Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Communication Server 1000E R7.5, Avaya Aura® Session Manager R6.1, Acme Packet Net-Net Session Director 3800 to Support Gamma Telecom IPConnect SIP Trunk Service – Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) Trunking between Gamma Telecom IPConnect SIP Trunk Service and an Avaya SIP enabled Enterprise Solution. The Avaya solution consists of Avaya Aura® Session Manager, Avaya Communication Server 1000E and Acme Packet Net-Net Session Director 3800.

Gamma Telecom 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 lab.

1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between Gamma Telecom IPConnect SIP Trunk Service and an Avaya SIP enabled enterprise solution. The Avaya solution consists of Avaya Aura® Session Manager, Avaya Communication Server 1000E (CS1000E) connected to Gamma's SIP Trunk Service via an Acme Packet Net-Net Session Director 3800 (Acme SBC). Customers using this Avaya SIP enabled enterprise solution with Gamma's 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, Acme SBC and CS1000E. The enterprise site was configured to use the SIP Trunk Service provided by Gamma Telecom.

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 Gamma. Incoming PSTN calls were made to Unistim, SIP, Digital and analog telephones at the enterprise.
- Outgoing calls from the enterprise to the PSTN were made from Unistim, SIP, Digital and analog telephones.
- G729 annex b (silence suppression) is not supported by Gamma's SIP Trunk Service and thus was not tested.
- Calls using G.729, G.711A codec's.
- Fax calls to/from a group 3 fax machine to a PSTN connected fax machine using the T.38 mode.
- User features such as hold and resume, transfer, conference, call forwarding, etc.
- Caller ID Presentation and Caller ID Restriction.
- Call coverage and call forwarding for endpoints at the enterprise site.

2.2. Test Results

Interoperability testing of the sample configuration was completed with successful results for Gamma IPConnect SIP Trunk Service with the following observations.

- Outbound fax calls from the Communication Server 1000E using G.729 work. The fax call starts off at G729, however an invite is sent to the CS1K to switch to G711. The fax call then changes to use T38 and the fax goes through as normal.
- Incoming call to busy trunks or SIP Trunk signaling failure the following was observed - PSTN receives NU Tone eventually and 500 Service Unavailable sip message. The global parameter set on Gamma's SBC is 4 hunts per call, so if the call doesn't set up on the first try Gamma's SBC will re-try a further 3 times.

2.3. Support

For technical support on Gamma products please contact the following website:
http://www.gammatelecom.com/

3. Reference Configuration

Figure 1 illustrates the test configuration. The test configuration shows an enterprise site connected to Gamma Telecom using SIP Trunks. Located at the enterprise site are Session Manager, Acme SBC and a Communication Server 1000E. Endpoints are Avaya 1140 series IP telephones, Avaya 1200 series IP telephones (with Unistim and SIP firmware), Avaya IP Softphones (SMC3456, 2050 and Avaya one-X® Communicator), Avaya Digital telephone, Analog telephone and fax machine. For security purposes, any public IP addresses or PSTN routable phone numbers used in the compliance test are not shown in these Application Notes.

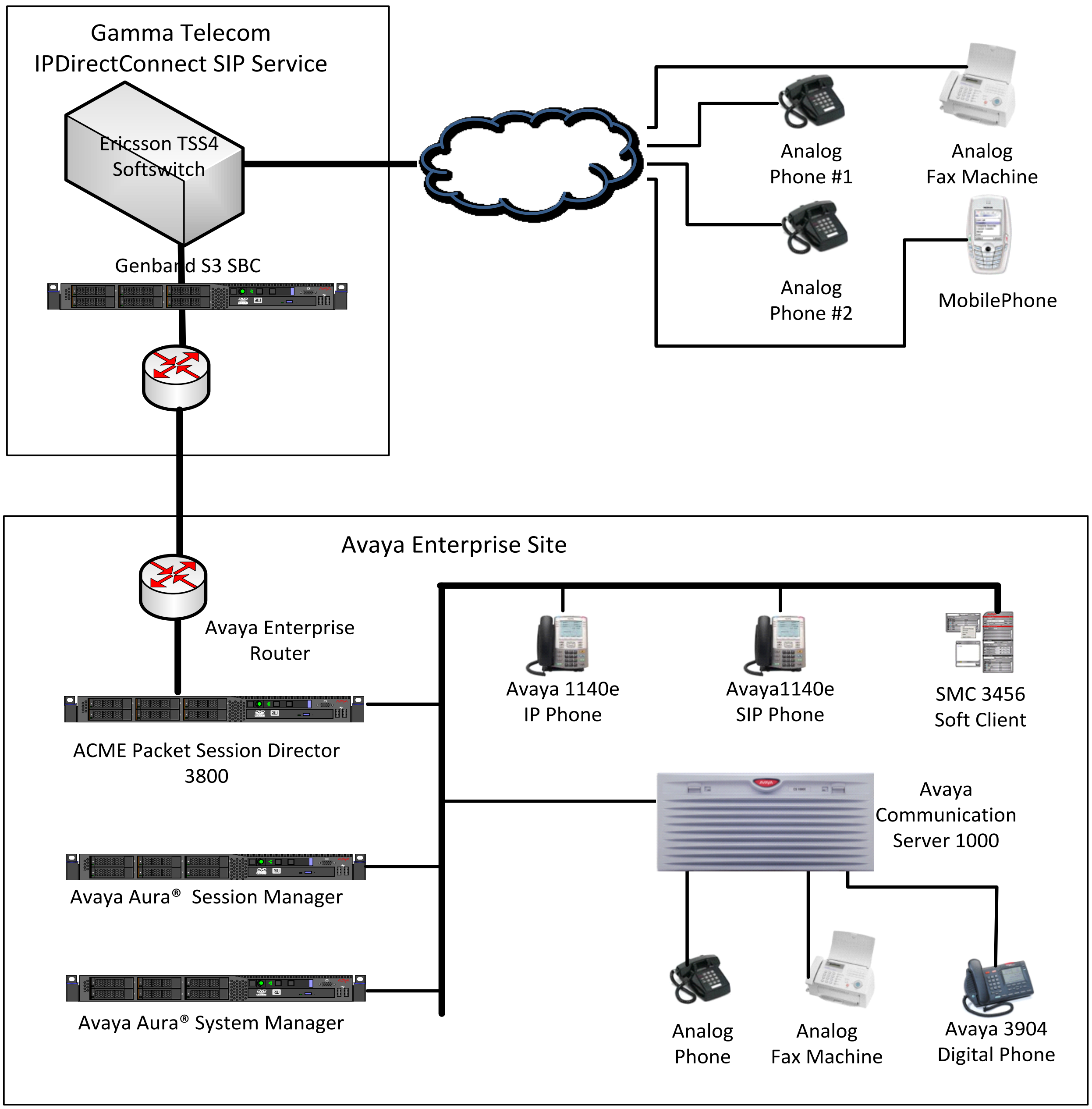


Figure 1: Gamma Telecom IPConnect SIP Trunk Topology

4. Equipment and Software Validated

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

Equipment	Software
Avaya Media S8800 server	Avaya Aura® Session Manager R6.1 Build: 6.1.0.0.610023
Avaya Media S8800 server	Avaya Aura® System Manager R6.1 Load: 6.1.0.0.7345 Service Pack 0
Avaya Communication Server 1000E running on CP+PM server as co-resident configuration	Avaya Communication Server 1000E R 7.5, Version 7.50.17 Service Update: 7.50_17Nov23 Deplist: X21 07.50Q
Acme Packet 3820 Net-Net SBC	Acme Packet 3820 Net-Net SBC Ver 6.1.0 Build 738
Avaya Communication Server 1000E Media Gateway	CSP Version: MGCC CD01 MSP Version: MGCM AB01 APP Version: MGCA BA07 FPGA Version: MGCF AA18 BOOT Version: MGCB BA07 DSP1 Version: DSP1 AB04
Avaya 1140e and 1230 Unistim Telephones	FW: 0625C8A
Avaya 1140e and 1230 SIP Telephones	FW: 04.01.13.00.bin
Avaya SMC 3456	Version 2.6 build 57666
Avaya one-X® Communicator	Version cs6.1.0.10
Avaya Analogue Telephone	N/A
Avaya M3904 Digital Telephone	N/A
Gamma Telecom IPConnect SIP Trunk Service	GENBAND iServer version-5.2.2.0

5. Configure Avaya Communication Server 1000E

This section describes the steps required to configure Communication Server 1000E for SIP Trunking and also the necessary configuration for terminals (analog, SIP and IP phones). SIP trunks are established between Communication Server 1000E and Session Manager. These SIP trunks carry SIP Signaling associated with Gamma's IPConnect SIP Trunk Service. For incoming calls, the Session Manager receives SIP messages from the Enterprise SBC, through which the Gamma IPConnect SIP Service directs incoming SIP messages to Communication Server 1000E (see **Figure 1**). Once a SIP message arrives at Communication Server 1000E, further incoming call treatment, such as incoming digit translations and class of service restrictions may be performed. All outgoing calls to the PSTN are processed within Communication Server 1000E and may be first subject to outbound features such as route selection, digit manipulation and class of service restrictions. Once Communication Server 1000E selects a SIP trunk, the SIP signaling is routed to the Session Manager. The Session Manager directs the outbound SIP messages to the Acme SBC and on to Gamma's network. Specific Communication Server 1000E configuration was performed using Element Manager and the system terminal interface. The general installation of the Communication Server 1000E, System Manager and Session Manager is presumed to have been previously completed and is not discussed here. For completeness a list of patches that are applied to the Communication Server 1000E are displayed in **Appendix A.**

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 Gamma's network, and any other SIP trunks needed. See the following screenshot for a typical System Limits printout. The value of **SIP ACCESS PORTS** defines the maximum number of SIP trunks for the Communication Server 1000E.

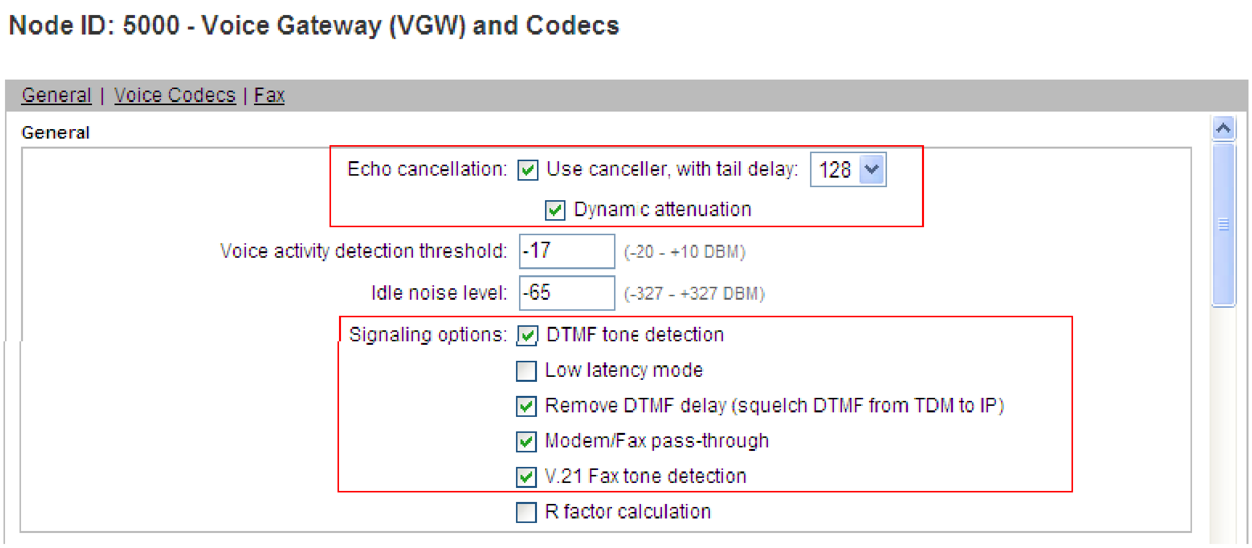
```
System type is - Communication Server 1000E/CPPM Linux
CPPM - Pentium M 1.4 GHz

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

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

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

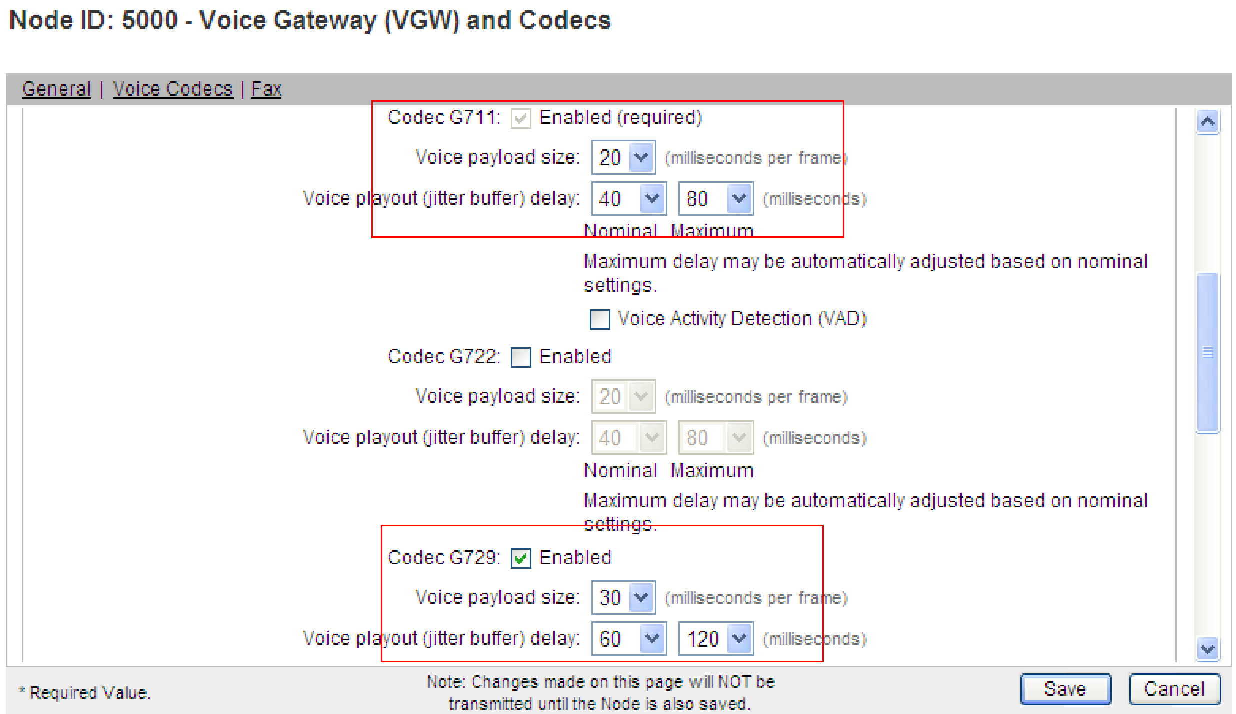
```
REQ: prt
TYPE: net
TYPE NET_DATA
CUST 0

