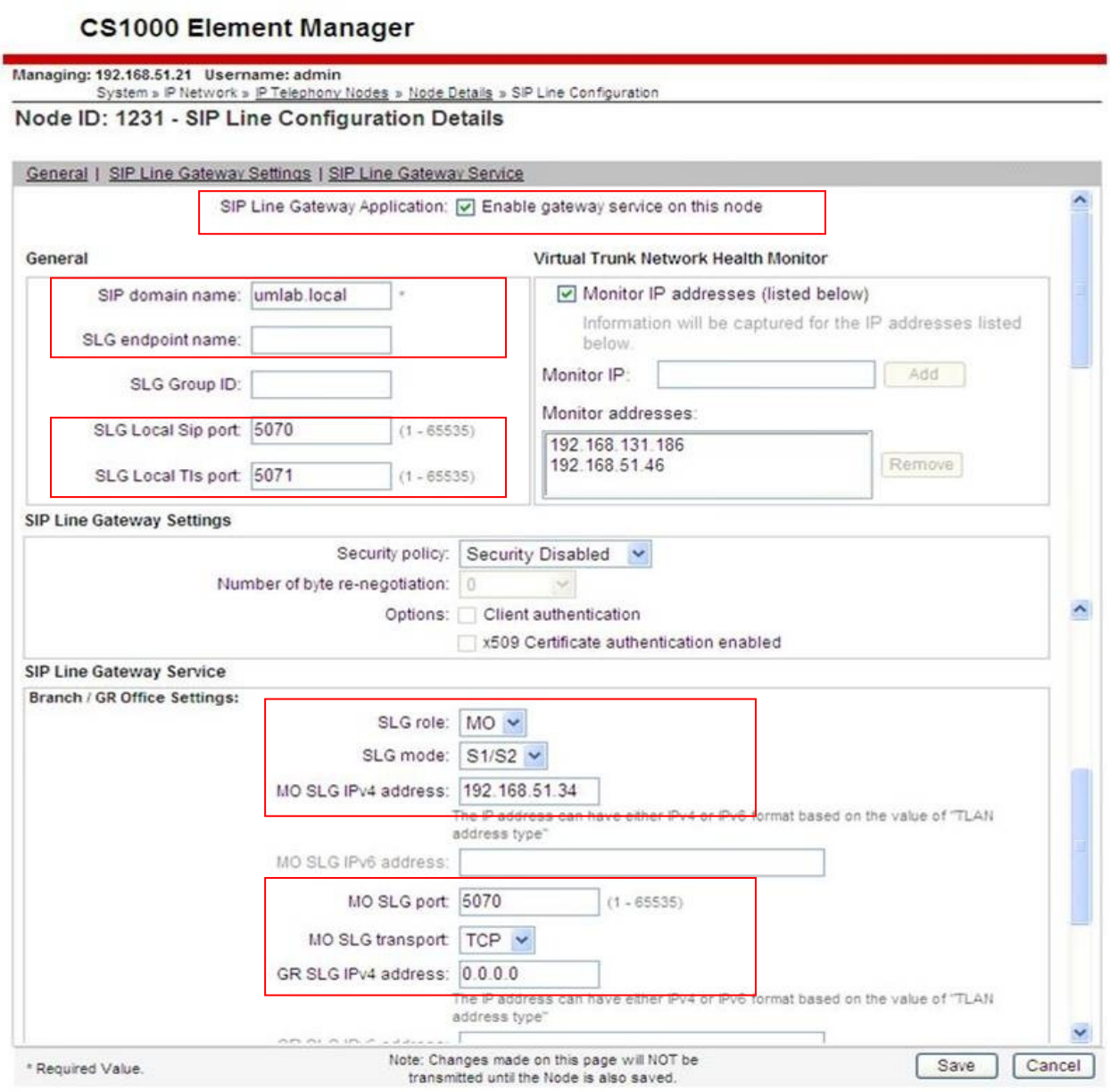
```
Overlay 20 – Analog Telephone Configuration
DES  500
TN   100 0 00 03
TYPE 500
CDEN 4D
CUST 0
MRT

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.

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

If a numerical value is entered against the **UAPR** setting, this number will be prepended 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 6.5.1**. The IP address configured in **MO SLG IPv4 address** is the system **NODE IP address**, as previously configured in **Section 5.3**.



5.9. Configure SIP Line Telephones

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

