



Application Notes for Configuring Avaya Communication Server 1000E R7.5, Avaya Aura[®] Session Manager R6.1, Avaya Session Border Controller for Enterprise R4.0.5 to support Telenor SIP Trunk Service – Issue 1.0

Abstract

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

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

1. Introduction

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

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

2.1. Interoperability Compliance Testing

The interoperability test included the following:

- Incoming PSTN calls were made to Unistim, SIP, Digital and Analog telephones at the enterprise
- Incoming calls to the enterprise site from the PSTN routed to the DDI numbers assigned by Telenor
- Outgoing calls from the enterprise to the PSTN were made from Unistim, SIP, Digital and Analog telephones
- Outgoing calls from the enterprise site completed via Telenor to PSTN destinations
- G.729 and G.729 Annex b (silence suppression) are not supported by Telenor SIP Trunk Service and thus was not tested
- Calls using G.711A and G.711U codec's supported by Telenor
- Fax calls to/from a group 3 fax machine to a PSTN connected fax machine using the T.38 mode
- DTMF transmission using RFC 2833 with successful Voice Mail/Vector navigation for inbound and outbound calls
- User features such as hold and resume, transfer, conference, call forwarding, etc
- Coverage and call forwarding for endpoints at the enterprise site
- Caller ID Presentation and Caller ID Restriction

- No emergency calls were tested

2.2. Test Results

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

- Issue observed when testing Mobile X, extend call from host station to EC500 mobile. When incoming PSTN call is answered at twinned set and is handed off to EC500 mobile, the INVITE sent to the Service Provider contains no SDP information. The Signalling Server needed to be patched with Linux Patch MPLR30260 in order to populate the INVITE with the SDP information.
- Incoming calling number from PSTN is restricted. With restricted calls to UNIstim phones, P-Called-Party-ID is displayed. The INVITE header fields FROM and P-Asserted-Identity both are populated with “Anonymous”.
- No inbound toll free numbers were tested as none were available from the Service Provider
- No Emergency Services numbers were tested as test calls to these numbers should be pre-arranged with the Operator

2.3. Support

For technical support on Telenor products please contact the following website:

<http://www.telenor.com/>

3. Reference Configuration

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

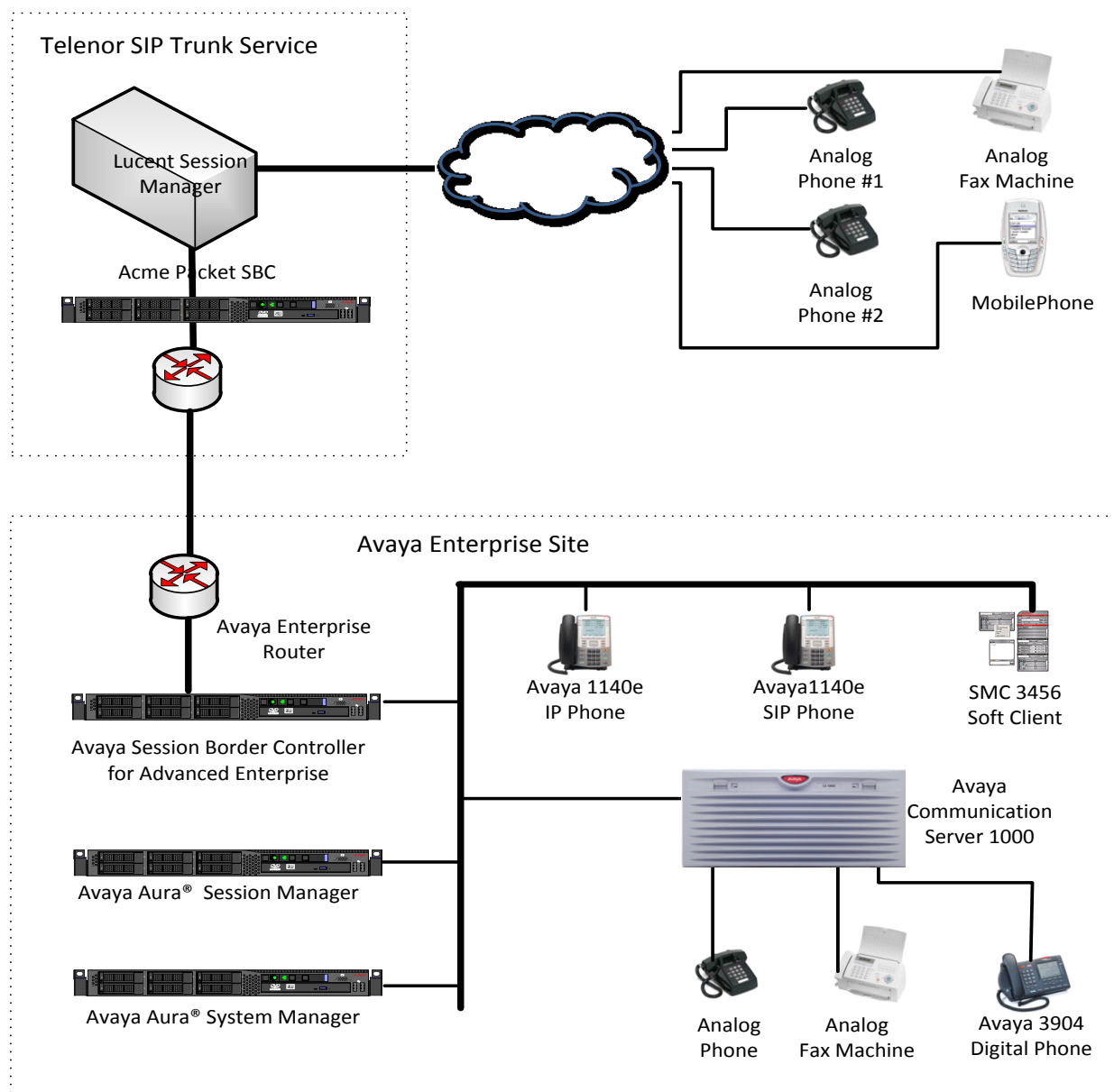


Figure 1: Telenor SIP Trunk Topology

4. Equipment and Software Validated

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

Equipment	Software
Avaya S8800 server	Avaya Aura® Session Manager R6.1 Build: 6.1.0.0.610023
Avaya S8800 server	Avaya Aura® System Manager R6.1 Load: 6.1.0.0.7345 Service Pack 6
Avaya Communication Server 1000E running on CP+PM server as co-resident configuration	Avaya Communication Server 1000E R7.5, Version 7.50.17 Service Update: 7.50_17Jan11 Deplist: X21 07.50Q
Avaya S8800 server	Avaya Session Border Controller for Enterprise Build: 4.0.5.Q02
Avaya Communication Server 1000E Media Gateway	CSP Version: MGCC CD01 MSP Version: MGCM AB01 APP Version: MGCA BA07 FPGA Version: MGCF AA18 BOOT Version: MGCB BA07 DSP1 Version: DSP1 AB03
Avaya 1140e and 1230 Unistim Telephones	FW: 0625C8A
Avaya 1140e and 1230 SIP Telephones	FW: 04.01.13.00.bin
Avaya SMC 3456	Version 2.6 build 53715
Avaya one-X® Communicator	Avaya one-X® Communicator -Version cs6.1.0.10
Avaya Analogue Telephone	N/A
Avaya M3904 Digital Telephone	N/A
Telenor SIP Trunk Service	ACME Net-Net 4250 Firmware SC6.1.0 MR-10 Patch 4 (Build 10002) Build date – 14/12/2011 Lucent Session Manager – 14.28.00.18 Telenor IPT Version 2.1.2.125

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 Telenor SIP Trunk Service. For incoming calls, the Session Manager receives SIP messages from the Avaya SBCE; through which Telenor 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 Avaya SBCE and on to Telenor's network. Specific Communication Server 1000E configuration was performed using Element Manager and the system terminal interface. The general installation of the Communication Server 1000E, System Manager and Session Manager is presumed to have been previously completed and is not discussed here.

5.1. Log into the Avaya Communication Server 1000E

Log in using SSH to the ELAN IP address of the Call Server using a user with correct privileges. Once logged in type **csconsole**, this will take the user into the vxworks shell of the call server. Next type **logi**, the user will then be asked to login with correct credentials. Once logged in the user can then progress to load any overlay.