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

5.2. Configure Codec's for Voice and FAX operation

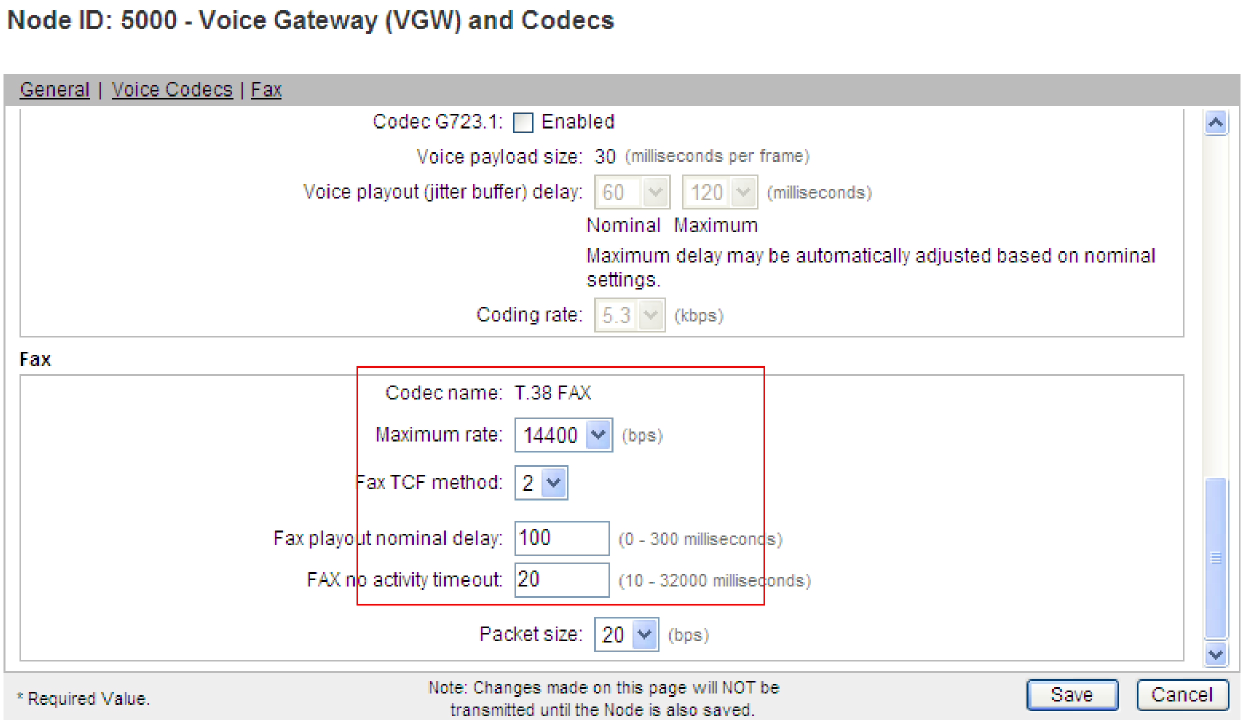
Gamma voice SIP Trunk service supports G.711A, G.729A voice codecs and T.38 FAX transmissions. Using the Communication Server 1000E element manager sidebar, navigate to the **IP Network → IP Telephony Nodes → Node Details → Voice Gateway (VGW) and Codecs** property page and configure the Communication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



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

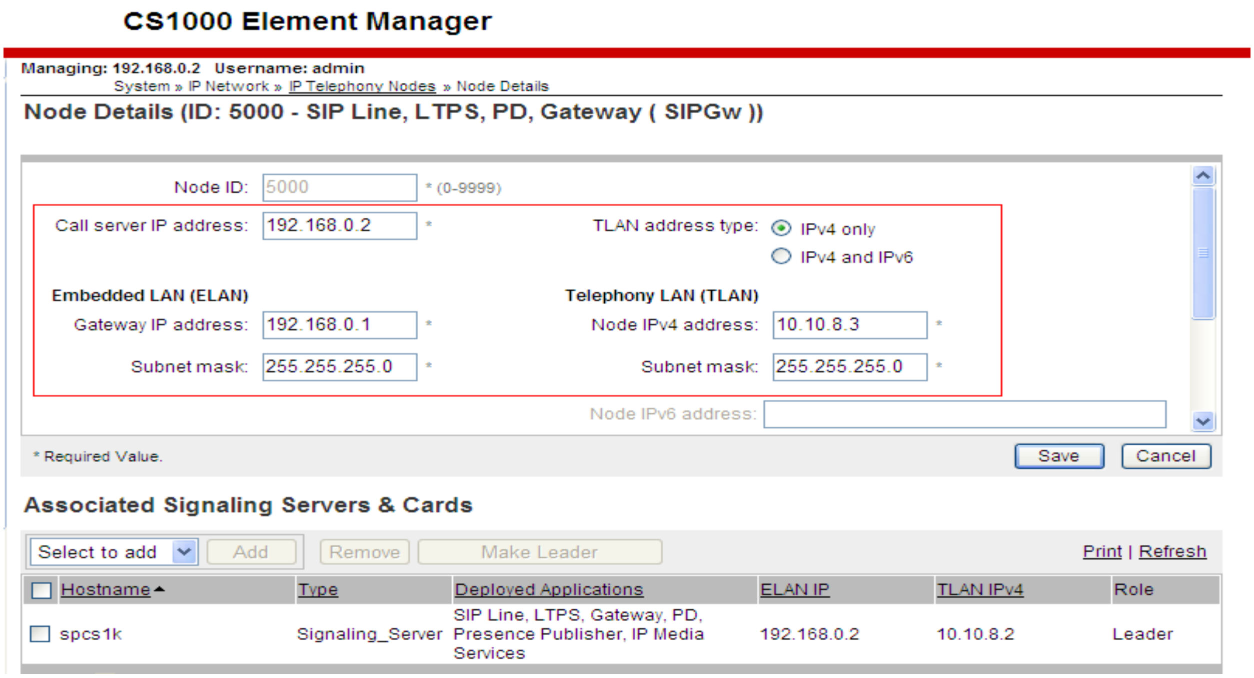


Finally, configure the **Fax** settings as in the highlighted section of the next screenshot.



5.3. Virtual Trunk Gateway Configuration

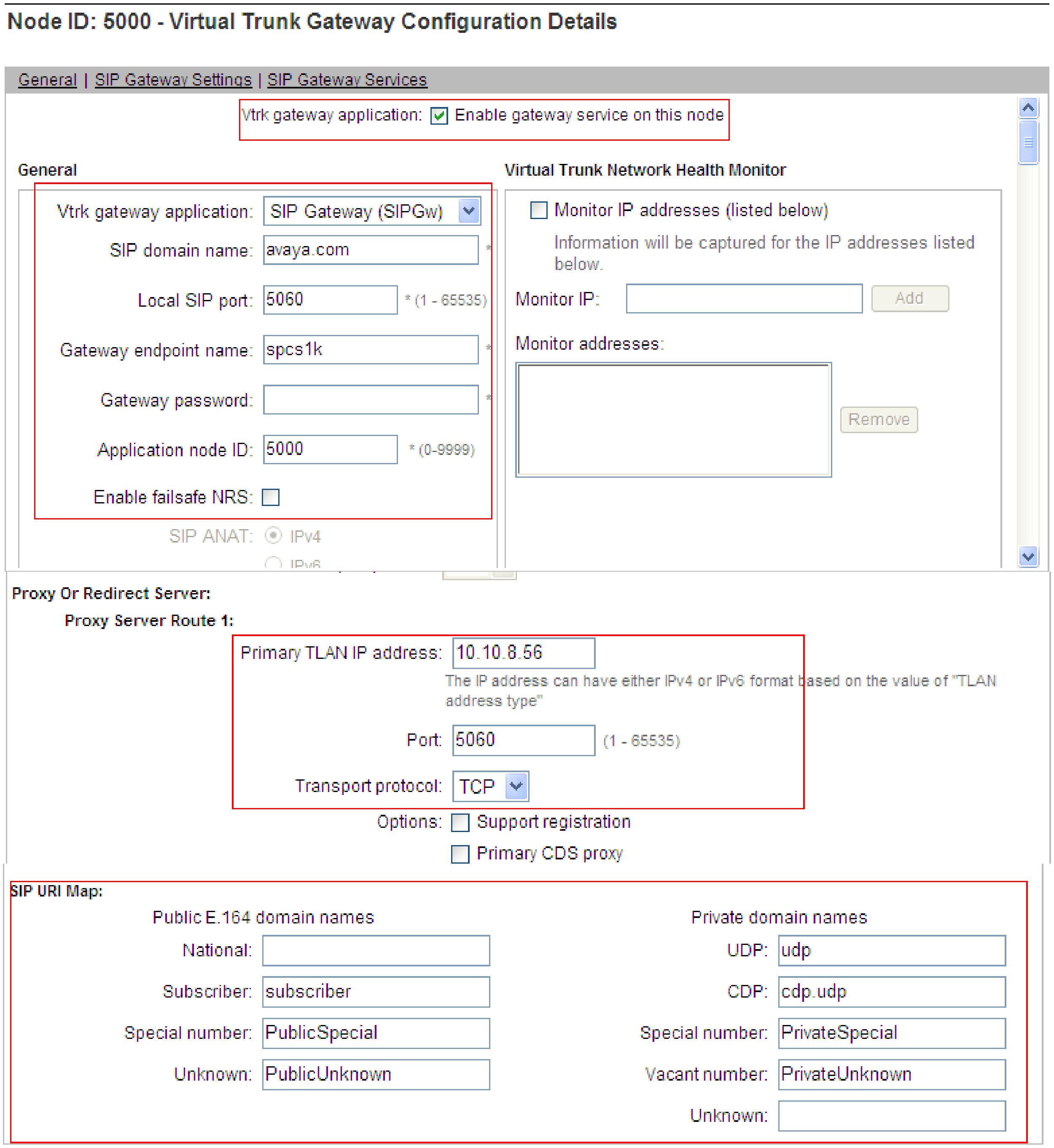
Use Communication Server 1000E Element Manager to configure the system node properties. Navigate to the **System → IP Network → IP Telephony Nodes → Node Details** and verify the highlighted section is completed with the correct IP addresses and subnet masks of the Node. At this stage the call server has an ip address and so too does the signalling server. The Node ip is the ip address that the IP phones use to register. This is also where the SIP trunk connection is made to the Session Manager. When an entity is added in Session Manager for the CS1000E it is the Node ip that is used (please see **Section 6.4** – Define SIP Entities for more details).