```
Overlay 20 – SIP Telephone Configuration
DES  SIPD
TN   096 0 01 15  VIRTUAL
TYPE UEXT
CDEN 8D
CTYP XDLC
CUST 0
UXTY SIPL
MCCL YES
SIPN 1
SIP3 0
FMCL 0
TLSV 0
SIPU 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
```

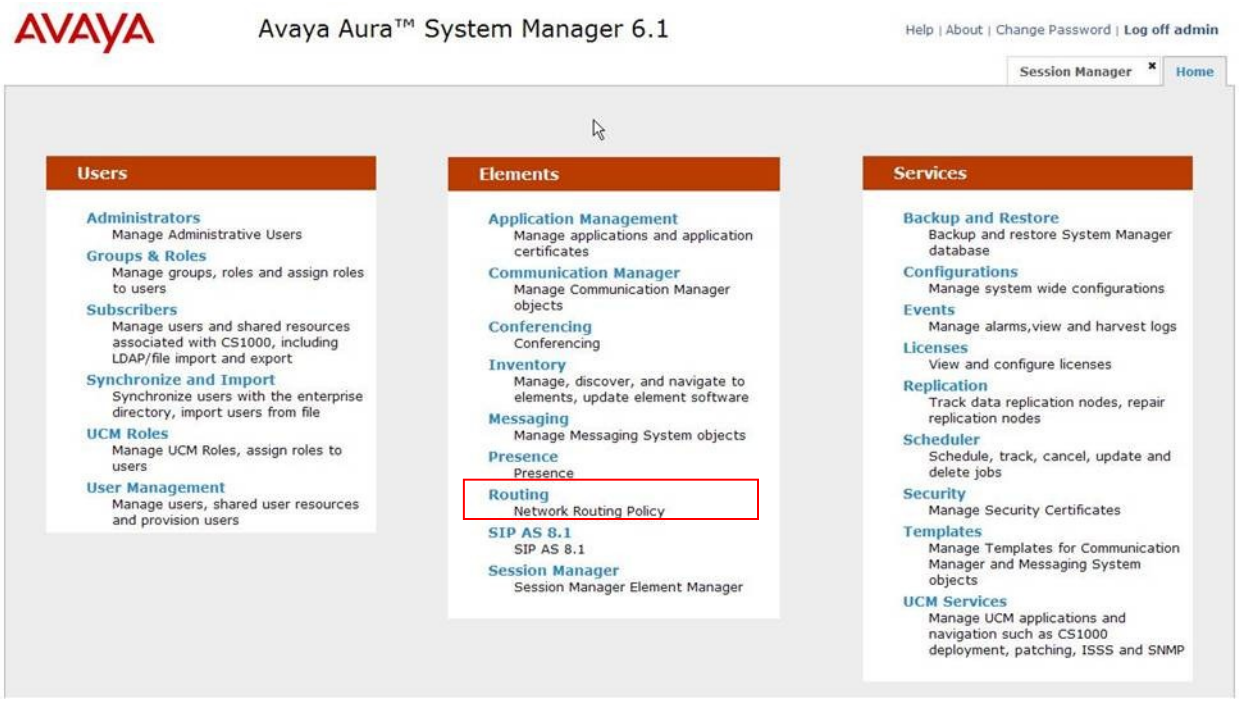
6. Configuring Avaya Aura® Session Manager

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 Avaya Aura® Session 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

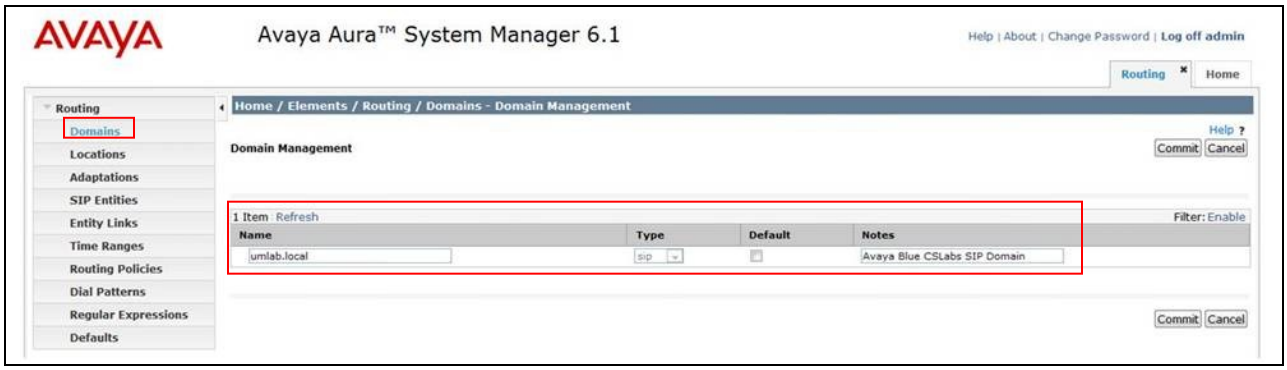
Access the System Manager using a Web Browser by entering **http://<FQDN >/SMGR**, where **<FQDN>** is the fully qualified domain name of System Manager. Log in using appropriate credentials (not shown) and the **Home** tab will be presented with menu options shown below.



6.2. Administer SIP Domain

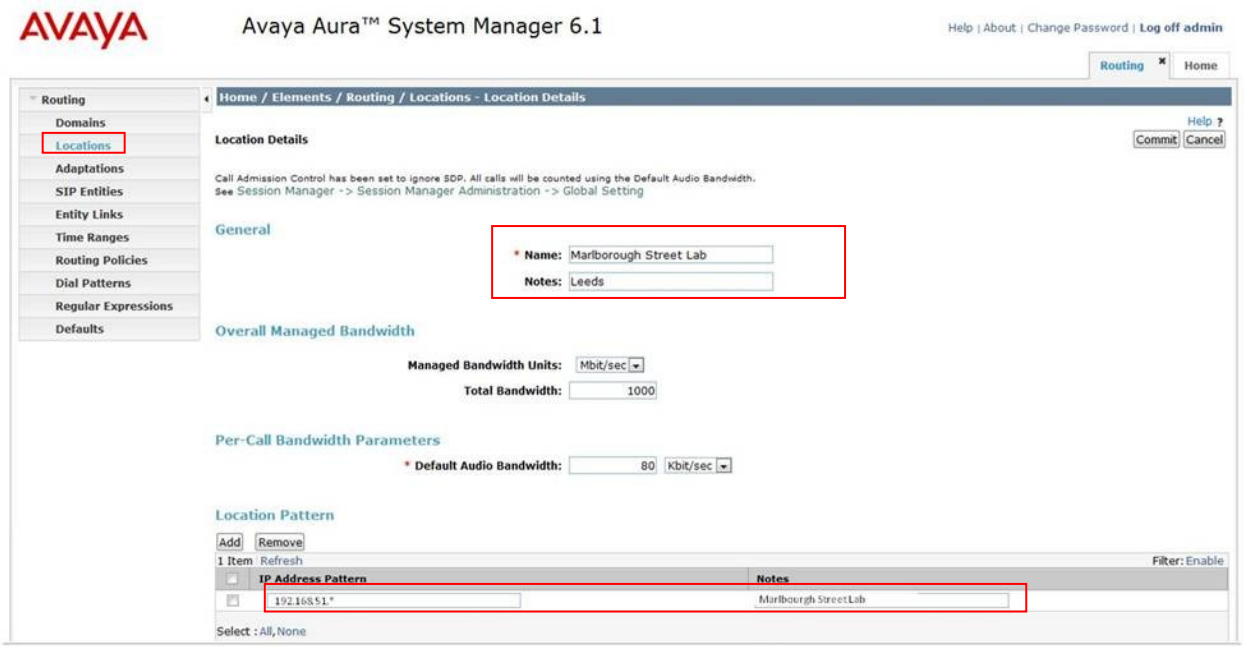
To add the SIP domain that will be used with Session Manager, select **Routing** from the Elements Home tab menu and in the resulting tab select **Domains** from left hand menu. Click the **New** button (not shown) to create a new SIP domain entry. In the **Name** field, enter the domain

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 the **Routing** tab, select **Locations** from the left hand menu. Under **General**, in the **Name** field enter an informative name for the location. Scroll to the bottom of the page and under **Location Pattern**, click **Add**, then enter an **IP Address Pattern** in the resulting new row, '*' is used to specify any number of allowed characters at the end of the string. Below is the location configuration used for the simulated Enterprise site.

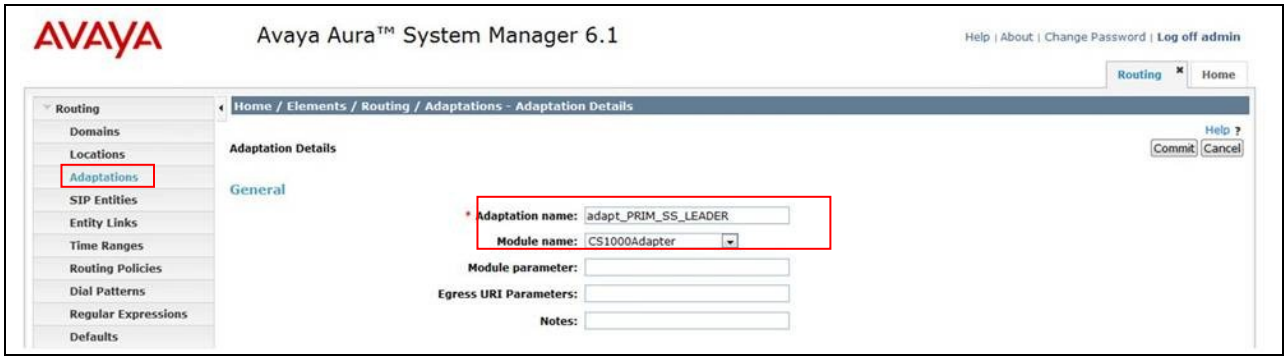


6.4. Administer Adaptations

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 the **Routing** tab, select **Adaptations** on the left hand menu and then click on the **New** button (not shown).

Under **Adaption Details →General**:

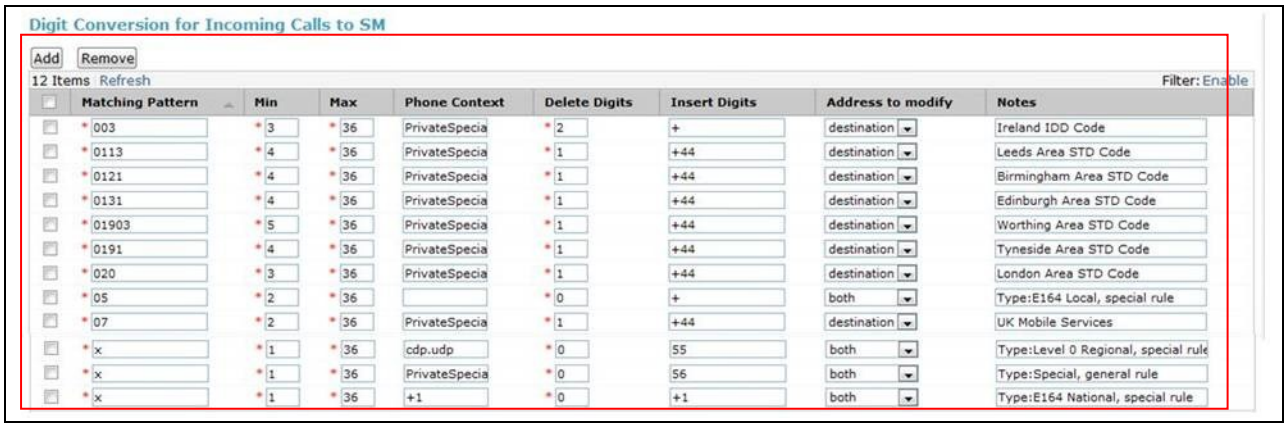
- In the **Adaptation name** field enter an informative name.
- In the **Module name** field, click on the down arrow and then select the <**click to add module**> entry from the drop down list and type **CS1000Adapter** in the resulting New Module Name field.



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.

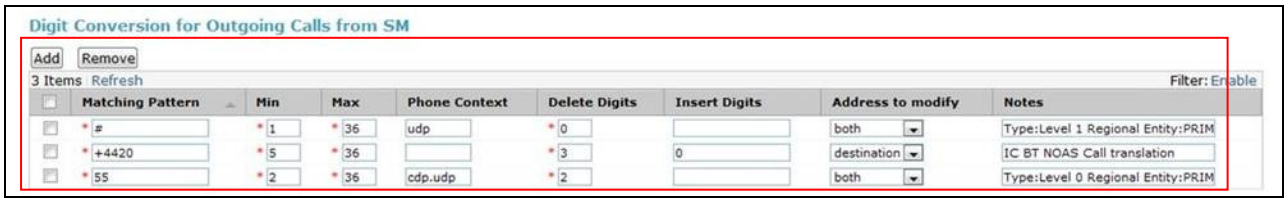
This will ensure any destination numbers received from Communication Server 1000E are converted to the E.164 numbering format before being processed by Session Manager. The following screenshot shows the settings used.



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**:

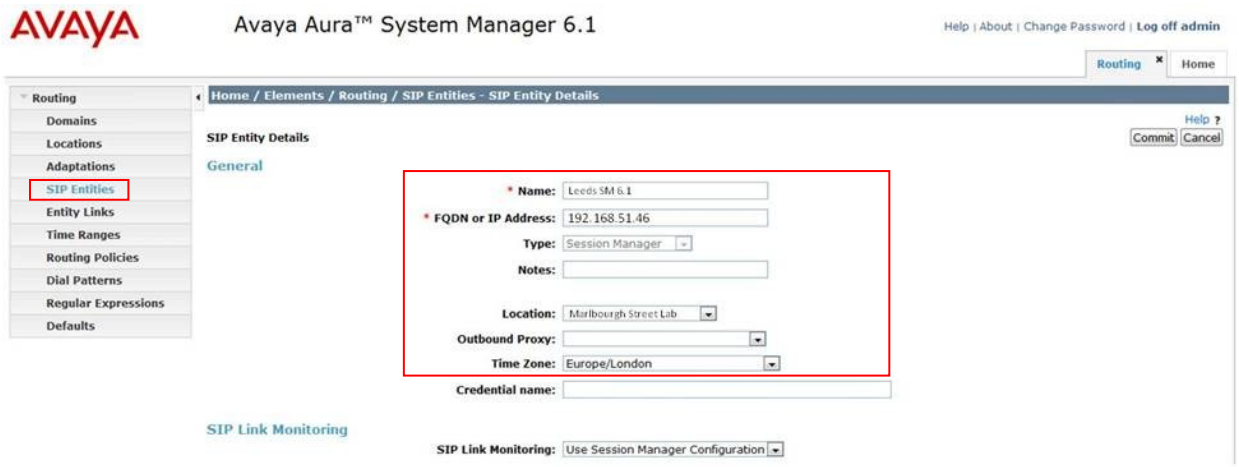
- In the **Name** field enter an informative name.
- In the **FQDN or IP Address** field enter the IP address of Session Manager or the signaling interface on the connecting system.
- In the **Type** field use **Session Manager** for a Session Manager SIP entity, **Other** for a Communication Server 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.

- Session Manager SIP Entity
- Communication Server 1000E SIP Entity
- 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.

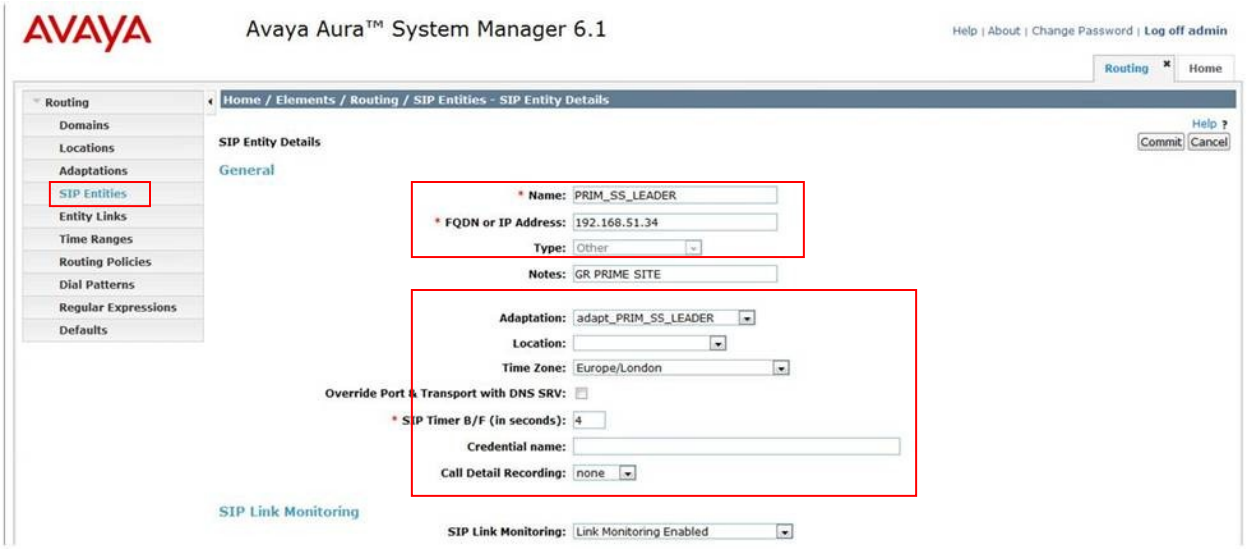