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

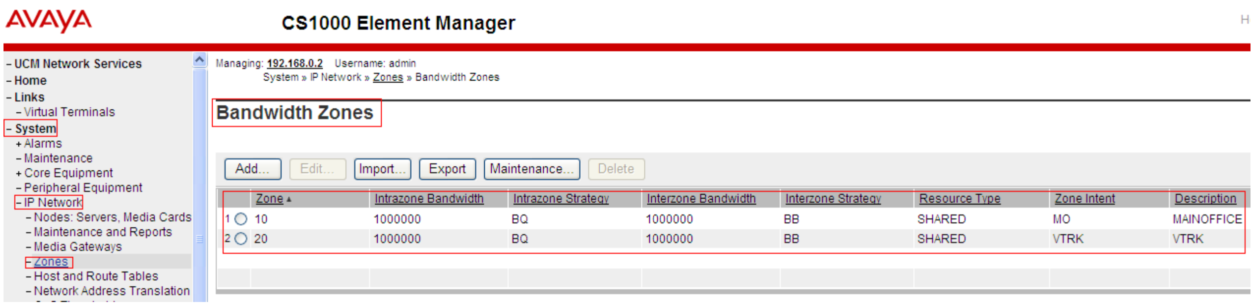
- **Vtrk gateway application:** Provides option to select Gateway applications. The three supported modes are SIP Gateway (SIPGw), H. 323Gw, and SIPGw and H.323Gw
- **SIP domain name:** The SIP Domain Name is the SIP Service Domain. The SIP Domain Name configured in the Signaling Server properties must match the Service Domain name configured in the Session Manager
- **Local SIP port:** The Local SIP Port is the port to which the gateway listens. The default value is 5060
- **Gateway endpoint name:** This field cannot be left blank so a value is needed here. This field is used when a Network Routing Server is used for registration of the endpoint. In this network a Session Manager is used so any value can be put in here and will not be used.

- **Application node id:** This is a unique value that can be alphanumeric and is for the new Node that is being created, in this case 5000
- **Proxy or Redirect Server:** Primary TLAN ip address is the SM100 ip address of the Session Manager. The transport protocol used for SIP, in this case is TCP
- **SIP URI Map: Public National** and **Private Unknown** are left blank. All other fields in the SIP URI Map are left with default values.



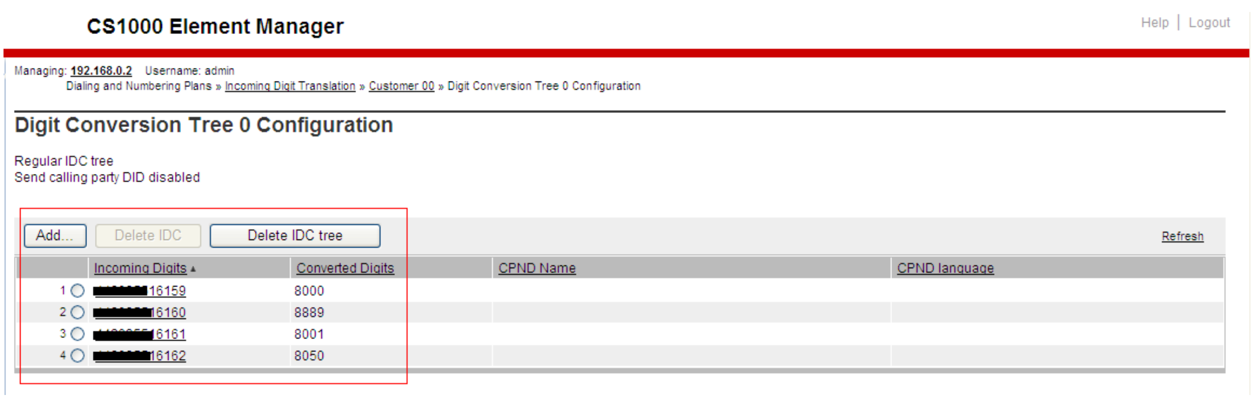
5.4. Configure Bandwidth Zones

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 a separate zones. Use Element Manager to define bandwidth zones as in the following highlighted example. Use Element Manager and navigate to **System → IP Network → Zones → Bandwidth Zones** and add new zones as required.



5.5. Configure Incoming Digit Conversion Table

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



5.6. Configure SIP Trunks

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

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

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

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

Next, configure the SIP trunk Route Data Block (RDB) using the Communication Server 1000E system terminal and overlay 16. Load **Overlay 16**, enter **RDB** at the prompt, press return and commence configuration. The value for **DCH** is the same as previously entered in overlay 17. The value for **NODE** should match the value in the **Node ID:** field on the **Node Details** form in **Section 5.3.** The value for **ZONE** should match the value for the **VTRK** zone used in **Section 5.4.** 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 00020
PCID SIP
CRID NO
NODE 5000
DTRK NO
ISDN YES
    MODE ISLD
    DCH  10
    IFC  SL1
    PNI  00001
    NCNA YES
    NCRD YES
    TRO  NO
    FALT NO
    CTYP UKWN
    INAC NO
    ISAR NO
    DAPC NO
MBXR NO
MBXOT NPA
MBXT 0
PTYP ATT
CNDP UKWN
AUTO NO
DNIS NO
DCDR NO
ICOG IAO
SRCH LIN
TRMB YES
STEP
ACOD 1600
TCPP NO
PII NO
AUXP NO
TARG
CLEN 1
BILN NO
OABS
INST
IDC  YES
DCNO 0
NDNO 0 *
DEXT NO
DNAM NO
SIGO STD
STYP SDAT
MFC  NO
ICIS YES
OGIS YES
TIMR ICF  1920
     OGF  1920
     EOD  13952
     LCT  256
     DSI  34944
     NRD  10112
     DDL  70
     ODT  4096
     RGV  640
     GTO  896
     GTI  896
     SFB  3
     PRPS  800
     NBS  2048
     NBL  4096
     IENB  5
     TFD  0
     VSS  0
     VGD  6
     EESD  1024
SST  5 0
DTD  NO
SCDT NO
2 DT NO
NEDC ORG
FEDC ORG
CPDC NO
DLTN NO
HOLD 02 02 40
SEIZ 02 02
SVFL 02 02
DRNG NO
CDR  NO
NATL YES
SSL
CFWR NO
IDOP NO
VRAT NO
MUS  YES
MRT  21
PANS YES
RACD NO
MANO NO
FRL  0 0
FRL  1 0
FRL  2 0
FRL  3 0
FRL  4 0
FRL  5 0
FRL  6 0
FRL  7 0
OHQ  NO
OHQT 00
CBQ  NO
AUTH NO
TTBL 0
ATAN NO
OHTD NO
PLEV 2
OPR  NO
ALRM NO
ART  0
PECL NO
DCTI 0
TIDY 1600 100
ATRR NO
TRRL NO
SGRP 0
ARDN NO
CTBL 0
AACR NO
```

Next, configure virtual trunk members using the Communication Server 1000E system terminal and **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 00020
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 Route List Index (**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** values. The value for **CFG_ZONE** is the same value used in **Section 5.4** for **VIRTUALSETS**.

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

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

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

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

Digital telephones are 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 8001 0     MARP
        CPND
          CPND_LANG ROMAN
            NAME Digital Set
            XPLN 10
            DISPLAY_FMT FIRST,LAST
     01 MCR 8001 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 Old Telephone Service (POTS) and also configured to allow T.38 Fax transmission. A unique value is entered for **DN**, this is the extension number. **DTN** is required if the telephone uses DTMF dialing. Values **FAXA** and **MPTD** configure the port for T.38 Fax transmissions.

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

ERL 00000
WRLS NO
DN   8002
AST  NO
IAPG 0
HUNT
TGAR 0
LDN  NO
NCOS 0
SGRP 0
RNPG 0
XLST
SCI  0
SCPW
SFLT NO
CAC_MFC 0
CLS  UNR DTN FBD XFD WTA THFD FND HTD ONS
     LPR XRD AGRD CWD SWD MWD RMMD SMWD LPD XHD SLKD CCSD LND TVD
     CFTD SFD MRD C6D CNID CLBD AUTU
     ICDD CDMD LLCN EHTD MCTD
     GPUD DPUD CFXD ARHD OVDD AGTD CLTD LDTD ASCD SDND
     MBXD CPFA CPTA UDI RCC HBTD IRGD  DDGA NAMA MIND
     NRWD NRCD NROD SPKD CRD PRSD MCRD
     EXR0 SHL SMSD ABDD CFHD DNDY DNO3
     CWND USMD USRD CCBD BNRD OCBD RTDD RBDD RBHD FAXA CNUD CNAD PGND FTTC
     FDSD NOVD CDMR PRED MCDD T87D SBMD PKCH MPTD
PLEV 02
PUID
AACS NO
MLWU_LANG 0
FTR  DCFW 4
```

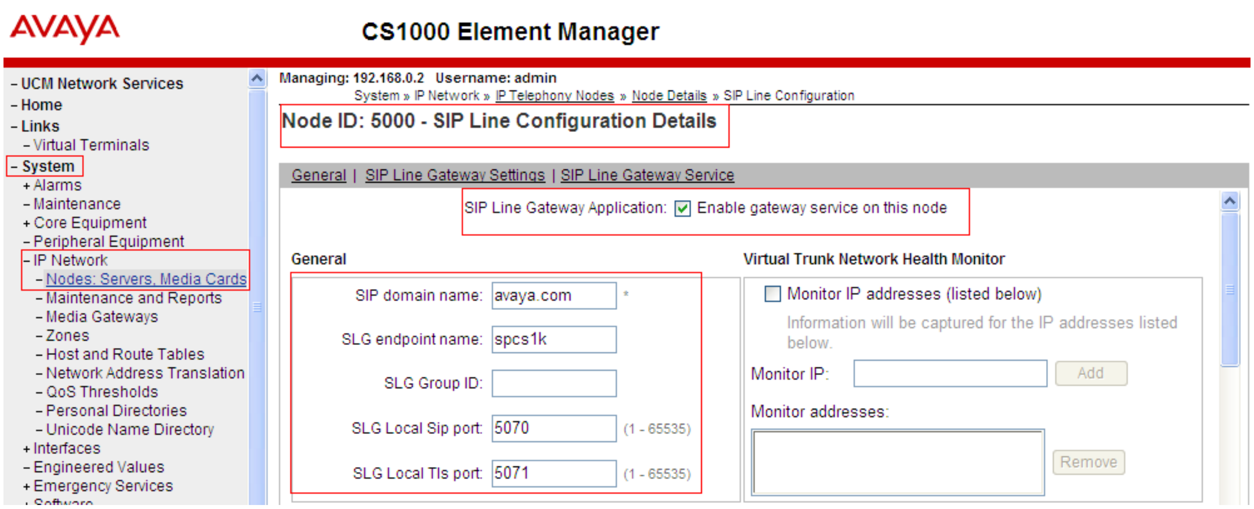
5.8. Configure the SIP Line Gateway Service

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

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

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

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



5.9. Configure SIP Line Telephones

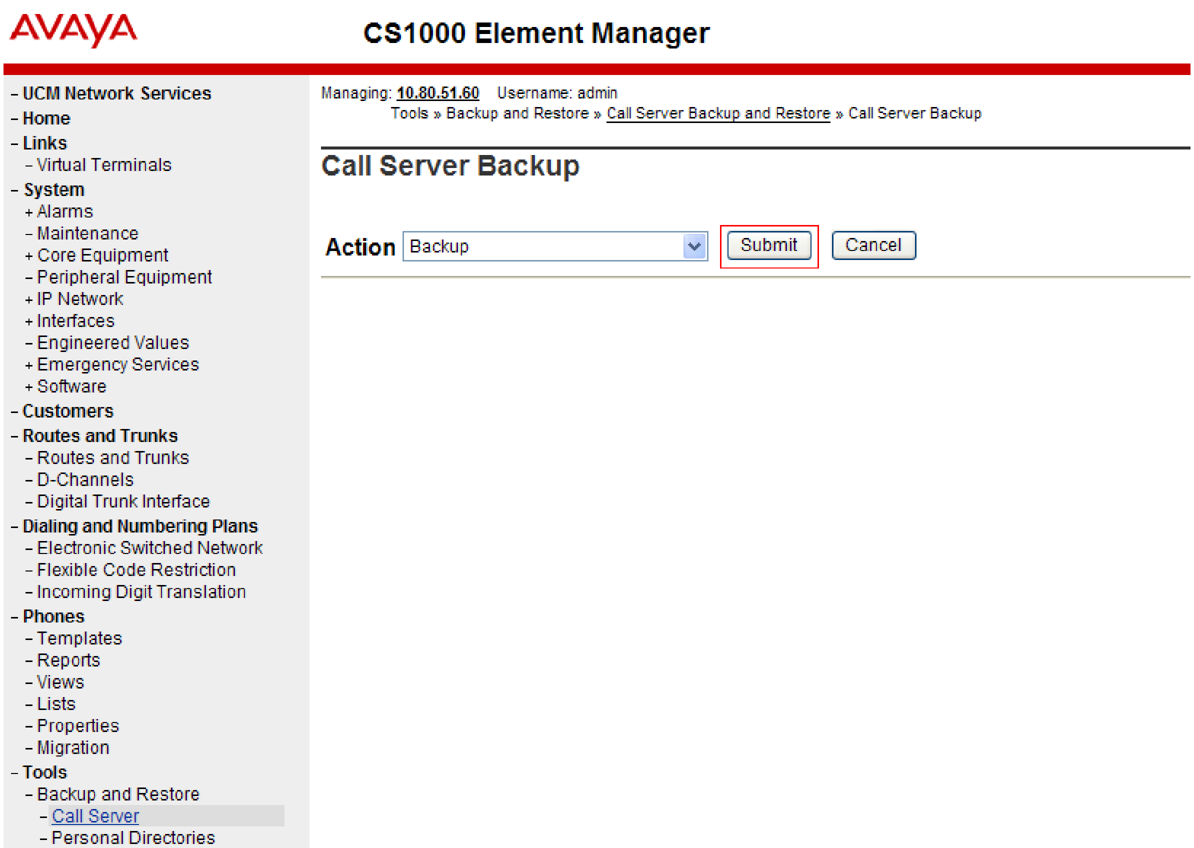
When SIP Line service configuration is completed, use the Communication Server 1000E system terminal and overlay 20 to add a Universal Extension (UEXT). See the following example of a SIP Line extension. The value for **UXTY** must be **SIPL**. This example is for an Avaya SIP telephone, so the value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

```
Overlay 20 – SIP Telephone Configuration
DES  SIPD
TN   096 0 01 15  VIRTUAL
TYPE UEXT
CDEN 8D
CTYP XDLC
CUST 0
UXTY SIPL
MCCL YES
SIPN 1
SIP3 0
FMCL 0
TLSV 0
SIPU 8889
NDID 5
SUPR NO
SUBR DFLT MWI RGA CWI MSB
UXID
NUID
NHTN
CFG_ZONE 00010
CUR_ZONE 00010
ERL  0
ECL  0
VSIT NO
FDN
TGAR 0
LDN  NO
NCOS 0
SGRP 0
RNPG 0
SCI  0
SSU
XLST
SCPW 1234
SFLT NO
CAC_MFC 0
CLS  UNR FBD WTA LPR MTD FNA HTA TDD HFD CRPD
     MWD LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
     POD SLKD CCSD SWD LND CNDA
     CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBD
     ICDD CDMD LLCN MCTD CLBD AUTU
     GPUD DPUD DNDA CFXA ARHD FITD CLTD ASCD
     CPFA CPTA ABDD CFHD FICD NAID BUZZ AGRD MOAD

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

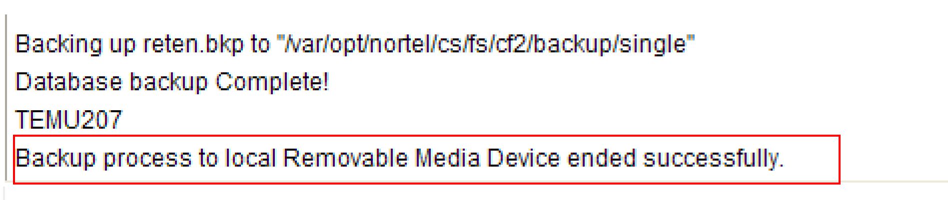
```
---continued from previous page---

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

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

5.10. Save Configuration

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



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



Configuration of Communication Server 1000E is complete.

6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager to receive and route calls over the SIP trunk between Communication Server 1000E and Session Manager. These instructions assume other administration activities have already been completed such as defining the SIP entity for Session Manager, defining the network connection between System Manager and Session Manager, and adding SIP endpoints. The following administration activities will be described.

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

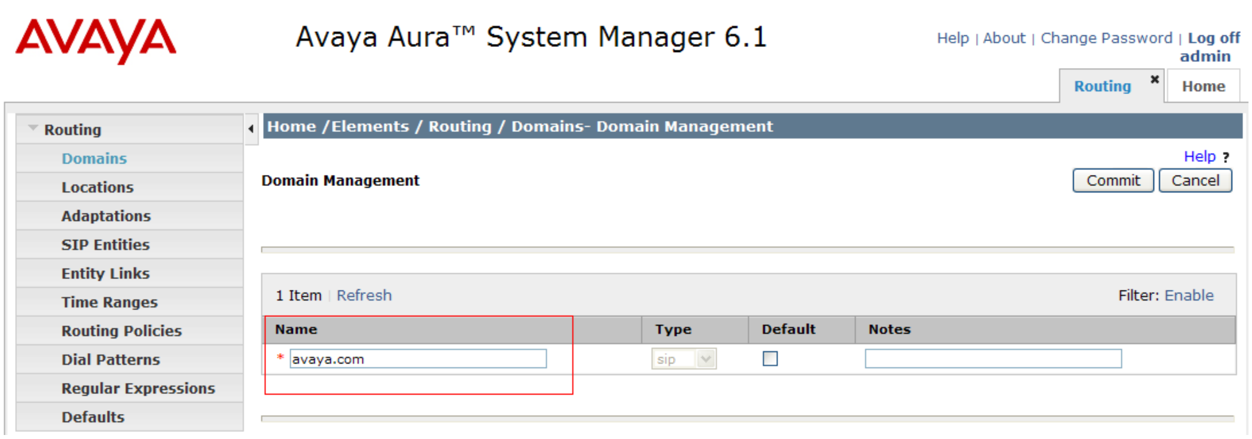
Configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL "**http://<ip-address>/SMGR**", where **<ip-address>** is the IP address of System Manager. Log in with the appropriate login credentials. Some administration screens have been abbreviated for clarity.

6.1. Define SIP domains

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

- **Name** Enter the Domain Name specified for the SIP Gateway in **Section 5.3.** In the sample configuration, **avaya.com** was used
- **Type** Verify **SIP** is selected
- **Notes** Add a brief description [Optional]

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



6.2. Define Location for Avaya Communication Server 1000E

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

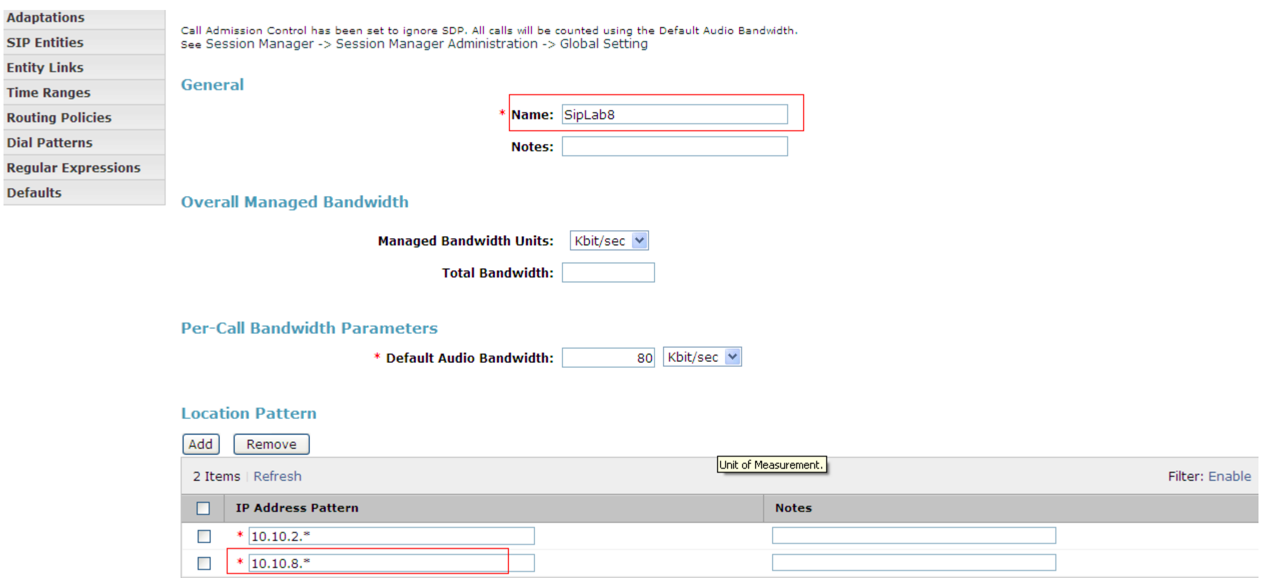
- **Name:** Enter a descriptive name for the location
- **Notes:** Add a brief description [Optional]

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

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

Click **Commit** to save.

The screenshot below shows the Location defined for Communication Server 1000E in the sample configuration.



6.3. Define SIP Entities

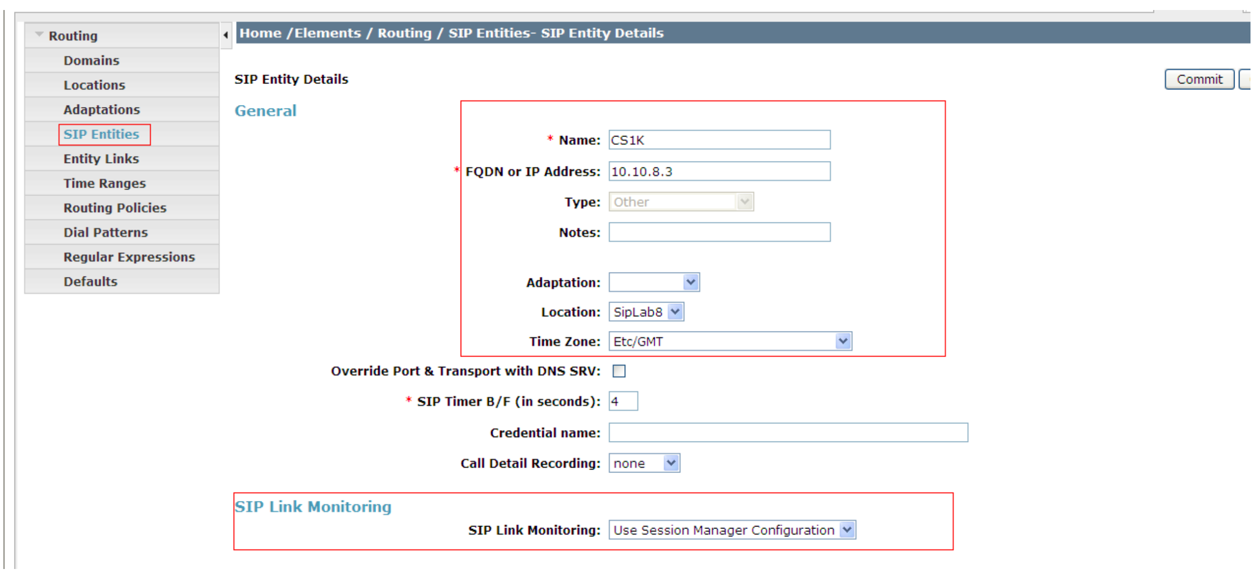
A SIP Entity must be added for Communication Server 1000E and also for the Acme SBC. Expand **Elements → Routing** and select **SIP Entities** from the left navigation menu. 2 new SIP Entities will need to be added as noted above. Click **New** (not shown**).** In the **General** section, enter the following values and use default values for remaining fields**.**

- **Name:** Enter an identifier for the SIP Entity
- **FQDN or IP Address:** Enter TLAN IP address of Communication Server 1000E Node identified in **Section 5.3** For the Acme SBC enter the private interface IP address
- **Type:** Select **other** for the Communication Server 1000E and **gateway** for the Acme SBC
- **Notes:** Enter a brief description [Optional]
- **Location:** Select the Location defined for Communication Server 1000E in **Section 6.2** and also apply this same location to the Acme SBC

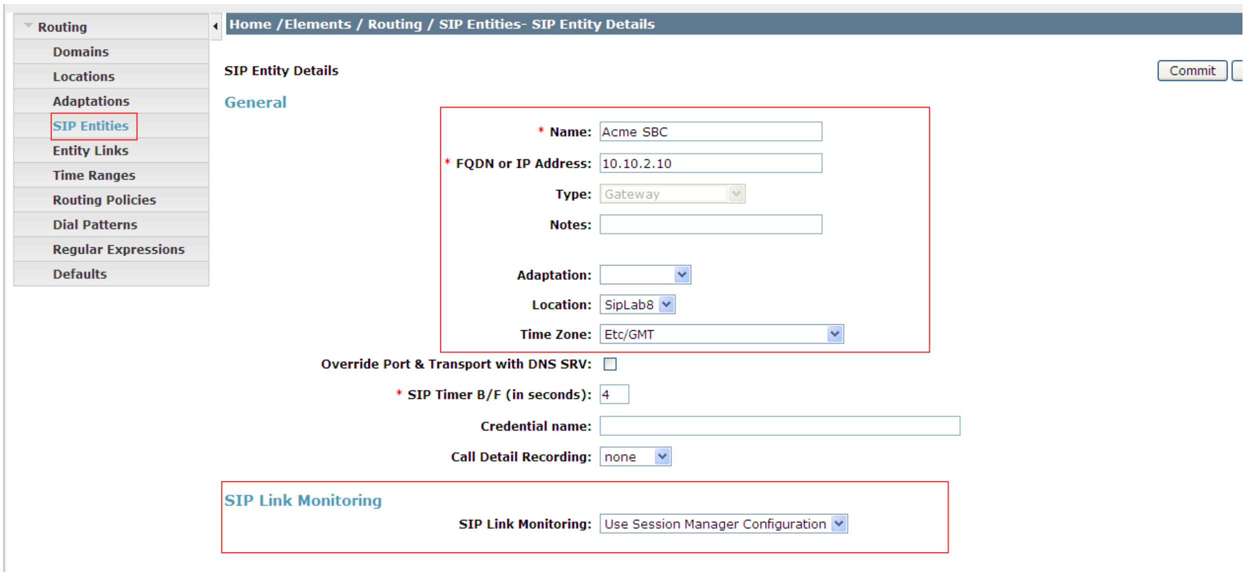
In the **SIP Link Monitoring** section.