The Session Manager must be configured with the port numbers of the protocols that will be used by the other SIP entities. To configure these, scroll to the bottom of the page and under Port, click Add, then edit the fields in the resulting new row.

- 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.

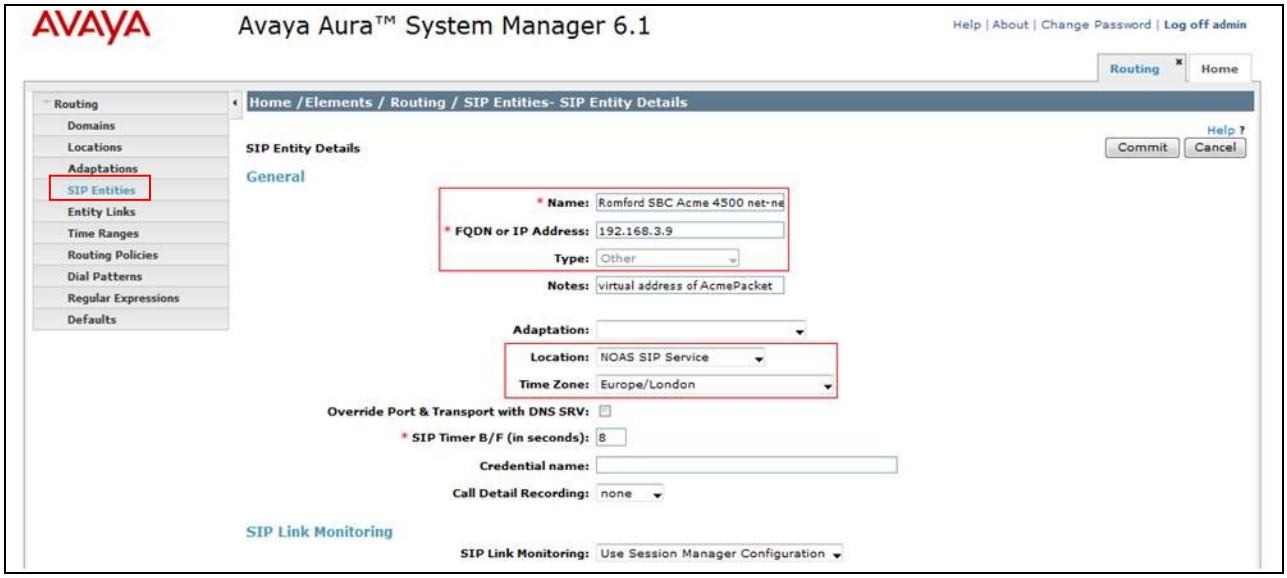
6.5.2. Avaya Communication Server 1000E SIP Entity

The following screenshot shows the SIP entity for Communication Server 1000E which is configured as **Type 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. Acme Packet Net-Net 4500 SBC SIP Entity

The following screen shows the SIP Entity for the Acme Packet 4500 SBC. The **FQDN or IP Address** field is set to the IP address of the SBC private network interface.

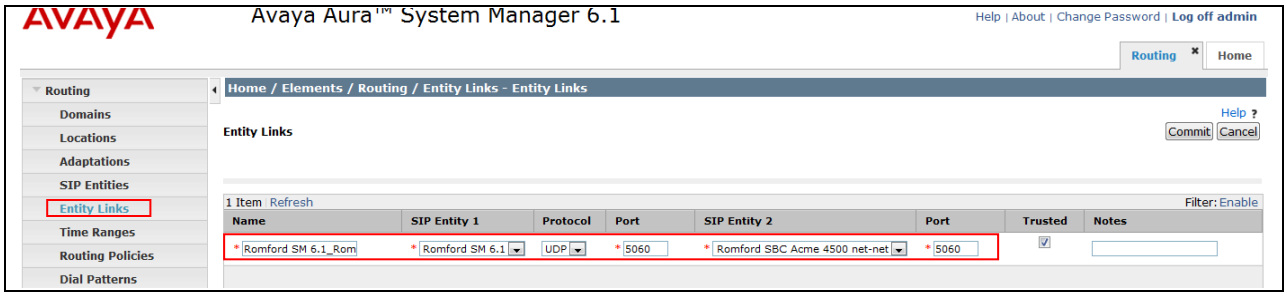


6.6. Administer Entity Links

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 to 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 an example Entity Link used in this configuration.

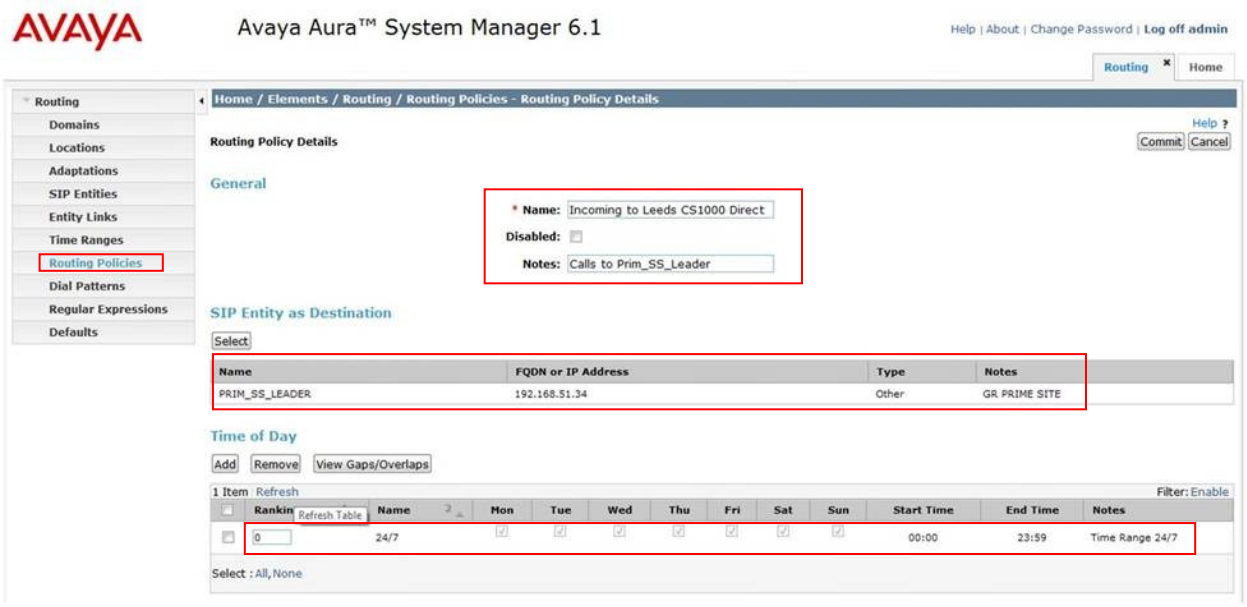


6.7. Administer Routing Policies

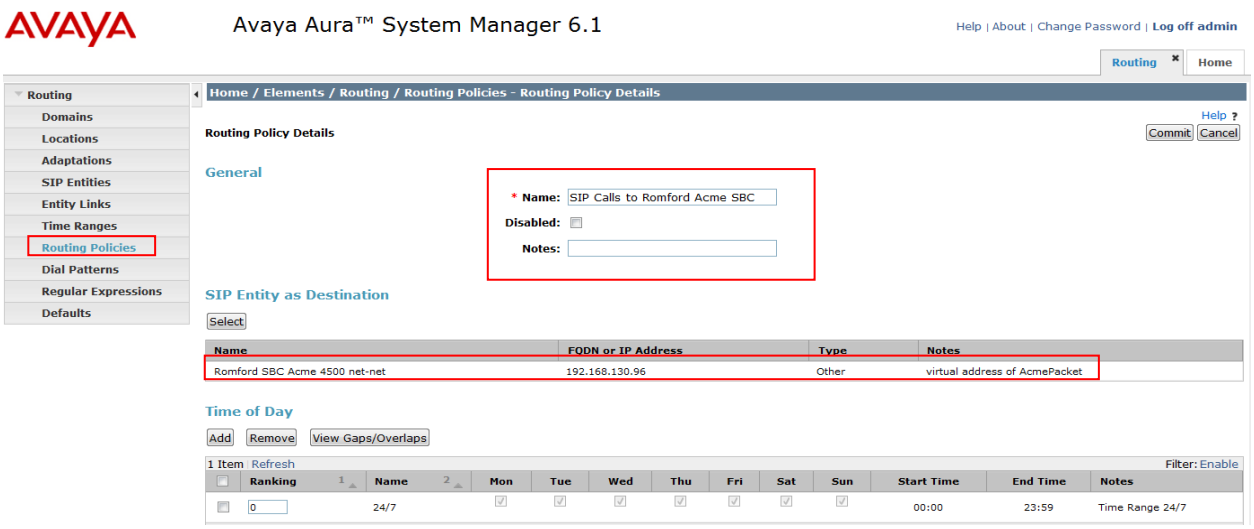
Routing policies must be created to direct how calls will be routed to a system. To add a routing policy, select **Routing Policies** on the left panel menu (see next screenshot) and then click on the **New** button (not shown).

- 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 Acme Packet 4500 SBC.



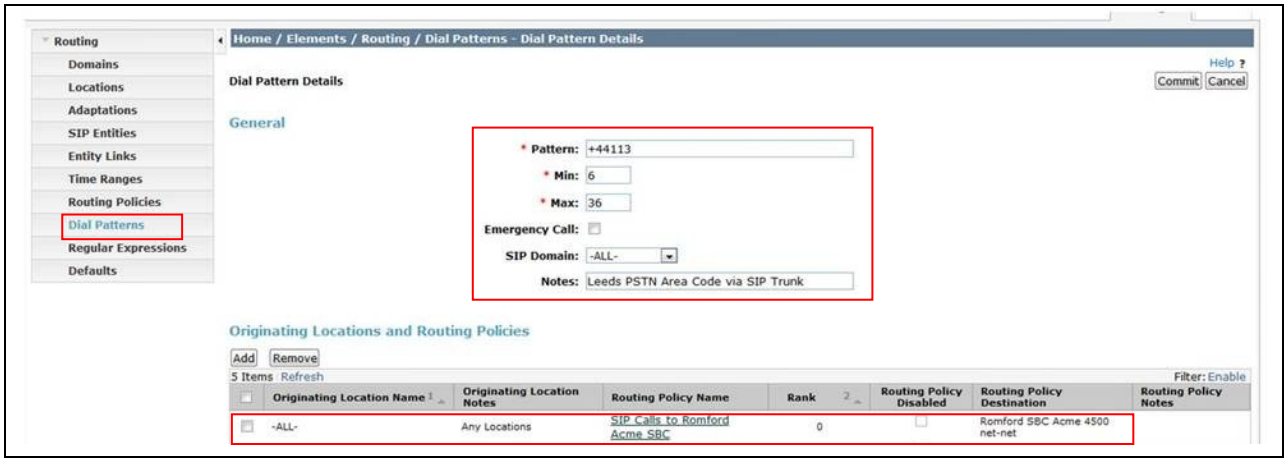
6.8. Administer Dial Patterns

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).

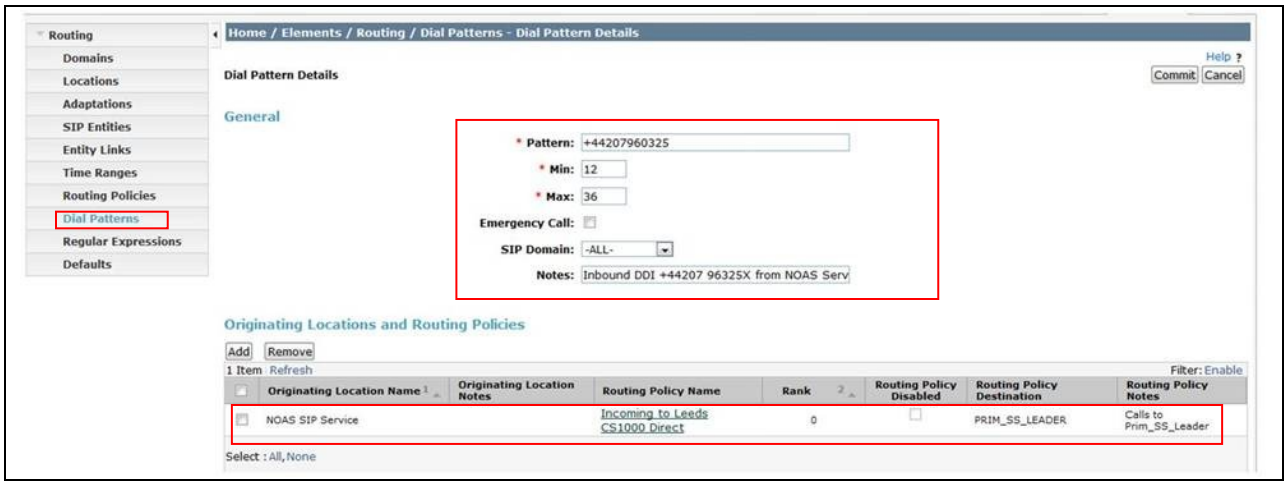
Under **Dial Pattern Details → General**:

- 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 the Acme Packet 45000 SBC routing policy defined in **Section 6.7**. Click **Select** button to save. The following screen shows an example dial pattern configured for BT SIP Trunk Service.



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



7. Configure Acme Packet 4500 Net-Net SBC

This section describes the configuration of the Acme Packet Net-Net 4500 SBC. The Acme Packet 4500 SBC was configured using the Acme Packet Command Line Interface (ACLI). This section assumes the reader is familiar with accessing and configuring the Acme Packet 4500 SBC. This section does not cover the Acme Packet configuration in its entirety, only the fields directly related to the interoperability test will be covered. For completeness the running configuration used during the interoperability testing is displayed in **Appendix B.**

7.1. Accessing Acme Packet 4500 SBC

Connect to the Acme Packet 4500 SBC and login with the appropriate user password. At the prompt, enter the **enable** command and then the superuser password. Once in superuser mode, enter the command **configure terminal** to enter the configuration mode.

7.2. System Configuration

The system configuration defines system-wide parameters for the Acme Packet 4500 SBC. Access the **system-config** element and set the following element parameters:

- **default-gateway**: The IP address of the default gateway for Acme Packet 4500 SBC. In this case, the default gateway is **192.168.131.1**.
- **source-routing**: Set to **enabled**