- **SIP Link Monitoring:** Select **Use Session Manager Configuration**

Click **Commit** to save the definition of the new SIP Entity. The following screenshot shows the SIP Entity defined for Communication Server 1000E in the sample configuration.



The following screenshot shows the SIP Entity defined for Acme SBC in the sample configuration.



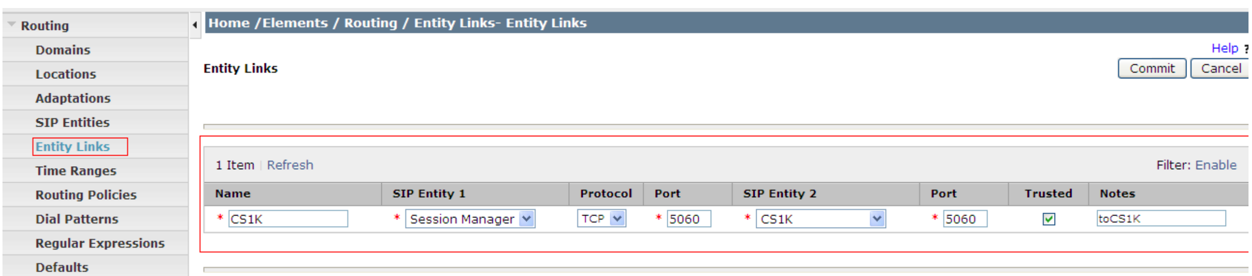
A SIP Entity link must also be defined for your Session Manager but that is not shown in this document.

6.4. Define Entity links

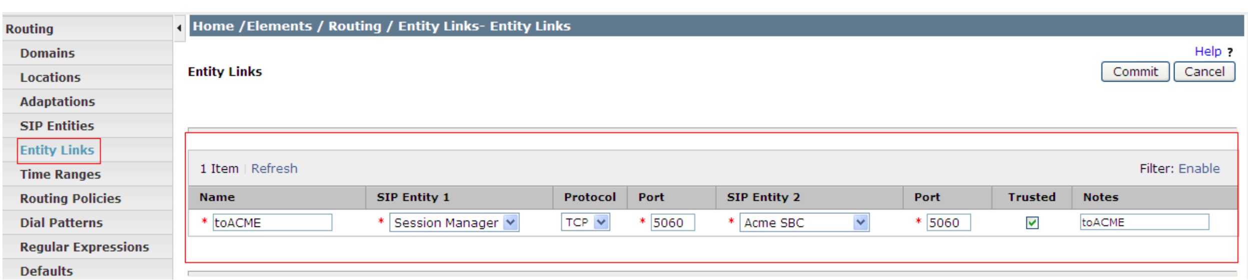
The SIP trunk between the Session Manager and the Communication Server 1000E is described by an Entity link. The same is needed between the Session Manager and Acme SBC. Expand **Elements → Routing** and select **Entity Links** from the left navigation menu. Click **New** (not shown). Enter the following values**.**

- **Name** Enter an identifier for the link to each telephony system
- **SIP Entity 1** Select SIP Entity defined for Session Manager
- **SIP Entity 2** Select the SIP Entity defined for Avaya Communication Server 1000E/Acme SBC in **Section 6.3**
- **Protocol** After selecting both SIP Entities, select **TCP** as the required protocol
- **Port** Verify **Port** for both SIP entities is the default listen port. For the sample configuration, default listen port is **5060**
- **Trusted** Enter a tick in the box
- **Notes** Enter a brief description [Optional]

Click **Commit** to save **Entity Link** definition. The following screen shows the entity link defined for the SIP trunk between Session Manager and Communication Server 1000E.



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



6.5. Define Routing Policy

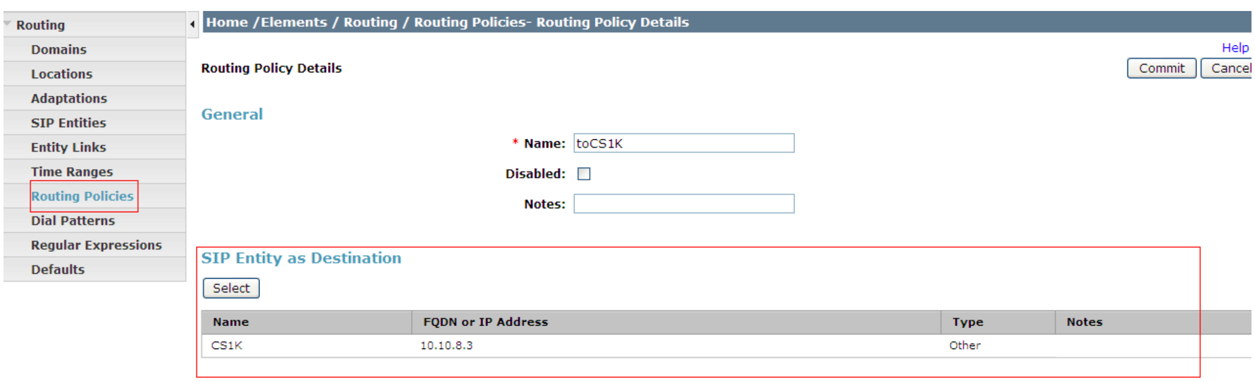
Routing policies describe the conditions under which calls will be routed to Communication Server 1000E from either SIP endpoint registered to Session Manager or from other telephony system. It also describes the routing polices for which calls will be routed to the Acme SBC and therefore to Gamma's SIP network. To add a routing policy, expand **Elements → Routing** and select **Routing Policies.** Click **New** (not shown). In the **General** section, enter the following values.

- **Name:** Enter an identifier to define the routing policy
- **Disabled:** Leave unchecked
- **Notes:** Enter a brief description [Optional]

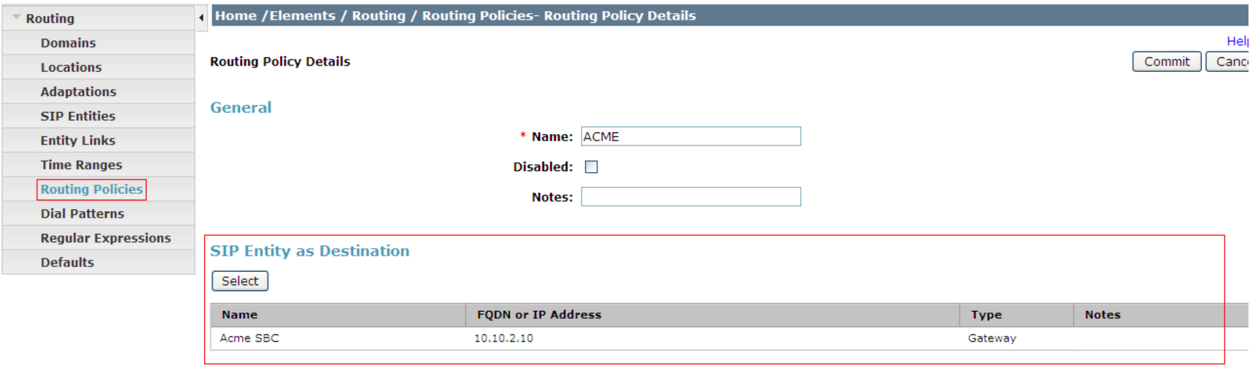
In the **SIP Entity as Destination** section, click **Select.** The **SIP Entity List** page opens (not shown). For routing policy to the Communication Server 1000E, select the SIP Entity associated with Communication Server 1000E defined in **Section 6.3**and click **Select.** The selected SIP Entity displays on the **Routing Policy Details** page. Use default values for remaining fields. Click **Commit** to save Routing Policy definition.

Note: The routing policy defined in this section is an example and was used in the sample configuration. Other routing policies may be appropriate for different customer networks.

The following screenshot shows the Routing Policy for CS1K:



For routing policy to the Acme SBC – Gamma SIP Trunk, select the SIP Entity associated with Acme SBC defined in **Section 6.3** and click **Select.** The selected SIP Entity displays on the **Routing Policy Details** page. Use default values for remaining fields. Click **Commit** to save Routing Policy definition. The following screenshot shows the Routing Policy for Acme SBC – Gamma SIP Trunk.



6.6. Define Dial Pattern

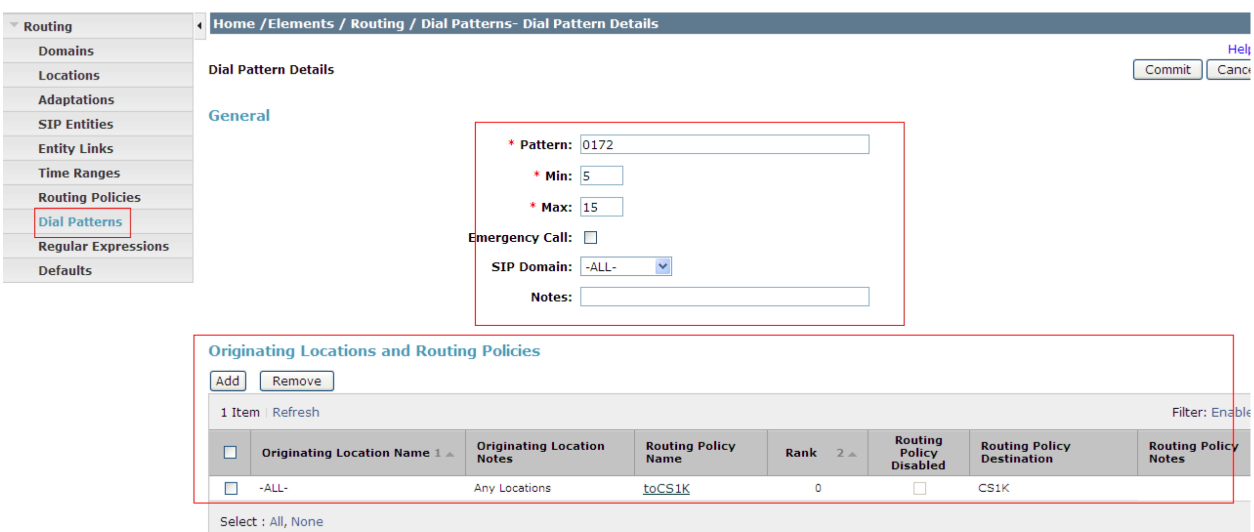
Dial patterns are used to route calls to appropriate SIP Entities. In the sample configuration the DDI number range given for the testing start with **0172, these** will be routed to the Communication Server 1000E for terminating to test sets. Alternately calls that are originated on the Communication Server 1000E that start with digits **00353** will be routed to the Acme SBC and then on to Gamma's SIP network, there is a dialing pattern added for this as well. To define a dial pattern, expand **Elements → Routing** and select **Dial Patterns** (not shown). Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Pattern:** Enter dial pattern for calls to Avaya Communication Server 1000E
- **Min:** Enter the minimum number digits that must to be dialed
- **Max:** Enter the maximum number digits that may be dialed
- **SIP Domain:** Select the SIP Domain from drop-down menu or select **All** if Session Manager should accept incoming calls from all SIP domains
- **Notes:** Enter a brief description.[Optional]