```
system-config
        hostname
        description
        location

      < text removed for brevity >

        call-trace                    disabled
        internal-trace                disabled
        log-filter                    all
        default-gateway               192.168.131.1
        restart                       enabled
        exceptions
        telnet-timeout                0
        console-timeout               0
        remote-control                enabled
        cli-audit-trail               enabled
        link-redundancy-state         disabled
        source-routing                enabled
        cli-more                      disabled
        terminal-height               24

      < text removed for brevity >
```

7.3. Physical Interfaces

During the compliance test, the Ethernet interface slot 0 / port 0 of the Acme Packet 4500 SBC was connected to the outside, untrusted network. Ethernet slot 1 / port 0 was connected to the inside, enterprise network. A network interface was defined for each physical interface to assign it a routable IP address. Access the **system→ phy-interface** element and set the following element parameters:

- **name**: A descriptive string used to reference the Ethernet interface.
- **operation-type**: Set to **Media** to indicate both signalling and media packets are sent on this interface.
- **slot / port**: The identifier of the specific Ethernet interface used.

```
phy-interface
      name                          M10
      operation-type                Media
      port                          0
      slot                          1
      virtual-mac                   00:08:25:a1:90:0E
      admin-state                   enabled
      auto-negotiation              enabled
      duplex-mode                   FULL
      speed                         100
      last-modified-by              admin@console
      last-modified-date            2010-09-07 15:15:33
phy-interface
      name                          M00
      operation-type                Media
      port                          0
      slot                          0
      virtual-mac                   00:08:25:a1:8f:4E
      admin-state                   enabled
      auto-negotiation              enabled
      duplex-mode                   FULL
      speed                         100
      last-modified-by              admin@console
      last-modified-date            2010-09-07 15:15:49
```

7.4. Network Interfaces

Access the **network-interface** element and set the following element parameters:

- **name**: The name of the physical interface defined in **Section 7.3.**
- **ip-address**: The IPv4 address assigned to this interface.
- **pri-utility-addr**: The physical address of the primary Acme Packet 4500 SBC in the high availability pair.
- **sec-utility-addr**: The physical address of the secondary Acme Packet 4500 SBC in the high availability pair.
- **netmask**: Subnet mask for the IP subnet.
- **gateway**: The subnet gateway address.
- **hip-ip-list**: The virtual IP address assigned to the Acme Packet 4500 SBC on this interface.
- **icmp-address**: The list of IP addresses which the Acme Packet 4500 SBC will answer ICMP requests on this interface.

The settings for the outside, untrusted side network interface are shown below

```
network-interface
       name                          M00
       sub-port-id                   0
       description                   Facing Noas
       hostname
       ip-address                     192.168.131.133
       pri-utility-addr                  192.168.131.130
       sec-utility-addr                  192.168.131.132
       netmask                        255.255.255.0
       gateway                       192.168.131.1
       sec-gateway
       gw-heartbeat
              state                         enabled
              heartbeat                     10
              retry-count                   3
              retry-timeout                 3
              health-score                  30
       dns-ip-primary
       dns-ip-backup1
       dns-ip-backup2
       dns-domain
       dns-timeout                   11
        hip-ip-list                     192.168.131.133
       ftp-address
        icmp-address                   192.168.131.133
       snmp-address
       telnet-address
       last-modified-by              admin@192.168.131.60
```

The settings for the inside, enterprise side network interface are shown below.

```
network-interface
       name                          M10
       sub-port-id                   0
       description                   Facing Avaya
       hostname
       ip-address                     192.168.130.96
       pri-utility-addr                  192.168.130.170
       sec-utility-addr                 192.168.130.171
       netmask                       255.255.255.0
       gateway                       192.168.130.1
       sec-gateway
       gw-heartbeat
             state                         disabled
             heartbeat                     0
             retry-count                   0
             retry-timeout                 1
             health-score                  32
       dns-ip-primary
       dns-ip-backup1
       dns-ip-backup2
       dns-domain
       dns-timeout                   11
        hip-ip-list                     192.168.130.96
       ftp-address
        icmp-address                   192.168.130.96
       snmp-address
       telnet-address
       last-modified-by              admin@192.168.131.60
       last-modified-date            2010-09-08 14:18:22
```

7.5. **Realm**

A realm represents a group of related Acme Packet 4500 SBC components. Two realms were defined for the compliance test. The **access-noas** realm was defined for the external untrusted network and the **core-noas** realm was defined for the internal enterprise network. Access the **media-manager → realm-config** element and set the following element parameters:

- **identifier**: A descriptive string used to reference the realm.
- **network interfaces**: The network interfaces located in this realm.

```
realm-config
        identifier                     access-noas
        description                    Access Realm for NOAS SAG
        addr-prefix                    0.0.0.0
        network-interfaces
                                       M00:0
        mm-in-realm                    disabled
        mm-in-network                  enabled

< text removed for brevity >

realm-config
        identifier                     core-noas
        description                    Core Realm calls from NOAS SAG to AVAYA
        addr-prefix                    0.0.0.0
        network-interfaces
                                       M10:0
```

```
        mm-in-realm                     disabled
        mm-in-network                   enabled

< text removed for brevity >
```

7.6. SIP Configuration

The SIP configuration defines the global system-wide SIP parameters. Access the **session-router → sip-config** element and set the following element parameters:

- **home-realm-id**: The name of the realm on the internal enterprise side of the Acme Packet 4500 SBC.
- **nat-mode**: Set to **public** which indicates that IPv4 addresses are encoded in SIP messages received from the external realm defined by the SIP NAT. The IPv4 addresses are decoded in messages that are sent to the realm for further information on SIP NAT see reference **[9-11]**
- **registrar-domain**: An asterisk * is specified to allow any domain.
- **registrar-host**: An asterisk * is specified to allow any host.
- **registrar-port**: port used for registration.

```
sip-config
        state                           enabled
        operation-mode                  dialog
        dialog-transparency             disabled
        home-realm-id                   core-noas
        egress-realm-id
        nat-mode                        Public
        registrar-domain                *
        registrar-host                  *
        registrar-port                  5060
        register-service-route          always
        init-timer                      500
        max-timer                       4000

< text removed for brevity >
```

7.7. SIP Interface

The SIP interface defines the IP address and port upon which the Acme Packet 4500 SBC receives and sends SIP messages. Two SIP interfaces were defined; one for each realm. Access the **session-router → sip-interface** element and set the following element parameters:

- **realm-id**: The name of the realm to which this interface is assigned.
- **sip port:**
  - **address**: The IP address assigned to this sip-interface.
  - **port**: The port assigned to this sip-interface.
  - **transport-protocol**: The transport method used for this interface.
  - **allow-anonymous:** Defines from whom SIP requests will be allowed. The value of **agents-only** means SIP requests will only be accepted on this interface from session agents defined in **Section 7.8**)
- **trans-expire:** The time to live in seconds for SIP transactions, this setting controls timers B, F, H and TEE specified in RFC 3261. A value of **0** indicates the timers in **sip-config (Section 7.6)** will be used.

- **invite expire:** The time to live in seconds for SIP transactions that have received a provisional response. A value of **0** indicates the timers in **sip-config** will be used.

```
sip-interface
        state                           enabled
        realm-id                        core-noas
        description                     Core NOAS SAG SIP Interface
        sip-port
                address                         192.168.3.9
                port                            5060
                transport-protocol              UDP
                tls-profile
                allow-anonymous                 agents-only
                ims-aka-profile
        carriers
        trans-expire                    0
        invite-expire                   0

< text removed for brevity >

sip-interface
        state                           enabled
        realm-id                        access-noas
        description                     Interface
        sip-port
                address                         192.168.4.9
                port                            5060
                transport-protocol              UDP
                tls-profile
                allow-anonymous                 agents-only
                ims-aka-profile
        carriers
        trans-expire                    4
        invite-expire                   185

< text removed for brevity >
```

7.8. Session Agent

A session agent defines the characteristics of a signalling peer to the Acme Packet 4500 SBC such as Session Manager. During testing, BT PRI replacement had multiple SBCs. A session agent must be defined for each SIP peer. Access the **session router → session-agent** element and set the following element parameters:

- **hostname**: Fully qualified domain name or IP address of the SIP peer.
- **ip-address**: IP address of the SIP peer
- **port**: The port used by the peer for SIP traffic.
- **app-protocol**: Set to **SIP**.
- **transport-method**: The transport method used for this session agent.
- **realm-id**: The realm id where the peer resides.
- **description**: A descriptive name for the peer.
- **ping-method**: This setting enables SIP OPTIONS to be sent to the peer to verify that the SIP connection is functional and sets the value that will be used In the SIP Max-Forward field. As an example an entry of **OPTIONS;hops=66** would generate OPTIONS messages with a Max Forwards value of 66.

- **ping-interval**: Specifies the interval (in seconds) between each ping attempt.
- **ping-in-service-response-codes:** A list of response codes that the session agent will accept in response to ping requests in order for the session agent to remain in service.
- **in-manipulationid:** The name of the SIP header manipulation to apply to inbound SIP packets.
- **out-manipulationid:** The name of the SIP header manipulation to apply to outbound SIP packets.

The settings for the session agent on the private enterprise side are shown below.

```
session-agent
    hostname                        rom2.bt.com
        ip-address                    192.168.1.186
        port                           5060
        state                          enabled
        app-protocol                  SIP
        app-type
        transport-method              UDP
        realm-id                       core-noas
        egress-realm-id
        description                   Avaya SM 6.0
        carriers

< text removed for brevity >

        response-map
        ping-method                     OPTIONS;hops=0
        ping-interval                 60
        ping-send-mode                  keep-alive

< text removed for brevity >

        in-manipulationid
        out-manipulationid            CoreNoasEgress
        manipulation-string

< text removed for brevity >
```

The settings for the session agent relating to BT SBC2 are shown below.

```
session-agent
        hostname                        xxx.yyy.5.58
        ip-address                      xxx.yyy.5.58
        port                            5060
        state                           enabled
        app-protocol                    SIP
        app-type
        transport-method                UDP
        realm-id                        access-noas
        egress-realm-id
        description                     NOAS SBC2
        carriers

< text removed for brevity >

        response-map
        ping-method                     OPTIONS;hops=66
        ping-interval                   60
        ping-send-mode                  keep-alive
        ping-in-service-response-codes  200-407,409-499,501-502,505-699
        out-service-response-codes

< text removed for brevity >

        li-trust-me                     disabled
        in-manipulationid               AccessNoasIngress
        out-manipulationid              AccessNoasEgress
        manipulation-string             NOASSBC2

< text removed for brevity >
```

7.9. Session Agent Group

Where multiple session agents exist, a session group is used to define a list of session agents and the hunting order for the defined session agents. Access the **session-group** element and set the following element parameters:

- **group-name:** A descriptive string used to reference the Session Agent Group (SAG).
- **app-protocol:** Set to **SIP.**
- **strategy:** Defines the method for hunting through the defined session agents, the default value is **Hunt.**
- **dest:** A list of the session agents available to the session agent group in priority order

For the purposes of these tests, the list contained a single session agent.

```
session-group
        group-name                      ACCESS-NOAS
        description                     NOAS SBC Hunt Group
        state                           enabled
        app-protocol                    SIP
        strategy                        Hunt
        dest
                                        192.168.5.62
        trunk-group
        sag-recursion                   enabled
        stop-sag-recurse                404,422-423,480,484,486,505-599
        last-modified-by                admin@192.168.1.6
        last-modified-date              2010-09-14 15:49:08
```

7.10. SIP Manipulation

SIP manipulations are rules used to modify the SIP messages during the compliance test. Three sip manipulations were used. These were assigned to session agents in **Section 7.8**. Multiple header rules can exist for each sip manipulation. Only the first sip manipulation and first header rule within that sip manipulation will be discussed in this section, the additional header rules and additional sip manipulations can be observed in **Appendix B.** Access the **sip-manipulation** element and set the following element parameters:

- **name**: A descriptive string used to reference the sip manipulation.
- **header-rule**:
  - **name**: The name of this individual header rule.
  - **header-name**: The SIP header to be modified.
  - **action**: The action to be performed on the header.
  - **comparison-type**: The type of comparison performed when determining a match.
  - **msg-type**: The type of message to which this rule applies.
  - **element-rule**:
    - **name:** The name of this individual element rule.
    - **type:** Defines the particular element in the header to be modified.
    - **action:** The action to be performed on the element.
    - **match-val-type**: The type of value to be matched. If the default value of **any** is used then the sip message is compared with the **match value** field.
    - **comparison-type**: The type of comparison performed when determining a match.
    - **match-value**: The value to be matched.
    - **new-value**: The new value to be used .

In the example below the sip manipulation **AccessNoasEgress** is shown, the first header rule called **ModFrom** specifies the From header in SIP request messages will be manipulated based on the element rule defined. The element rule called **AcmeNatFromHost** specifies that the host part of the URI in the From header should be replaced with the value $LOCAL_IP. The value $LOCAL_IP is the IP address of the SIP interface that message is being sent from.

```
sip-manipulation
        name                            AccessNoasEgress
        description                     Access NOAS Egress HMR
        header-rule
                name                            ModFrom
                header-name                     From
                action                          manipulate
                comparison-type                 case-sensitive
                match-value
                msg-type                        any
                new-value
                methods
                element-rule
                        name                            AcmeNatFromHost
                        parameter-name
                        type                            uri-host
                        action                          replace
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value
                        new-value                       $LOCAL_IP

< text removed for brevity >
```

7.11. Steering Pools

Steering pools define the range of ports to be used for the RTP voice stream. Two steering pools are defined; one for each realm. Access the **media-manager → steering-pool** element and set the following element parameters:

- **ip-address:** The address of the interface on the Acme Packet 4500 SBC.
- **start-port:** The number of the port that begins the range.
- **end-port:** The number of the port that ends the range.
- **realm-id:** The realm to which this steering pool is assigned.

```
steering-pool
        ip-address                      192.168.4.9
        start-port                      49152
        end-port                        65535
        realm-id                        access-noas
        network-interface
        last-modified-by                admin@192.168.1.6
        last-modified-date              2010-09-08 11:57:15
steering-pool
        ip-address                      192.168.3.9
        start-port                      49152
        end-port                        65535
        realm-id                        core-noas
        network-interface
        last-modified-by                admin@console
        last-modified-date              2010-09-07 15:28:21
```

7.12. Local Policy

Local policy controls the routing of SIP calls from one realm to another. Access the **session-router → local-policy** element and set the following element parameters:

- **from-address**: The originating IP address to which this policy applies. An asterisk * indicates any IP address.
- **to-address**: The destination IP address to which this policy applies. An asterisk * indicates any IP address.
- **source-realm**: The realm from which traffic is received.
- **policy-attribute**:
  - **next-hop**: The session agent or session agent group where the message should be sent when the policy rules match.
  - **realm**: The egress realm associated with the next-hop.

The settings for the first local-policy are shown below. The first policy indicates that messages originating from the **core-noas** realm are to be sent to the **access-noas** realm using the SAG defined in **Section 7.9**.

```
local-policy
        from-address
                                        *
        to-address
                                        *
        source-realm
                                        core-noas
        description                     Avaya To NOAS SAG
        activate-time                   N/A
        deactivate-time                 N/A
        state                           enabled
        policy-priority                 none
        last-modified-by                admin@console
        last-modified-date              2010-06-28 12:56:52
        policy-attribute
                next-hop                        SAG:ACCESS-NOAS
                realm                           access-noas
                action                          replace-uri

< text removed for brevity >
```

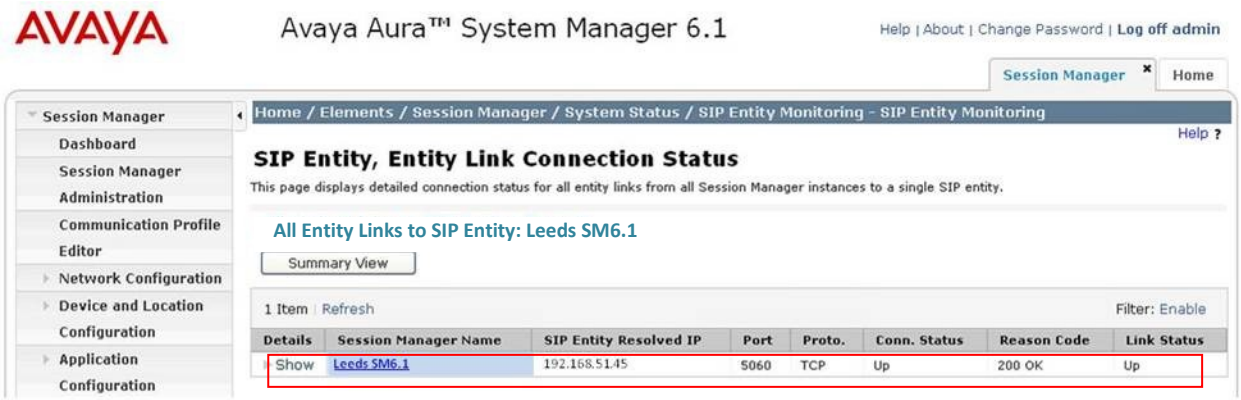
Settings for the second local-policy are shown below. This policy indicates that messages originating from the **access-noas** realm are to be sent to the **core-noas** realm using IP address 192.168.1.186. This concludes the Acme Packet 4500 SBC configuration steps.

```
local-policy
        from-address                            *
        to-address                              *
        source-realm                            access-noas
        description                             NOAS SAG To Avaya
        activate-time                           N/A
        deactivate-time                         N/A
        state                                   enabled
        policy-priority                         none
        last-modified-by                        admin@192.168.1.6
        last-modified-date                      2011-02-03 17:26:35
        policy-attribute
                next-hop                        192.168.1.186
                realm                           core-noas
                action                          none

< text removed for brevity >
```

8. Verification Steps

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

1. From System Manager **Home** Tab (see **Section 6.1**), click on **Session Manager** and navigate to **Session Manager → System Status → SIP Entity Monitoring**. Select the relevant SIP Entity from the list and observe if the **Conn Status** and **Link Status** are showing as up. See the following for an example.



2. From the Communication Server 1000E system 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.

9. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Communication Server 1000E and Avaya Aura® Session Manager to BT SIP Trunk Service via an Acme Packet Net-Net 4500 Session Border Controller. 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.

10. 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, June 2010.

[2] *Administering Avaya Aura® System Platform*, Release 6, June 2010.

[3] Avaya *Communication Server 1000E Installation and Commissioning*, November 2010, Document Number NN43041-310.

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

[5] *Installing and Upgrading Avaya Aura® System Manager Release 6.1*, November 2010.

[6] *Installing and Configuring Avaya Aura® Session Manager*, January 2011, Document Number 03-603473

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

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

Appendix A – Avaya Communication Server 1000E Software

Avaya Communication Server 1000E call server patches and plug_ins

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

VERSION 4021

System type is - Communication Server 1000E/CP PM
CP PM - Pentium M 1.4 GHz
IPMGs Registered:               4IPMGs Unregistered:             0IPMGs 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
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
```