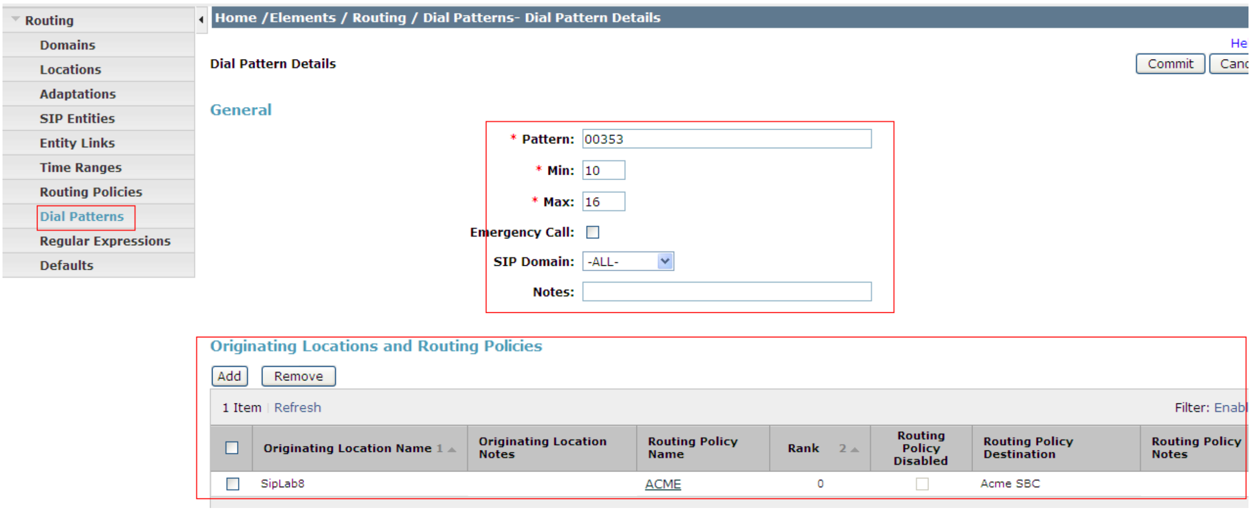
In the **Originating Locations and Routing Policies** section, click **Add.** The **Originating Locations and Routing Policy List** page opens (not shown).

- **Originating Locations** Select **All**
- **Routing Policies** Select the Routing Policy defined for Communication Server 1000E in **Section 6.5**

Click **Select** to save these changes and return to **Dial Pattern Details** page. Click **Commit** to save. The following screen shows the Dial Pattern defined for sample configuration. The following screenshot shows the Routing Policy for Communication Server 1000E.



Repeat the above steps to add the dial Pattern to the Acme SBC, select the routing policy defined for the Acme SBC in **Section 6.5**. The following screenshot shows the Routing Policy for Acme SBC – Gamma's SIP network.



7. Configure Acme Packet 3800 Net-Net Session Director

This section describes the configuration of the Acme SBC. The Acme Packet Session Director was configured via the Acme Packet Command Line Interface (ACLI). This section assumes the reader is familiar with accessing and configuring the Acme Packet Session Director. 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 3800 Net-Net Session Director

Connect to the Acme Packet Session Director 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 Session Director. All public ip addresses will be hidden and replaced by xx.xx.xx.xx.
Access the **system-config** element and set the following element parameters:

- **default-gateway**: The IP address of the default gateway for acme packet session director. In this case, the default gateway is **10.10.2.1**
- **source-routing**: should be set to **enabled**

```
system-config
        hostname
        description
        location

      < text removed for brevity >

        call-trace                    disabled
        internal-trace                disabled
        log-filter                    all
        default-gateway               10.10.2.1
        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 Session Director 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 **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                          S0P0
        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                          S0P1
        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
- **netmask**: Subnet mask for the IP subnet
- **gateway**: The subnet gateway address
- **hip-ip-list**: The virtual IP address assigned to the Acme Packet Session Director on this interface
- **icmp-address**: The list of IP addresses which the Acme Packet Session Director will answer ICMP requests on this interface

The settings for the outside, untrusted side network interface are shown below. The ip addresses have been replaced with xx.xx.xx.xx for security purposes.

```
network-interface
        name                           S0P0
        sub-port-id                    0
        description                    OUTSIDE
        hostname
        ip-address                     xx.xx.xx.xx
        pri-utility-addr
        sec-utility-addr
        netmask                        255.255.255.128
        gateway                        xx.xx.xx.xx
        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                    xx.xx.xx.xx
        ftp-address
        icmp-address                   xx.xx.xx.xx
        snmp-address
        telnet-address
        last-modified-by               admin@192.168.1.6
        last-modified-date             2010-09-08 12:11:55
```

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

```
network-interface
        name                           S0P1
        sub-port-id                    0
        description                    INSIDE
        hostname
        ip-address                     10.10.2.10
        pri-utility-addr
        sec-utility-addr
        netmask                        255.255.255.0
        gateway                        10.10.2.1
        sec-gateway
        gw-heartbeat
                state                          enabled
                heartbeat                      10
                retry-count                    3
                retry-timeout                  1
                health-score                   30
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                    11
        hip-ip-list                    10.10.2.10
        ftp-address                    10.10.2.10
        icmp-address                   10.10.2.10
        snmp-address
        telnet-address                 10.10.2.10
        last-modified-by               admin@192.168.1.6
        last-modified-date             2010-09-08 14:18:22
```

7.5. Realm

A realm represents a group of related Acme Packet Session Director components. Two realms were defined for the compliance test. The **outside** realm was defined for the external untrusted network and the **inside** realm was defined for the internal enterprise network. Access the **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                      OUTSIDE
        description                     SIP_LAB_OUTSIDE
        addr-prefix                     0.0.0.0
        network-interfaces
                                        S0P0:0
        mm-in-realm                     enabled
        mm-in-network                   enabled
        mm-same-ip                      enabled
        mm-in-system                    enabled

< text removed for brevity >

realm-config
        identifier                      INSIDE
        description                     SIP_LAB_INSIDE
        addr-prefix                     0.0.0.0
        network-interfaces
                                        S0P1:0
        mm-in-realm                     enabled
        mm-in-network                   enabled
        mm-same-ip                      enabled
        mm-in-system                    enabled

< text removed for brevity >
```

7.6. SIP Configuration

The SIP configuration defines the global system-wide SIP parameters. Access the **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 Session Director.
- **nat-mode**: Set to **none** - no SIP NAT function is necessary.
- **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            enabled
        home-realm-id                  INSIDE
        egress-realm-id
        nat-mode                       None
        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 Session Director receives and sends SIP messages. Two SIP interfaces were defined; one for each realm. Access the **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 **init-timer and max-timer** 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 **init-timer and max-timer** in **sip-config (Section 7.6)** will be used.

The ip addresses have been replaced with xx.xx.xx.xx for security purposes.

```
sip-interface
        state                          enabled
        realm-id                       OUTSIDE
        description                    SIP_LAB_outside
        sip-port
                address                        XX.XX.XX.XX
                port                           5060
                transport-protocol             UDP
                tls-profile
                allow-anonymous                all
                ims-aka-profile
        carriers
        trans-expire                   0
        invite-expire                  0

< text removed for brevity >

sip-interface
        state                          enabled
        realm-id                       INSIDE
        description                    Avaya SBC
        sip-port
                address                        10.10.2.10
                port                           5060
                transport-protocol             TCP
                tls-profile
                allow-anonymous                all
                ims-aka-profile
        carriers
        trans-expire                   0
        invite-expire                  0

< text removed for brevity >
```

7.8. Session Agent

A session agent defines the characteristics of a signalling peer to the Acme Packet Session Director such as Session Manager. Access the **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.
- **state**: Set to **enabled**
- **app-protocol**: Is 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.
- **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, **SIPGAM** (more details in **Section 7.9**)

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

```
session-agent
        hostname                       10.10.8.56
        ip-address                     10.10.8.56
        port                           5060
        state                          enabled
        app-protocol                   SIP
        app-type
        transport-method               UDP+TCP
        realm-id                       INSIDE
        egress-realm-id
        description                    SM100
        carriers

< text removed for brevity >
        response-map
        ping-method                    OPTIONS;hops=0
        ping-interval                  120
        ping-send-mode                 keep-alive

< text removed for brevity >
        in-manipulationid
        out-manipulationid             SIPGAM
        manipulation-string

< text removed for brevity >
```

The settings for the session agent relating to Gamma's SBC are shown below. The ip addresses have been replaced with xx.xx.xx.xx for security purposes.

```
session-agent
        hostname                       xx.xx.xx.xx
        ip-address                     xx.xx.xx.xx
        port                           5060
        state                          enabled
        app-protocol                   SIP
        app-type
        transport-method               UDP
        realm-id                       OUTSIDE
        egress-realm-id
        description                    Gamma
        carriers

< text removed for brevity >

        response-map
        ping-method                    OPTIONS;hops=66
        ping-interval                  120
        ping-send-mode                 keep-alive

< text removed for brevity >

        in-manipulationid
        out-manipulationid             SIPGAM
        manipulation-string

< text removed for brevity >
```

7.9. SIP Manipulation

SIP manipulations are rules used to modify the SIP messages. During the compliance testing two sip manipulations were used, these were assigned to session agents in **Section 7.8 in the out-manipulationid** field**.** 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 **SIPGAM** 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 **ModFromHost** 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. The second header rule called **ModTo** specifies the to header in sip request messages will be manipulated based on the element rule defined. The element rule called **ModToHost** specifies that the host part of the URI in the to header should be replaced with the Value $REMOTE_IP. The Value REMOTE_IP is the IP address of the SIP interface that message is being sent to.

```
sip-manipulation
        name                           SIPGAM
        description
        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
```

7.10. 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 **steering-pool** element and set the following element parameters:

- **ip-address:** The address of the interface on the Acme Packet Session Director.
- **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                     10.10.2.10
        start-port                     2048
        end-port                       3329
        realm-id                       INSIDE
        network-interface
        last-modified-by               admin@console
        last-modified-date             2011-05-26 07:16:43
steering-pool
        ip-address                     xx.xx.xx.xx
        start-port                     10000
        end-port                       20000
        realm-id                       OUTSIDE
        network-interface
        last-modified-by               admin@console
        last-modified-date             2011-05-26 07:17:24
```

7.11. Local Policy

Local policy controls the routing of SIP calls from one realm to another. Access the **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 **outside** realm are to be sent to the **inside** realm and sent to the Session Manager SM100 ip address 10.10.8.56.

```
local-policy
        from-address
                                       *
        to-address
                                       *
        source-realm
                                       OUTSIDE
        description                    Far-side-realm
        activate-time                  N/A
        deactivate-time                N/A
        state                          enabled
        policy-priority                none
        last-modified-by               admin@console
        last-modified-date             2011-05-26 07:25:20
        policy-attribute
                next-hop                       10.10.8.56
                realm                          INSIDE
                action                         none

< text removed for brevity >
```

The settings for the second **local-policy** are shown below. This policy indicates that messages originating from the **inside** realm are to be sent to the **outside** realm using IP address of Gamma's SBC.

```
local-policy
        from-address
                                      *
        to-address
                                      *
        source-realm
                                      INSIDE
        description
        activate-time                 N/A
        deactivate-time               N/A
        state                         enabled
        policy-priority               none
        last-modified-by              admin@console
        last-modified-date            2011-05-26 07:24:29
        policy-attribute
                next-hop                      xx.xx.xx.xx
                realm                         OUTSIDE
                action                        none

< text removed for brevity >
```

7.12. Media Profile

The Media Profile that was added for this testing was needed for some MobileX call scenarios e.g. when a call is handed off to the mobile device from the station handset on the Communication Server 1000E. For this particular call scenario when the call is handed off to the mobile device the INVITE sent to the mobile did not contain any SDP information. The media profile rule was setup so that if any INVITE is received without any SDP information the following would be added:

- **name:** **PCMA** – this needs to be a relevant MIME type in the SDP
- **media type:** **audio**
- **payload:** **8** (for PCMA)
- **transport:** **RTP/AVP**

```
media-profile
        name                          PCMA
        subname
        media-type                    audio
        payload-type                  8
        transport                     RTP/AVP
        req-bandwidth                 0
        frames-per-packet             0
        parameters
        average-rate-limit            0
        sdp-rate-limit-headroom       0
        sdp-bandwidth                 disabled
        police-rate                   0
```

This media profile is then associated to the outside interface:

- **add-sdp-invite:** The rule that the media profile applies to – invite.
- **add-sdp-profiles:** The media profile that was created, in this case PCMA . This will apply to an outgoing INVITE that has no SDP.