Appendix B – Acme Packet Net-Net 4500 SBC Configuration

Acme Packet Net-Net 4500 SBC Configuration File

```
show running-config
access-control
       realm-id                        core-noas
       description                     Avaya To NOAS SAG
       source-address                  0.0.0.0
       destination-address             192.168.130.96:22
       application-protocol            NONE
       transport-protocol              ALL
       access                          permit
       average-rate-limit              0
       trust-level                     high
       minimum-reserved-bandwidth      0
       invalid-signal-threshold        1
       maximum-signal-threshold        12000
       untrusted-signal-threshold      0
       nat-trust-threshold             0
       deny-period                     30
       last-modified-by                admin@console
       last-modified-date              2010-09-07 15:58:33
access-control
       realm-id                        core-noas
       description                     ACL for Avaya devices in the core side
       source-address                  192.168.131.183
       destination-address             192.168.130.96:5060
       application-protocol            SIP
       transport-protocol              UDP
       access                          permit
       average-rate-limit              0
       trust-level                     high
       minimum-reserved-bandwidth      0
       invalid-signal-threshold        1
       maximum-signal-threshold        12000
       untrusted-signal-threshold      0
       nat-trust-threshold             0
       deny-period                     30
       last-modified-by                admin@192.168.131.105
       last-modified-date              2011-02-09 11:37:53
access-control
       realm-id                        core-noas
       description                     ACL for Avaya devices in the core side
       source-address                  192.168.131.186
       destination-address             192.168.130.96:5060
       application-protocol            SIP
       transport-protocol              UDP
       access                          permit
       average-rate-limit              0
       trust-level                     high
       minimum-reserved-bandwidth      0
       invalid-signal-threshold        1
       maximum-signal-threshold        12000
       untrusted-signal-threshold      0
       nat-trust-threshold             0
       deny-period                     30
       last-modified-by                admin@192.168.131.105
       last-modified-date              2011-02-09 11:38:46
access-control
       realm-id                        access-noas
       description                     ACL for NOAS SBCs
       source-address                  xxx.yyy.149.62
       destination-address             192.168.131.133:5060
       application-protocol            SIP
       transport-protocol              UDP
       access                          permit
```

```
        average-rate-limit              0
        trust-level                     medium
        minimum-reserved-bandwidth      0
        invalid-signal-threshold        1
        maximum-signal-threshold        12000
        untrusted-signal-threshold      4
        nat-trust-threshold             0
        deny-period                     30
        last-modified-by                admin@192.168.131.105
        last-modified-date              2011-02-09 10:59:37
access-control
        realm-id                        access-noas
        description                     ACL for NOAS SBCs
        source-address                  xxx.yyy.149.58
        destination-address             192.168.131.133:5060
        application-protocol            SIP
        transport-protocol              UDP
        access                          permit
        average-rate-limit              0
        trust-level                     medium
        minimum-reserved-bandwidth      0
        invalid-signal-threshold        1
        maximum-signal-threshold        12000
        untrusted-signal-threshold      4
        nat-trust-threshold             0
        deny-period                     30
        last-modified-by                admin@192.168.131.105
        last-modified-date              2011-02-09 11:02:46
access-control
        realm-id                        access-noas
        description                     ACL for NOAS SBCs
        source-address                  xxx.yyy.149.54
        destination-address             192.168.131.133:5060
        application-protocol            SIP
        transport-protocol              UDP
        access                          permit
        average-rate-limit              0
        trust-level                     medium
        minimum-reserved-bandwidth      0
        invalid-signal-threshold        1
        maximum-signal-threshold        12000
        untrusted-signal-threshold      4
        nat-trust-threshold             0
        deny-period                     30
        last-modified-by                admin@192.168.131.105
        last-modified-date              2011-02-09 11:05:13
access-control
        realm-id                        access-noas
        description                     ACL for NOAS SBCs
        source-address                  xxx.yyy.149.50
        destination-address             192.168.131.133:5060
        application-protocol            SIP
        transport-protocol              UDP
        access                          permit
        average-rate-limit              0
        trust-level                     medium
        minimum-reserved-bandwidth      0
        invalid-signal-threshold        1
        maximum-signal-threshold        12000
        untrusted-signal-threshold      4
        nat-trust-threshold             0
        deny-period                     30
        last-modified-by                admin@192.168.131.105
        last-modified-date              2011-02-09 11:36:00
capture-receiver
        state                           enabled
        address                         192.168.51.48
        network-interface               M00:0
        last-modified-by                admin@192.168.50.131
        last-modified-date              2011-04-08 10:33:18
```

```
local-policy
       from-address
                                    *
       to-address
                                    *
       source-realm
                                    core-noas
       description                  Avaya To NOAS SAG
       activate-time                N/A
       deactivate-time              N/A
       state                        enabled
       policy-priority              none
       last-modified-by             admin@10.16.48.45
       last-modified-date           2010-06-28 12:56:52
       policy-attribute
              next-hop                      SAG:ACCESS-NOAS
              realm                         access-noas
              action                        replace-uri
              terminate-recursion           enabled
              carrier
              start-time                    0000
              end-time                      2400
              days-of-week                  U-S
              cost                          0
              app-protocol                  SIP
              state                         enabled
              methods
              media-profiles
local-policy
       from-address
                                    *
       to-address
                                    *
       source-realm
                                    access-noas
       description                  NOAS SAG To Avaya
       activate-time                N/A
       deactivate-time              N/A
       state                        enabled
       policy-priority              none
       last-modified-by             admin@192.168.131.60
       last-modified-date           2011-02-03 17:26:35
       policy-attribute
              next-hop                      192.168.131.186
              realm                         core-noas
              action                        none
              terminate-recursion           enabled
              carrier
              start-time                    0000
              end-time                      2400
              days-of-week                  U-S
              cost                          0
              app-protocol                  SIP
              state                         enabled
              methods
              media-profiles
media-manager
       state                        enabled
       latching                     enabled
       flow-time-limit              86400
       initial-guard-timer          300
       subsq-guard-timer            300
       tcp-flow-time-limit          86400
       tcp-initial-guard-timer      300
       tcp-subsq-guard-timer        300
       tcp-number-of-ports-per-flow 2
       hnt-rtcp                     disabled
       algd-log-level               NOTICE
       mbcd-log-level               NOTICE
       options                      active-arp
```

```
        red-flow-port                   1985
        red-mgcp-port                   0
        red-max-trans                   10000
        red-sync-start-time             5000
        red-sync-comp-time              1000
        media-policing                  enabled
        max-signaling-bandwidth         775880
        max-untrusted-signaling         1
        min-untrusted-signaling         1
        app-signaling-bandwidth         0
        tolerance-window                30
        rtcp-rate-limit                 0
        min-media-allocation            2000
        min-trusted-allocation          4000
        deny-allocation                 64000
        anonymous-sdp                   disabled
        arp-msg-bandwidth               32000
        fragment-msg-bandwidth          0
        rfc2833-timestamp               disabled
        default-2833-duration           100
        rfc2833-end-pkts-only-for-non-sig enabled
        translate-non-rfc2833-event     disabled
        dnsalg-server-failover          disabled
        last-modified-by                admin@192.168.131.105
        last-modified-date              2011-02-09 11:46:23
network-interface
        name                            wancom1
        sub-port-id                     0
        description
        hostname
        ip-address
        pri-utility-addr                xxx.yyy.1.1
        sec-utility-addr                xxx.yyy.1.2
        netmask                         255.255.255.252
        gateway
        sec-gateway
        gw-heartbeat
                state                           disabled
                heartbeat                       0
                retry-count                     0
                retry-timeout                   1
                health-score                    0
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                     11
         hip-ip-list
        ftp-address
         icmp-address
        snmp-address
        telnet-address
        last-modified-by                admin@console
        last-modified-date              2010-09-07 15:00:12
network-interface
        name                            wancom2
        sub-port-id                     0
        description
        hostname
        ip-address
        pri-utility-addr                xxx.yyy.2.1
        sec-utility-addr                xxx.yyy.2.2
        netmask                         255.255.255.252
        gateway
        sec-gateway
        gw-heartbeat
                state                           disabled
                heartbeat                       0
                retry-count                     0
                retry-timeout                   1
```

```
                health-score                    0
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                     11
         hip-ip-list
        ftp-address
         icmp-address
        snmp-address
        telnet-address
        last-modified-by                admin@console
        last-modified-date              2010-09-07 15:00:12
network-interface
        name                            M10
        sub-port-id                     0
        description                     Facing Avaya
        hostname
        ip-address                      192.168.130.96
        pri-utility-addr                192.168.130.170
        sec-utility-addr                192.168.130.171
        netmask                         255.255.255.0
        gateway                         192.168.130.1
        sec-gateway
        gw-heartbeat
                state                           disabled
                heartbeat                       0
                retry-count                     0
                retry-timeout                   1
                health-score                    32
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                     11
         hip-ip-list                     192.168.130.96
        ftp-address
         icmp-address                    192.168.130.96
        snmp-address
        telnet-address
        last-modified-by                admin@192.168.131.60
        last-modified-date              2010-09-08 14:18:22
network-interface
        name                            M00
        sub-port-id                     0
        description                     Facing Noas
        hostname
        ip-address                      192.168.131.133
        pri-utility-addr                192.168.131.130
        sec-utility-addr                192.168.131.132
        netmask                         255.255.255.0
        gateway                         192.168.131.1
        sec-gateway
        gw-heartbeat
                state                           enabled
                heartbeat                       10
                retry-count                     3
                retry-timeout                   3
                health-score                    30
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                     11
         hip-ip-list                     192.168.131.133
        ftp-address
         icmp-address                    192.168.131.133
        snmp-address
        telnet-address
        last-modified-by                admin@192.168.131.60
```

```
        last-modified-date              2010-09-08 12:11:55
ntp-config
        last-modified-by                admin@192.168.131.60
        last-modified-date              2010-09-22 15:06:51
phy-interface
        name                            wancom1
        operation-type                  Control
        port                            1
        slot                            0
        virtual-mac
        wancom-health-score             8
        last-modified-by                admin@console
        last-modified-date              2010-09-07 15:00:12
phy-interface
        name                            wancom2
        operation-type                  Control
        port                            2
        slot                            0
        virtual-mac
        wancom-health-score             9
        last-modified-by                admin@console
        last-modified-date              2010-09-07 15:00:12
phy-interface
        name                            M10
        operation-type                  Media
        port                            0
        slot                            1
        virtual-mac                     00:08:25:a1:90:0E
        admin-state                     enabled
        auto-negotiation                enabled
        duplex-mode                     FULL
        speed                           100
        last-modified-by                admin@console
        last-modified-date              2010-09-07 15:15:33
phy-interface
        name                            M00
        operation-type                  Media
        port                            0
        slot                            0
        virtual-mac                     00:08:25:a1:8f:4E
        admin-state                     enabled
        auto-negotiation                enabled
        duplex-mode                     FULL
        speed                           100
        last-modified-by                admin@console
        last-modified-date              2010-09-07 15:15:49
realm-config
        identifier                      access-noas
        description                     Access Realm for NOAS SAG
        addr-prefix                     0.0.0.0
        network-interfaces
                                        M00:0
        mm-in-realm                     disabled
        mm-in-network                   enabled
        mm-same-ip                      enabled
        mm-in-system                    enabled
        bw-cac-non-mm                   disabled
        msm-release                     disabled
        qos-enable                      disabled
        generate-UDP-checksum           disabled
        max-bandwidth                   0
        fallback-bandwidth              0
        max-priority-bandwidth          0
        max-latency                     0
        max-jitter                      0
        max-packet-loss                 0
        observ-window-size              0
        parent-realm
        dns-realm
        media-policy
```

```
        in-translationid
        out-translationid
        in-manipulationid
        out-manipulationid
        manipulation-string
        class-profile
        average-rate-limit              0
        access-control-trust-level      medium
        invalid-signal-threshold        1
        maximum-signal-threshold        1
        untrusted-signal-threshold      1
        nat-trust-threshold             0
        deny-period                     60
        ext-policy-svr
        symmetric-latching              disabled
        pai-strip                       disabled
        trunk-context
        early-media-allow
        enforcement-profile
        additional-prefixes
        restricted-latching             none
        restriction-mask                32
        accounting-enable               enabled
        user-cac-mode                   none
        user-cac-bandwidth              0
        user-cac-sessions               0
        icmp-detect-multiplier          0
        icmp-advertisement-interval     0
        icmp-target-ip
        monthly-minutes                 0
        net-management-control          disabled
        delay-media-update              disabled
        refer-call-transfer             disabled
        codec-policy
        codec-manip-in-realm            disabled
        constraint-name
        call-recording-server-id
        stun-enable                     disabled
        stun-server-ip                  0.0.0.0
        stun-server-port                3478
        stun-changed-ip                 0.0.0.0
        stun-changed-port               3479
        match-media-profiles
        qos-constraint
        last-modified-by                admin@192.168.131.105
        last-modified-date              2011-02-09 11:42:10
realm-config
        identifier                      core-noas
        description                     Core Realm calls from NOAS SAG to AVAYA
        addr-prefix                     0.0.0.0
        network-interfaces
                                        M10:0
        mm-in-realm                     disabled
        mm-in-network                   enabled
        mm-same-ip                      enabled
        mm-in-system                    enabled
        bw-cac-non-mm                   disabled
        msm-release                     disabled
        qos-enable                      disabled
        generate-UDP-checksum           disabled
        max-bandwidth                   0
        fallback-bandwidth              0
        max-priority-bandwidth          0
        max-latency                     0
        max-jitter                      0
        max-packet-loss                 0
        observ-window-size              0
        parent-realm
        dns-realm
        media-policy
```

```
        in-translationid
        out-translationid
        in-manipulationid
        out-manipulationid
        manipulation-string
        class-profile
        average-rate-limit              0
        access-control-trust-level      high
        invalid-signal-threshold        1
        maximum-signal-threshold        1
        untrusted-signal-threshold      0
        nat-trust-threshold             0
        deny-period                     60
        ext-policy-svr
        symmetric-latching              disabled
        pai-strip                       disabled
        trunk-context
        early-media-allow
        enforcement-profile
        additional-prefixes
        restricted-latching             none
        restriction-mask                32
        accounting-enable               enabled
        user-cac-mode                   none
        user-cac-bandwidth              0
        user-cac-sessions               0
        icmp-detect-multiplier          0
        icmp-advertisement-interval     0
        icmp-target-ip
        monthly-minutes                 0
        net-management-control          disabled
        delay-media-update              disabled
        refer-call-transfer             disabled
        codec-policy
        codec-manip-in-realm            disabled
        constraint-name
        call-recording-server-id
        stun-enable                     disabled
        stun-server-ip                  0.0.0.0
        stun-server-port                3478
        stun-changed-ip                 0.0.0.0
        stun-changed-port               3479
        match-media-profiles
        qos-constraint
        last-modified-by                admin@192.168.131.105
        last-modified-date              2011-02-09 12:35:58
redundancy-config
        state                           enabled
        log-level                       INFO
        health-threshold                75
        emergency-threshold             50
        port                            9090
        advertisement-time              500
        percent-drift                   210
        initial-time                    1250
        becoming-standby-time           180000
        becoming-active-time            100
        cfg-port                        1987
        cfg-max-trans                   10000
        cfg-sync-start-time             5000
        cfg-sync-comp-time              1000
        gateway-heartbeat-interval      0
        gateway-heartbeat-retry         0
        gateway-heartbeat-timeout       1
        gateway-heartbeat-health        0
        media-if-peercheck-time         0
        peer
                name                            SBC1
                state                           enabled
                type                            Primary
```

```
                destination
                       address                         xxx.yyy.1.1:9090
                       network-interface               wancom1:0
                destination
                       address                         xxx.yyy.2.1:9090
                       network-interface               wancom2:0
        peer
                name                            SBC2
                state                           enabled
                type                            Secondary
                destination
                       address                         xxx.yyy.1.2:9090
                       network-interface               wancom1:0
                destination
                       address                         xxx.yyy.2.2:9090
                       network-interface               wancom2:0
        last-modified-by                admin@console
        last-modified-date              2010-09-07 15:00:12
session-agent
        hostname                        192.168.131.183
        ip-address                      192.168.131.183
        port                            5060
        state                           enabled
        app-protocol                    SIP
        app-type
        transport-method                UDP
        realm-id                        core-noas
        egress-realm-id
        description                     Avaya SIP Port For NOAS SAG
        carriers
        allow-next-hop-lp               enabled
        constraints                     disabled
        max-sessions                    0
        max-inbound-sessions            0
        max-outbound-sessions           0
        max-burst-rate                  0
        max-inbound-burst-rate          0
        max-outbound-burst-rate         0
        max-sustain-rate                0
        max-inbound-sustain-rate        0
        max-outbound-sustain-rate       0
        min-seizures                    5
        min-asr                         0
        time-to-resume                  0
        ttr-no-response                 0
        in-service-period               0
        burst-rate-window               0
        sustain-rate-window             0
        req-uri-carrier-mode            None
        proxy-mode
        redirect-action
        loose-routing                   enabled
        send-media-session              enabled
        response-map
        ping-method                     OPTIONS;hops=0
        ping-interval                   60
        ping-send-mode                  keep-alive
        ping-in-service-response-codes
        out-service-response-codes
        media-profiles
        in-translationid
        out-translationid
        trust-me                        disabled
        request-uri-headers
        stop-recurse
        local-response-map
        ping-to-user-part
        ping-from-user-part
        li-trust-me                     disabled
        in-manipulationid
```

```
        out-manipulationid              CoreNoasEgress
        manipulation-string
        p-asserted-id
        trunk-group
        max-register-sustain-rate       0
        early-media-allow
        invalidate-registrations        disabled
        rfc2833-mode                    none
        rfc2833-payload                 0
        codec-policy
        enforcement-profile
        refer-call-transfer             disabled
        reuse-connections               TCP
        tcp-keepalive                   none
        tcp-reconn-interval             0
        max-register-burst-rate         0
        register-burst-window           0
        last-modified-by                admin@192.168.131.60
        last-modified-date              2010-09-14 18:14:20
session-agent
        hostname                        xxx.yyy.149.62
        ip-address                      xxx.yyy.149.62
        port                            5060
        state                           enabled
        app-protocol                    SIP
        app-type
        transport-method                UDP
        realm-id                        access-noas
        egress-realm-id
        description                     NOAS SBC1
        carriers
        allow-next-hop-lp               enabled
        constraints                     disabled
        max-sessions                    0
        max-inbound-sessions            0
        max-outbound-sessions           0
        max-burst-rate                  0
        max-inbound-burst-rate          0
        max-outbound-burst-rate         0
        max-sustain-rate                0
        max-inbound-sustain-rate        0
        max-outbound-sustain-rate       0
        min-seizures                    5
        min-asr                         0
        time-to-resume                  0
        ttr-no-response                 0
        in-service-period               0
        burst-rate-window               0
        sustain-rate-window             0
        req-uri-carrier-mode            None
        proxy-mode
        redirect-action
        loose-routing                   enabled
        send-media-session              enabled
        response-map
        ping-method                     OPTIONS;hops=66
        ping-interval                   60
        ping-send-mode                  keep-alive
        ping-in-service-response-codes 200-407,409-499,501-502,505-699
        out-service-response-codes
        options                         trans-timeouts=2
        media-profiles
        in-translationid
        out-translationid
        trust-me                        disabled
        request-uri-headers
        stop-recurse
        local-response-map
        ping-to-user-part
        ping-from-user-part
```

```
        li-trust-me                     disabled
        in-manipulationid               AccessNoasIngress
        out-manipulationid              AccessNoasEgress
        manipulation-string             NOASSBC1
        p-asserted-id
        trunk-group
        max-register-sustain-rate       0
        early-media-allow
        invalidate-registrations        disabled
        rfc2833-mode                    none
        rfc2833-payload                 0
        codec-policy
        enforcement-profile
        refer-call-transfer             disabled
        reuse-connections               NONE
        tcp-keepalive                   none
        tcp-reconn-interval             0
        max-register-burst-rate         0
        register-burst-window           0
        last-modified-by                admin@console
        last-modified-date              2010-09-07 15:43:06
session-agent
        hostname                        xxx.yyy.149.58
        ip-address                      xxx.yyy.149.58
        port                            5060
        state                           enabled
        app-protocol                    SIP
        app-type
        transport-method                UDP
        realm-id                        access-noas
        egress-realm-id
        description                     NOAS SBC2
        carriers
        allow-next-hop-lp               enabled
        constraints                     disabled
        max-sessions                    0
        max-inbound-sessions            0
        max-outbound-sessions           0
        max-burst-rate                  0
        max-inbound-burst-rate          0
        max-outbound-burst-rate         0
        max-sustain-rate                0
        max-inbound-sustain-rate        0
        max-outbound-sustain-rate       0
        min-seizures                    5
        min-asr                         0
        time-to-resume                  0
        ttr-no-response                 0
        in-service-period               0
        burst-rate-window               0
        sustain-rate-window             0
        req-uri-carrier-mode            None
        proxy-mode
        redirect-action
        loose-routing                   enabled
        send-media-session              enabled
        response-map
        ping-method                     OPTIONS;hops=66
        ping-interval                   60
        ping-send-mode                  keep-alive
        ping-in-service-response-codes  200-407,409-499,501-502,505-699
        out-service-response-codes
        options                         trans-timeouts=2
        media-profiles
        in-translationid
        out-translationid
        trust-me                        disabled
        request-uri-headers
        stop-recurse
        local-response-map
```

```
        ping-to-user-part
        ping-from-user-part
        li-trust-me                     disabled
        in-manipulationid               AccessNoasIngress
        out-manipulationid              AccessNoasEgress
        manipulation-string             NOASSBC2
        p-asserted-id
        trunk-group
        max-register-sustain-rate       0
        early-media-allow
        invalidate-registrations        disabled
        rfc2833-mode                    none
        rfc2833-payload                 0
        codec-policy
        enforcement-profile
        refer-call-transfer             disabled
        reuse-connections               NONE
        tcp-keepalive                   none
        tcp-reconn-interval             0
        max-register-burst-rate         0
        register-burst-window           0
        last-modified-by                admin@192.168.131.60
        last-modified-date              2010-09-08 11:51:38
session-agent
        hostname                        xxx.yyy.149.54
        ip-address                      xxx.yyy.149.54
        port                            5060
        state                           enabled
        app-protocol                    SIP
        app-type
        transport-method                UDP
        realm-id                        access-noas
        egress-realm-id
        description                     NOAS SBC3
        carriers
        allow-next-hop-lp               enabled
        constraints                     disabled
        max-sessions                    0
        max-inbound-sessions            0
        max-outbound-sessions           0
        max-burst-rate                  0
        max-inbound-burst-rate          0
        max-outbound-burst-rate         0
        max-sustain-rate                0
        max-inbound-sustain-rate        0
        max-outbound-sustain-rate       0
        min-seizures                    5
        min-asr                         0
        time-to-resume                  0
        ttr-no-response                 0
        in-service-period               0
        burst-rate-window               0
        sustain-rate-window             0
        req-uri-carrier-mode            None
        proxy-mode
        redirect-action
        loose-routing                   enabled
        send-media-session              enabled
        response-map
        ping-method                     OPTIONS;hops=66
        ping-interval                   60
        ping-send-mode                  keep-alive
        ping-in-service-response-codes 200-407,409-499,501-502,505-699
        out-service-response-codes
        options                         trans-timeouts=2
        media-profiles
        in-translationid
        out-translationid
        trust-me                        disabled
        request-uri-headers
```

```
        stop-recurse
        local-response-map
        ping-to-user-part
        ping-from-user-part
        li-trust-me                     disabled
        in-manipulationid               AccessNoasIngress
        out-manipulationid              AccessNoasEgress
        manipulation-string             NOASSBC3
        p-asserted-id
        trunk-group
        max-register-sustain-rate       0
        early-media-allow
        invalidate-registrations        disabled
        rfc2833-mode                    none
        rfc2833-payload                 0
        codec-policy
        enforcement-profile
        refer-call-transfer             disabled
        reuse-connections               NONE
        tcp-keepalive                   none
        tcp-reconn-interval             0
        max-register-burst-rate         0
        register-burst-window           0
        last-modified-by                admin@192.168.131.60
        last-modified-date              2010-09-08 11:52:41
session-agent
        hostname                        xxx.yyy.149.50
        ip-address                      xxx.yyy.149.50
        port                            5060
        state                           enabled
        app-protocol                    SIP
        app-type
        transport-method                UDP
        realm-id                        access-noas
        egress-realm-id
        description                     NOAS SBC4
        carriers
        allow-next-hop-lp               enabled
        constraints                     disabled
        max-sessions                    0
        max-inbound-sessions            0
        max-outbound-sessions           0
        max-burst-rate                  0
        max-inbound-burst-rate          0
        max-outbound-burst-rate         0
        max-sustain-rate                0
        max-inbound-sustain-rate        0
        max-outbound-sustain-rate       0
        min-seizures                    5
        min-asr                         0
        time-to-resume                  0
        ttr-no-response                 0
        in-service-period               0
        burst-rate-window               0
        sustain-rate-window             0
        req-uri-carrier-mode            None
        proxy-mode
        redirect-action
        loose-routing                   enabled
        send-media-session              enabled
        response-map
        ping-method                     OPTIONS;hops=66
        ping-interval                   60
        ping-send-mode                  keep-alive
        ping-in-service-response-codes 200-407,409-499,501-502,505-699
        out-service-response-codes
        options                         trans-timeouts=2
        media-profiles
        in-translationid
        out-translationid
```

```
        trust-me                        disabled
        request-uri-headers
        stop-recurse
        local-response-map
        ping-to-user-part
        ping-from-user-part
        li-trust-me                     disabled
        in-manipulationid               AccessNoasIngress
        out-manipulationid              AccessNoasEgress
        manipulation-string             NOASSBC4
        p-asserted-id
        trunk-group
        max-register-sustain-rate       0
        early-media-allow
        invalidate-registrations        disabled
        rfc2833-mode                    none
        rfc2833-payload                 0
        codec-policy
        enforcement-profile
        refer-call-transfer             disabled
        reuse-connections               NONE
        tcp-keepalive                   none
        tcp-reconn-interval             0
        max-register-burst-rate         0
        register-burst-window           0
        last-modified-by                admin@192.168.131.60
        last-modified-date              2010-09-14 15:46:00
session-agent
        hostname                        rom2.bt.com
        ip-address                      192.168.131.186
        port                            5060
        state                           enabled
        app-protocol                    SIP
        app-type
        transport-method                UDP
        realm-id                        core-noas
        egress-realm-id
        description                     Avaya SM 6.0
        carriers
        allow-next-hop-lp               enabled
        constraints                     disabled
        max-sessions                    0
        max-inbound-sessions            0
        max-outbound-sessions           0
        max-burst-rate                  0
        max-inbound-burst-rate          0
        max-outbound-burst-rate         0
        max-sustain-rate                0
        max-inbound-sustain-rate        0
        max-outbound-sustain-rate       0
        min-seizures                    5
        min-asr                         0
        time-to-resume                  0
        ttr-no-response                 0
        in-service-period               0
        burst-rate-window               0
        sustain-rate-window             0
        req-uri-carrier-mode            None
        proxy-mode
        redirect-action
        loose-routing                   enabled
        send-media-session              enabled
        response-map
        ping-method                     OPTIONS;hops=0
        ping-interval                   60
        ping-send-mode                  keep-alive
        ping-in-service-response-codes
        out-service-response-codes
        media-profiles
        in-translationid
```

```
        out-translationid
        trust-me                        disabled
        request-uri-headers
        stop-recurse
        local-response-map
        ping-to-user-part
        ping-from-user-part
        li-trust-me                     disabled
        in-manipulationid
        out-manipulationid              CoreNoasEgress
        manipulation-string
        p-asserted-id
        trunk-group
        max-register-sustain-rate       0
        early-media-allow
        invalidate-registrations        disabled
        rfc2833-mode                    none
        rfc2833-payload                 0
        codec-policy
        enforcement-profile
        refer-call-transfer             disabled
        reuse-connections               TCP
        tcp-keepalive                   none
        tcp-reconn-interval             0
        max-register-burst-rate         0
        register-burst-window           0
        last-modified-by                admin@192.168.131.105
        last-modified-date              2011-02-09 12:32:21