```
sip-interface
        state                          enabled
        realm-id                       OUTSIDE
        description                    SIP_LAB_outside
        sip-port
                address                        86.47.122.52
                port                           5060
                transport-protocol             UDP
                tls-profile
                allow-anonymous                all
                ims-aka-profile

< text removed for brevity >

        add-sdp-invite                 invite
        add-sdp-profiles               PCMA
        last-modified-by               admin@10.10.2.110
        last-modified-date             2011-06-20 03:22:30
```

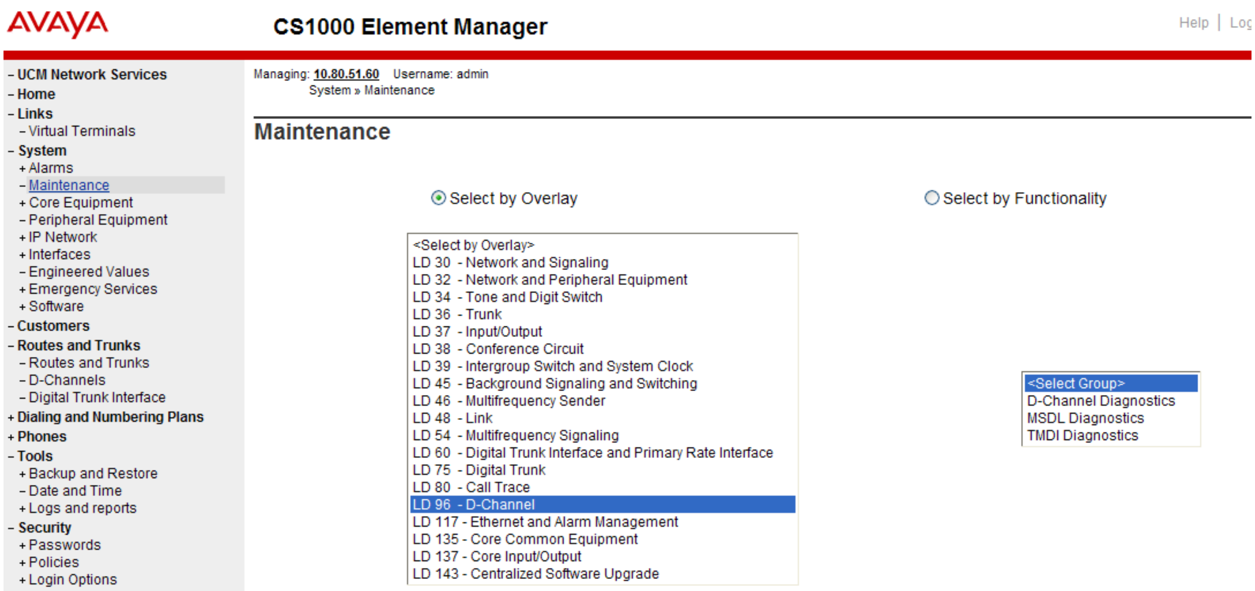
8. Service Provider Configuration

The configuration of Gamma's equipment used to support the IPConnect SIP trunk service is outside of the scope for these Application Notes and will not be covered. To obtain further information on Gamma's equipment and system configuration please contact an authorised Gamma representative.

9. Verification

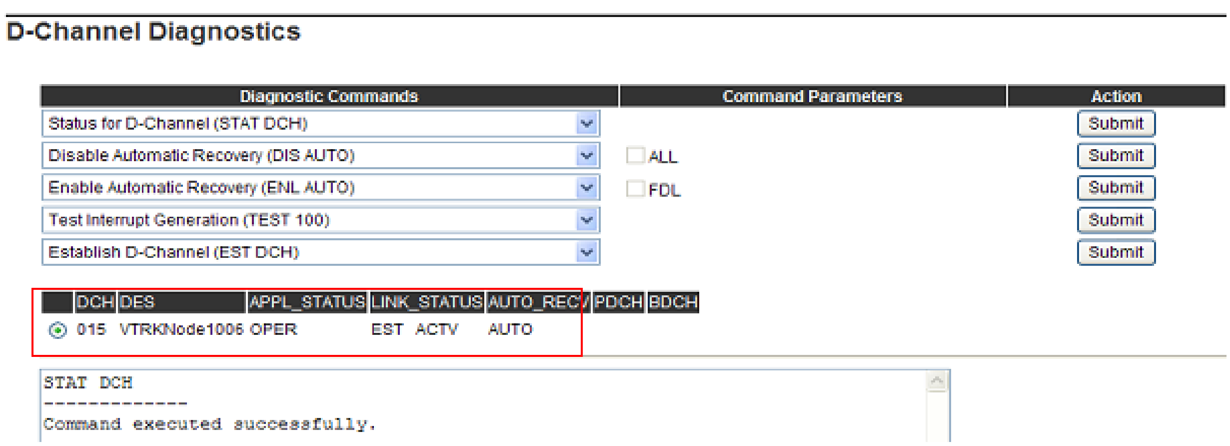
9.1. Verify Avaya Communication Server 1000E Operational Status

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



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

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

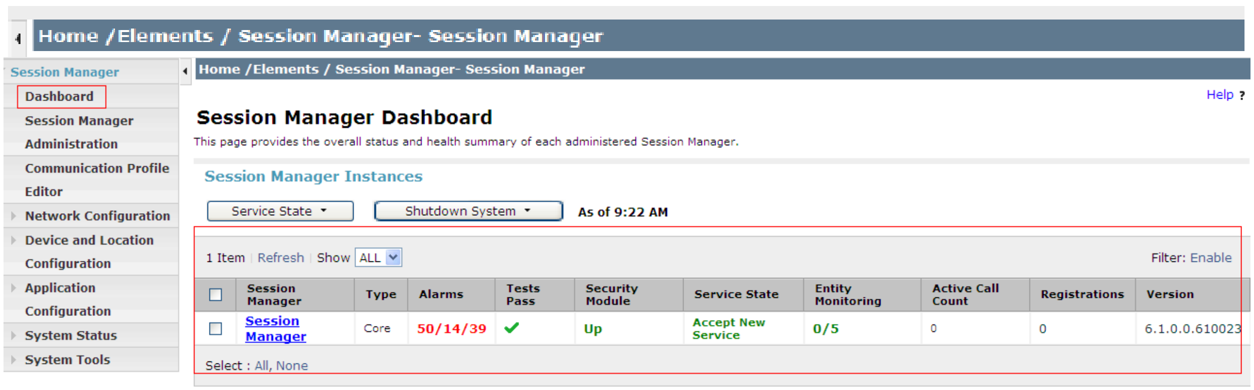


9.2. Verify Avaya Aura® Session Manager Operational Status

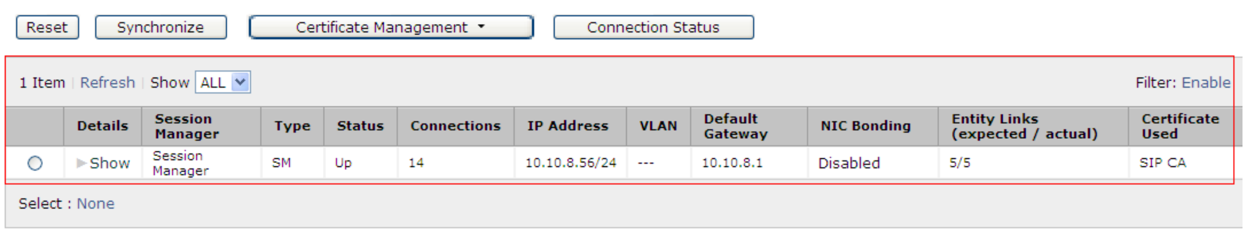
9.2.1. Verify Avaya Aura® Session Manager is Operational

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

- Tests Pass
- Security Module
- Service State

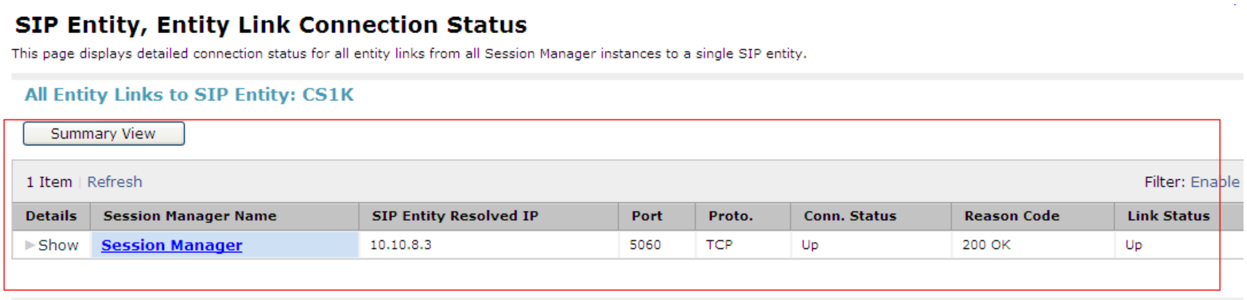


Navigate to **Elements → Session Manager → System Status → Security Module Status** (not shown) to view more detailed status information on the status of Security Module for the specific Session Manager. Verify the **Status** column displays **Up** as shown below.

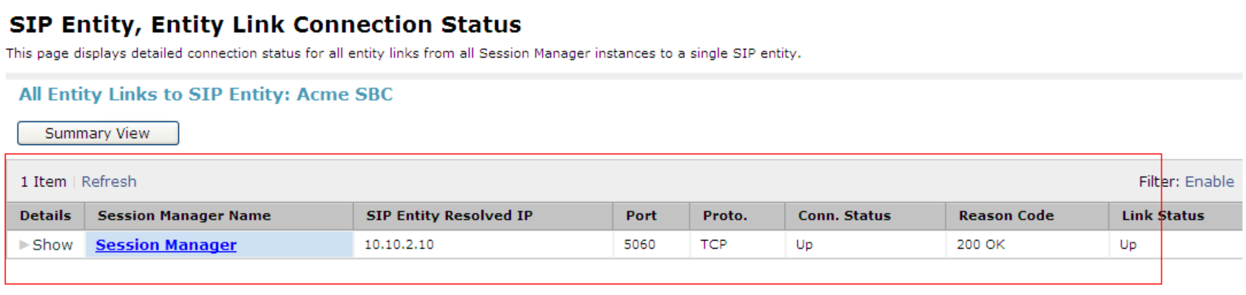


9.2.2. Verify SIP Entity Link Status

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



Verify the SIP link is up between the Session Manager and the Acme SBC by going through the same process as outlined above but selecting the SIP Entity for the Acme SBC in the **All Monitored SIP Entities** table.



10. Conclusion

These Application Notes describe the configuration necessary to connect the Avaya Communication Server 1000E, Avaya Aura® Session Manager and Acme Packet 3800 Net-Net Session Director to Gamma's IPConnect SIP Service. The IPConnect SIP Trunk Service is a SIP-based Voice over IP solution providing businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks.

11. Additional References

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

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

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

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

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

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

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

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

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

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

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

Product documentation for the Session Director can be obtained from Acme Packet's support web site https://support.acmepacket.com. (login required)

[11] Net-Net Session Director Installation Guide, Acme Packet Documentation Set.

[12] Net-Net 4000 ACLI Configuration Guide, Release Version S-C6.1.0, Acme Packet Documentation Set.

[13] Net-Net 4000 ACLI Reference Guide, Release Version S-C6.1.0, Acme Packet Documentation Set

Appendix A – Avaya Communication Server 1000E Software

Communication Server 1000E call server patches and plug ins

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

VERSION 4021

System type is - Communication Server 1000E/CP PM

CP PM - Pentium M 1.4 GHz

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

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

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

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

Communication Server 1000E call server deplists

```
VERSION 4121
RELEASE 7
ISSUE 50 Q +
DepList 1: core Issue: 01 (created: 2011-05-24 10:13:35 (est)) ALTERED