session-group
        group-name                      ACCESS-NOAS
        description                     NOAS SBC Hunt Group
        state                           enabled
        app-protocol                    SIP
        strategy                        Hunt
        dest
                                        xxx.yyy.149.62
                                        xxx.yyy.149.58
                                        xxx.yyy.149.54
                                        xxx.yyy.149.50
        trunk-group
        sag-recursion                   enabled
        stop-sag-recurse                404,422-423,480,484,486,505-599
        last-modified-by                admin@192.168.131.60
        last-modified-date              2010-09-14 15:49:08
sip-config
        state                           enabled
        operation-mode                  dialog
        dialog-transparency             disabled
        home-realm-id                   core-noas
        egress-realm-id
        nat-mode                        Public
        registrar-domain                *
        registrar-host                  *
        registrar-port                  5060
        register-service-route          always
        init-timer                      500
        max-timer                       4000
        trans-expire                    32
        invite-expire                   180
        inactive-dynamic-conn           32
        enforcement-profile
        pac-method
        pac-interval                    10
        pac-strategy                    PropDist
        pac-load-weight                 1
        pac-session-weight              1
        pac-route-weight                1
        pac-callid-lifetime             600
        pac-user-lifetime               3600
        red-sip-port                    1988
```

```
        red-max-trans                   10000
        red-sync-start-time             5000
        red-sync-comp-time              1000
        add-reason-header               disabled
        sip-message-len                 4096
        enum-sag-match                  disabled
        extra-method-stats              disabled
        registration-cache-limit        0
        register-use-to-for-lp          disabled
        options                         max-udp-length=0
                                         set-inv-exp-at-100-resp
        add-ucid-header                 disabled
        proxy-sub-events
        last-modified-by                admin@192.168.131.60
        last-modified-date              2011-04-06 09:53:59
sip-interface
        state                           enabled
        realm-id                        core-noas
        description                     Core NOAS SAG SIP Interface
        sip-port
                address                         192.168.130.96
                port                            5060
                transport-protocol              UDP
                tls-profile
                allow-anonymous                 agents-only
                ims-aka-profile
        carriers
        trans-expire                    4
        invite-expire                   185
        max-redirect-contacts           0
        proxy-mode
        redirect-action
        contact-mode                    none
        nat-traversal                   none
        nat-interval                    30
        tcp-nat-interval                90
        registration-caching            disabled
        min-reg-expire                  300
        registration-interval           3600
        route-to-registrar              disabled
        secured-network                 disabled
        teluri-scheme                   disabled
        uri-fqdn-domain
        options                         set-inv-exp-at-100-resp;max-udp-length=0
        trust-mode                      all
        max-nat-interval                3600
        nat-int-increment               10
        nat-test-increment              30
        sip-dynamic-hnt                 disabled
        stop-recurse                    401,407
        port-map-start                  0
        port-map-end                    0
        in-manipulationid
        out-manipulationid
        manipulation-string
        sip-ims-feature                 disabled
        operator-identifier
        anonymous-priority              none
        max-incoming-conns              0
        per-src-ip-max-incoming-conns   0
        inactive-conn-timeout           0
        untrusted-conn-timeout          0
        network-id
        ext-policy-server
        default-location-string
        charging-vector-mode            pass
        charging-function-address-mode  pass
        ccf-address
        ecf-address
        term-tgrp-mode                  none
```

```
        implicit-service-route         disabled
        rfc2833-payload                101
        rfc2833-mode                   transparent
        constraint-name
        response-map
        local-response-map
        ims-aka-feature                disabled
        enforcement-profile
        refer-call-transfer            disabled
        route-unauthorized-calls
        tcp-keepalive                  none
        add-sdp-invite                 disabled
        add-sdp-profiles
        last-modified-by               admin@192.168.50.131
        last-modified-date             2011-04-05 10:15:28
sip-interface
        state                          enabled
        realm-id                       access-noas
        description                    Interface
        sip-port
               address                         192.168.131.133
               port                            5060
               transport-protocol              UDP
               tls-profile
               allow-anonymous                 agents-only
               ims-aka-profile
        carriers
        trans-expire                   4
        invite-expire                  185
        max-redirect-contacts          0
        proxy-mode
        redirect-action
        contact-mode                   none
        nat-traversal                  none
        nat-interval                   30
        tcp-nat-interval               90
        registration-caching           disabled
        min-reg-expire                 300
        registration-interval          3600
        route-to-registrar             disabled
        secured-network                disabled
        teluri-scheme                  disabled
        uri-fqdn-domain
        trust-mode                     all
        max-nat-interval               3600
        nat-int-increment              10
        nat-test-increment             30
        sip-dynamic-hnt                disabled
        stop-recurse                   401,407
        port-map-start                 0
        port-map-end                   0
        in-manipulationid
        out-manipulationid
        manipulation-string
        sip-ims-feature                disabled
        operator-identifier
        anonymous-priority             none
        max-incoming-conns             0
        per-src-ip-max-incoming-conns  0
        inactive-conn-timeout          0
        untrusted-conn-timeout         0
        network-id
        ext-policy-server
        default-location-string
        charging-vector-mode           pass
        charging-function-address-mode pass
        ccf-address
        ecf-address
        term-tgrp-mode                 none
        implicit-service-route         disabled
```

```
        rfc2833-payload               101
        rfc2833-mode                  transparent
        constraint-name
        response-map
        local-response-map
        ims-aka-feature               disabled
        enforcement-profile
        refer-call-transfer           disabled
        route-unauthorized-calls
        tcp-keepalive                 none
        add-sdp-invite                disabled
        add-sdp-profiles
        last-modified-by              admin@192.168.131.60
        last-modified-date            2011-04-06 08:51:26
sip-manipulation
        name                          AccessNoasEgress
        description                   Access NOAS Egress HMR
        header-rule
                name                          ModFrom
                header-name                   From
                action                        manipulate
                comparison-type               case-sensitive
                match-value
                msg-type                      any
                new-value
                methods
                element-rule
                        name                          AcmeNatFromHost
                        parameter-name
                        type                          uri-host
                        action                        replace
                        match-val-type                any
                        comparison-type               case-sensitive
                        match-value
                        new-value                     $LOCAL_IP
        header-rule
                name                          ModTo
                header-name                   To
                action                        manipulate
                comparison-type               case-sensitive
                match-value
                msg-type                      any
                new-value
                methods
                element-rule
                        name                          AcmeNatToHost
                        parameter-name
                        type                          uri-host
                        action                        replace
                        match-val-type                any
                        comparison-type               case-sensitive
                        match-value
                        new-value                     $REMOTE_IP
        header-rule
                name                          ModAlertInfoHost
                header-name                   Alert-Info
                action                        find-replace-all
                comparison-type               pattern-rule
                match-value                   avaya.com
                msg-type                      any
                new-value                     $LOCAL_IP
                methods
        header-rule
                name                          ModPai
                header-name                   P-Asserted-Identity
                action                        manipulate
                comparison-type               case-sensitive
                match-value
                msg-type                      any
                new-value
```

```
               methods
               element-rule
                      name                            ModPaiHost
                      parameter-name
                      type                            uri-host
                      action                          replace
                      match-val-type                  any
                      comparison-type                 case-sensitive
                      match-value
                      new-value                       $LOCAL_IP
               element-rule
                      name                            ModPaiPort
                      parameter-name
                      type                            uri-port
                      action                          replace
                      match-val-type                  any
                      comparison-type                 case-sensitive
                      match-value
                      new-value                       $LOCAL PORT
       last-modified-by               admin@10.16.48.45
       last-modified-date             2010-06-28 18:32:02
sip-manipulation
       name                           ModAvayaUris
       description                    Modify R-URI, From & To Host Parts For Avaya
       header-rule
              name                                    ModRuri
              header-name                             request-uri
              action                                  manipulate
              comparison-type                         case-sensitive
              match-value
              msg-type                                any
              new-value
              methods
              element-rule
                      name                                    ModRuriHost
                      parameter-name
                      type                                    uri-host
                      action                                  replace
                      match-val-type                          any
                      comparison-type                         case-sensitive
                      match-value
                      new-value                               $REMOTE IP
       header-rule
              name                                    ModFrom
              header-name                             From
              action                                  manipulate
              comparison-type                         case-sensitive
              match-value
              msg-type                                any
              new-value
              methods
              element-rule
                      name                                    ModFromHost
                      parameter-name
                      type                                    uri-host
                      action                                  replace
                      match-val-type                          any
                      comparison-type                         case-sensitive
                      match-value
                      new-value                               $LOCAL IP
       header-rule
              name                                    ModTo
              header-name                             To
              action                                  manipulate
              comparison-type                         case-sensitive
              match-value
              msg-type                                any
              new-value
              methods
              element-rule
```

```
                        name                            ModToHost
                        parameter-name
                        type                            uri-host
                        action                          replace
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value
                        new-value                       $REMOTE IP
        last-modified-by                admin@192.168.131.60
        last-modified-date              2010-09-14 17:35:29
sip-manipulation
        name                            CoreNoasEgress
        description                     Core NOAS Egress HMR
        header-rule
                name                            CallModAvayaUris
                header-name                     From
                action                          sip-manip
                comparison-type                 case-sensitive
                match-value
                msg-type                        any
                new-value                       ModAvayaUris
                methods
        header-rule
                name                            ModFrom
                header-name                     From
                action                          manipulate
                comparison-type                 case-sensitive
                match-value
                msg-type                        any
                new-value
                methods
                element-rule
                        name                            ModFromPort
                        parameter-name
                        type                            uri-port
                        action                          replace
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value
                        new-value                       $LOCAL_PORT
        header-rule
                name                            ModTo
                header-name                     To
                action                          manipulate
                comparison-type                 case-sensitive
                match-value
                msg-type                        any
                new-value
                methods
                element-rule
                        name                            ModToPort
                        parameter-name
                        type                            uri-port
                        action                          replace
                        match-val-type                  any
                        comparison-type                 case-sensitive
                        match-value
                        new-value                       $REMOTE_PORT
        last-modified-by                admin@10.16.48.45
        last-modified-date              2010-06-29 08:09:15
sip-manipulation
        name                            AccessNoasIngress
        description                     Access NOAS Ingress HMR
        header-rule
                name                            AddUserAgentToOptions
                header-name                     User-Agent
                action                          add
                comparison-type                 case-sensitive
                match-value
                msg-type                        reply
```

```
               new-value                       $MANIP_STRING
               methods                         OPTIONS
       last-modified-by              admin@192.168.160.135
       last-modified-date            2010-09-29 17:24:08
steering-pool
       ip-address                    192.168.131.133
       start-port                    49152
       end-port                      65535
       realm-id                      access-noas
       network-interface
       last-modified-by              admin@192.168.131.60
       last-modified-date            2010-09-08 11:57:15
steering-pool
       ip-address                    192.168.130.96
       start-port                    49152
       end-port                      65535
       realm-id                      core-noas
       network-interface
       last-modified-by              admin@console
       last-modified-date            2010-09-07 15:28:21
system-config
       hostname
       description
       location
       mib-system-contact
       mib-system-name
       mib-system-location
       snmp-enabled                  enabled
       enable-snmp-auth-traps        disabled
       enable-snmp-syslog-notify     disabled
       enable-snmp-monitor-traps     disabled
       enable-env-monitor-traps      disabled
       snmp-syslog-his-table-length  1
       snmp-syslog-level             WARNING
       system-log-level              WARNING
       process-log-level             NOTICE
       process-log-ip-address        0.0.0.0
       process-log-port              0
       collect
              sample-interval                5
              push-interval                  15
              boot-state                     disabled
              start-time                     now
              end-time                       never
              red-collect-state              disabled
              red-max-trans                  1000
              red-sync-start-time            5000
              red-sync-comp-time             1000
              push-success-trap-state        disabled
       call-trace                    disabled
       internal-trace                disabled
       log-filter                    all
       default-gateway               192.168.131.1
       restart                       enabled
       exceptions
       telnet-timeout                0
       console-timeout               0
       remote-control                enabled
       cli-audit-trail               enabled
       link-redundancy-state         disabled
       source-routing                enabled
       cli-more                      disabled
       terminal-height               24
       debug-timeout                 0
       trap-event-lifetime           0
       cleanup-time-of-day           00:00
       last-modified-by              admin@192.168.131.60
       last-modified-date            2010-09-08 12:04:24
task done
```

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.