IN-SERVICE PEPS
PAT# CR #          PATCH REF #    NAME      DATE        FILENAME       SPECINS
012  wi00843623    ISS1:1OF1      p30731_1  16/06/2011  p30731_1.cpl   YES
013  WI00843571    ISS1:1OF1      p30627_1  16/06/2011  p30627_1.cpl   NO
014  wi00871739    ISS1:1OF1      p30856_1  16/06/2011  p30856_1.cpl   NO
015  wi00852365    ISS1:1OF1      p30707_1  16/06/2011  p30707_1.cpl   NO
016  wi00852389    ISS1:1OF1      p30641_1  16/06/2011  p30641_1.cpl   NO
017  wi00839134    ISS1:1OF1      p30698_1  16/06/2011  p30698_1.cpl   YES
018  wi00856702    ISS1:1OF1      p30573_1  16/06/2011  p30573_1.cpl   NO
019  wi00857566    ISS1:1OF1      p30766_1  16/06/2011  p30766_1.cpl   NO
020  wi00850521    ISS1:1OF1      p30709_1  16/06/2011  p30709_1.cpl   YES
021  wi00860722    ISS1:1OF1      p30784_1  16/06/2011  p30784_1.cpl   YES
022  wi00863876    ISS1:1OF1      p30787_1  16/06/2011  p30787_1.cpl   NO
023  WI00853473    ISS1:1OF1      p30625_1  16/06/2011  p30625_1.cpl   NO
024  wi00854130    ISS1:1OF1      p30443_1  16/06/2011  p30443_1.cpl   NO
025  wi00875425    ISS1:1OF1      p30943_1  16/06/2011  p30943_1.cpl   NO
026  wi00853658    ISS1:1OF1      p30990_1  16/06/2011  p30990_1.cpl   NO
027  wi00875701    ISS1:1OF1      p30942_1  16/06/2011  p30942_1.cpl   NO
028  wi00853031    ISS1:1OF1      p30531_1  16/06/2011  p30531_1.cpl   NO
029  wi00877367    ISS1:1OF1      p30534_1  16/06/2011  p30534_1.cpl   NO
030  wi00871969    ISS1:1OF1      p30768_1  16/06/2011  p30768_1.cpl   NO
031  wi00886321    ISS1:1OF1      p31009_1  16/06/2011  p31009_1.cpl   NO
032  WI00836334    ISS1:1OF1      p30481_1  16/06/2011  p30481_1.cpl   NO
033  wi00836182    ISS1:1OF1      p30450_1  16/06/2011  p30450_1.cpl   NO
034  wi00858335    ISS1:1OF1      p30819_1  16/06/2011  p30819_1.cpl   NO
035  wi00860279    ISS1:1OF1      p30789_1  16/06/2011  p30789_1.cpl   NO
036  wi00866570    ISS1:1OF1      p30477_1  16/06/2011  p30477_1.cpl   NO
037  wi00854415    ISS1:1OF1      p30593_1  16/06/2011  p30593_1.cpl   NO
038  WI00836292    ISS1:1OF1      p30554_1  16/06/2011  p30554_1.cpl   NO
```

```
039  WI00839794      ISS1:1OF1       p28647_1  16/06/2011  p28647_1.cpl   NO
040  wi00824257      ISS1:1OF1       p30447_1  16/06/2011  p30447_1.cpl   NO
041  wi00827950      ISS2:1OF1       p30471_2  16/06/2011  p30471_2.cpl   NO
042  wi00879814      ISS1:1OF1       p30970_1  16/06/2011  p30970_1.cpl   NO
043  WI00854150      ISS1:1OF1       p30468_1  16/06/2011  p30468_1.cpl   NO
044  wi00873382      ISS1:1OF1       p30832_1  16/06/2011  p30832_1.cpl   NO
045  wi00853178      ISS1:1OF1       p30719_1  16/06/2011  p30719_1.cpl   NO
046  wi00869695      ISS1:1OF1       p30654_1  16/06/2011  p30654_1.cpl   NO
047  wi00834382      ISS1:1OF1       p30548_1  16/06/2011  p30548_1.cpl   NO
048  wi00836472      ISS1:1OF1       p30626_1  16/06/2011  p30626_1.cpl   NO
049  wi00854409      ISS1:1OF1       p30479_1  16/06/2011  p30479_1.cpl   NO
050  WI00728461      ISS1:1OF1       p30346_1  16/06/2011  p30346_1.cpl   NO
MDP>LAST SUCCESSFUL MDP REFRESH :2011-05-25 10:18:44(Local Time)
MDP>USING DEPLIST ZIP FILE DOWNLOADED :2011-05-25 04:41:04(est)
```

Communication Server 1000E signaling server service updates

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

Communication Server 1000E system software

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

```
   sps                          7.50.17     [patched]
   ncs                          7.50.17
   gk                           7.50.17
   EmConfig                     7.50.17
   emWeb_6-0                    7.50.17     [patched]
   emWebLocal_6-0               7.50.17
   csmWeb                       7.50.17
   bcc                          7.50.17     [patched]
   ftrpkg                       7.50.17
   cs1000WebService_6-0         7.50.17
   managedElementWebService     7.50.17
   mscAnnc                      7.50.17
   mscAttn                      7.50.17
   mscConf                      7.50.17
   mscMusc                      7.50.17
   mscTone                      7.50.17
```

Appendix B: Acme Packet Session Director Configuration File

Included below is the Acme Packet Session Director configuration file used during the compliance testing. The contents of the configuration can be shown by using the **show running-config** command.

```
acmesystem# sh running
host-routes
        dest-network                xx.xx.xx.xx
        netmask                        255.255.255.0
        gateway                        xx.xx.xx.xx
        description                    route-to-gamma
        last-modified-by               admin@console
        last-modified-date             2011-05-26 07:47:37
host-routes
        dest-network                   10.10.8.0
        netmask                        255.255.255.0
        gateway                        10.10.2.1
        description
        last-modified-by               admin@console
        last-modified-date             2011-05-26 10:09:04
local-policy
        from-address
                                       *
        to-address
                                       *
        source-realm
                                       OUTSIDE
        description                    Far-side-realm
        activate-time                  N/A
        deactivate-time                N/A
        state                          enabled
        policy-priority                none
        last-modified-by               admin@console
        last-modified-date             2011-05-26 07:25:20
        policy-attribute
                next-hop                       10.10.8.56
                realm                          INSIDE
                action                         none
                terminate-recursion            disabled
                carrier
                start-time                     0000
                end-time                       2400
                days-of-week                   U-S
                cost                           0
                app-protocol
                state                          enabled
                methods
                media-profiles
local-policy
        from-address
                                       *
        to-address
                                       *
```

```
        source-realm
                                       INSIDE
        description
        activate-time                  N/A
        deactivate-time                N/A
        state                          enabled
        policy-priority                none
        last-modified-by               admin@console
        last-modified-date             2011-05-26 07:24:29
        policy-attribute
                next-hop                       xx.xx.xx.xx
                realm                          OUTSIDE
                action                         none
                terminate-recursion            disabled
                carrier
                start-time                     0000
                end-time                       2400
                days-of-week                   U-S
                cost                           0
                app-protocol
                state                          enabled
                methods
                media-profiles
media-profile
        name                           PCMA
        subname
        media-type                     audio
        payload-type                   8
        transport                      RTP/AVP
        req-bandwidth                  0
        frames-per-packet              0
        parameters
        average-rate-limit             0
        sdp-rate-limit-headroom        0
        sdp-bandwidth                  disabled
        police-rate                    0
        last-modified-by               admin@10.10.2.110
        last-modified-date             2011-06-20 03:21:49
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                        unique-sdp-id
        red-flow-port                  1985
        red-mgcp-port                  1986
        red-max-trans                  10000
        red-sync-start-time            5000
```

```
        red-sync-comp-time              1000
        media-policing                  enabled
        max-signaling-bandwidth         10000000
        max-untrusted-signaling         100
        min-untrusted-signaling         30
        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@10.10.2.110
        last-modified-date              2011-06-17 07:45:01
network-interface
        name                            S0P1
        sub-port-id                     0
        description                     INSIDE
        hostname
        ip-address                      10.10.2.10
        pri-utility-addr
        sec-utility-addr
        netmask                         255.255.255.0
        gateway                         10.10.2.1
        sec-gateway
        gw-heartbeat
                state                           enabled
                heartbeat                       10
                retry-count                     3
                retry-timeout                   1
                health-score                    30
        dns-ip-primary
        dns-ip-backup1
        dns-ip-backup2
        dns-domain
        dns-timeout                     11
        hip-ip-list                     10.10.2.10
        ftp-address                     10.10.2.10
        icmp-address                    10.10.2.10
        snmp-address                    10.10.2.10
        telnet-address                  10.10.2.10
        last-modified-by                admin@console
        last-modified-date              2011-05-20 03:26:11
network-interface
        name                            S0P0
        sub-port-id                     0
        description                     OUTSIDE
        hostname
        ip-address                      xx.xx.xx.xx
```

```
        pri-utility-addr
        sec-utility-addr
        netmask                         255.255.255.128
        gateway                         xx.xx.xx.xx
        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                     xx.xx.xx.xx
        ftp-address
        icmp-address                    xx.xx.xx.xx
        snmp-address
        telnet-address
        last-modified-by                admin@console
        last-modified-date              2011-05-25 08:51:18
phy-interface
        name                            S0P0
        operation-type                  Media
        port                            0
        slot                            0
        virtual-mac
        admin-state                     enabled
        auto-negotiation                enabled
        duplex-mode                     FULL
        speed                           100
        last-modified-by                admin@console
        last-modified-date              2011-03-22 05:22:58
phy-interface
        name                            S0P1
        operation-type                  Media
        port                            1
        slot                            0
        virtual-mac
        admin-state                     enabled
        auto-negotiation                enabled
        duplex-mode                     FULL
        speed                           100
        last-modified-by                admin@135.64.186.34
        last-modified-date              2011-03-22 07:50:27
realm-config
        identifier                      OUTSIDE
        description                     SIP_LAB_OUTSIDE
        addr-prefix                     0.0.0.0
        network-interfaces
                                        S0P0:0
        mm-in-realm                     enabled
        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      none
        invalid-signal-threshold        0
        maximum-signal-threshold        0
        untrusted-signal-threshold      0
        nat-trust-threshold             0
        deny-period                     30
        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@console
        last-modified-date             2011-05-26 09:13:02
realm-config
        identifier                     INSIDE
        description                    SIP_LAB_INSIDE
        addr-prefix                    0.0.0.0
        network-interfaces
                                       S0P1:0
        mm-in-realm                    enabled
        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     none
        invalid-signal-threshold       0
        maximum-signal-threshold       0
        untrusted-signal-threshold     0
        nat-trust-threshold            0
        deny-period                    30
        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@console
        last-modified-date             2011-05-26 09:13:25
session-agent
        hostname                       xx.xx.xx.xx
        ip-address                     xx.xx.xx.xx
        port                           5060
        state                          enabled
        app-protocol                   SIP
        app-type
        transport-method               UDP
        realm-id                       OUTSIDE
        egress-realm-id
        description                    Gamma
        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                  120
        ping-send-mode                 keep-alive
        ping-in-service-response-codes
        out-service-response-codes
        media-profiles
        in-translationid
        out-translationid              SIPGAM
        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             SIPGAM
        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              NONE
        tcp-keepalive                  none
        tcp-reconn-interval            0
        max-register-burst-rate        0
        register-burst-window          0
        last-modified-by               admin@10.10.2.110
        last-modified-date             2011-06-20 04:23:11
session-agent
        hostname                       10.10.8.56
        ip-address                     10.10.8.56
        port                           5060
        state                          enabled
        app-protocol                   SIP
        app-type
        transport-method               UDP+TCP
        realm-id                       INSIDE
        egress-realm-id
        description                    SM100
        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                  120
        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             SIPGAM
        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              NONE
        tcp-keepalive                  none
        tcp-reconn-interval            0
        max-register-burst-rate        0
        register-burst-window          0
        last-modified-by               admin@10.10.2.110
        last-modified-date             2011-06-20 04:17:44
sip-config
        state                          enabled
        operation-mode                 dialog
        dialog-transparency            enabled
        home-realm-id                  INSIDE
        egress-realm-id
        nat-mode                       None
```

```
        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
        add-ucid-header               disabled
        proxy-sub-events
        last-modified-by              admin@console
        last-modified-date            2011-03-22 05:44:50
sip-interface
        state                         enabled
        realm-id                      OUTSIDE
        description                   SIP_LAB_outside
        sip-port
                address                       xx.xx.xx.xx
                port                          5060
                transport-protocol            UDP
                tls-profile
                allow-anonymous               all
                ims-aka-profile
        carriers
        trans-expire                  0
        invite-expire                 0
        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                         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                  invite
        add-sdp-profiles                PCMA
        last-modified-by                admin@10.10.2.110
        last-modified-date              2011-06-20 03:22:30
sip-interface
        state                           enabled
        realm-id                        INSIDE
        description                     Avaya-SBC
        sip-port
                address                         10.10.2.10
                port                            5060
                transport-protocol              TCP
                tls-profile
                allow-anonymous                 all
```

```
                ims-aka-profile
        carriers
        trans-expire                   0
        invite-expire                  0
        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               disabled
        last-modified-by               admin@10.10.2.110
        last-modified-date             2011-06-20 02:11:26
sip-manipulation
        name                           SIPGAM
        description
        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@10.10.2.110
        last-modified-date             2011-06-20 04:04:18
steering-pool
        ip-address                     10.10.2.10
        start-port                     2048
        end-port                       3329
        realm-id                       INSIDE
        network-interface
        last-modified-by               admin@console
        last-modified-date             2011-05-26 07:16:43
steering-pool
        ip-address                     xx.xx.xx.xx
        start-port                     10000
        end-port                       20000
```

```
        realm-id                       OUTSIDE
        network-interface
        last-modified-by               admin@console
        last-modified-date             2011-05-26 07:17:24
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                10.10.2.1
        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@console
        last-modified-date             2011-05-25 08:33:36
task done
acmesystem#
```

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.