5.2. Confirm System Features

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

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

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

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

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

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

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

5.3. Configure Codec's for Voice and FAX Operation

Telenor SIP Trunk service supports G.711A/U voice codec and T.38 FAX transmissions. Use the Communication Server 1000E element manager to configure the Voice and Fax properties. Navigate to the **IP Network → IP Telephony Nodes → Node Details → VGW Gateway (VGW) and Codecs** property page and configure the Communication Server 1000E General codec settings as in the next screenshot.

Node ID: 100 - Voice Gateway (VGW) and Codecs

[General](#) | [Voice Codecs](#) | [Fax](#)

General

Echo cancellation: ☒ Use canceller, with tail delay:
☒ Dynamic attenuation

Voice activity detection threshold: (-20 - +10 DBM)

Idle noise level: (-327 - +327 DBM)

Signaling options: ☒ DTMF tone detection
☐ Low latency mode
☒ Remove DTMF delay (squench DTMF from TDM to IP)
☒ Modem/Fax pass-through
☒ V.21 Fax tone detection
☐ R factor calculation

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

Node ID: 100 - Voice Gateway (VGW) and Codecs

General | Voice Codecs | Fax

Voice Codecs

Codec G711: ☒ Enabled (required)

Voice payload size: 20 (milliseconds per frame)

Voice playout (jitter buffer) delay: 40 80 (milliseconds)

Nominal Maximum

Maximum delay may be automatically adjusted based on nominal settings.

☐ Voice Activity Detection (VAD)

Codec G722: ☐ Enabled

Voice payload size: 20 (milliseconds per frame)

Voice playout (jitter buffer) delay: 40 80 (milliseconds)

Nominal Maximum

Maximum delay may be automatically adjusted based on nominal settings.

Configure the **Fax** settings as in the highlighted section of the next screenshot.

Node ID: 100 - Voice Gateway (VGW) and Codecs

General | Voice Codecs | Fax

Codec G723.1: ☐ Enabled

Voice payload size: 30 (milliseconds per frame)

Voice playout (jitter buffer) delay: 60 120 (milliseconds)

Nominal Maximum

Maximum delay may be automatically adjusted based on nominal settings.

Coding rate: 5.3 (kbps)

Fax

Codec name: T.38 FAX

Maximum rate: 14400 (bps)

Fax TCF method: 2

Fax playout nominal delay: 100 (0 - 300 milliseconds)

FAX no activity timeout: 20 (10 - 32000 milliseconds)

Packet size: 30 (bps)

* Required Value.

Note: Changes made on this page will NOT be transmitted until the Node is also saved.

Save Cancel

5.4. Virtual Trunk Gateway Configuration

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

Managing: 192.168.1.5 Username: admin
System » IP Network » IP Telephony Nodes » Node Details

Node Details (ID: 100 - SIP Line, LTPS, Gateway (SIPGw))

Node ID: * (0-9999)

Call server IP address: *

TLAN address type: ☒ IPv4 only
☐ IPv4 and IPv6

Embedded LAN (ELAN)
Gateway IP address: *
Subnet mask: *

Telephony LAN (TLAN)
Node IPv4 address: *
Subnet mask: *

Node IPv6 address:

* Required Value. Save Cancel

Associated Signaling Servers & Cards

Select to add ▼ Add Remove Make Leader Print | Refresh

<input type="checkbox"/> Hostname ▲	Type	Deployed Applications	ELAN IP	TLAN IPv4	Role
<input type="checkbox"/> cs1kv3	Signaling_Server	SIP Line, LTPS, Gateway, PD, Presence Publisher, IP Media Services	192.168.1.5	10.10.3.5	Leader

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

- **Vtrk gateway application:** Provides option to select Gateway applications. The three supported modes are **SIP Gateway (SIPGw)**, **H.323Gw**, and **SIPGw and H.323Gw**. **SIPGw was used in the test configuration**
- **SIP domain name:** The SIP domain name configured in this section must match the SIP domain name configured in the Session Manager **Section 6.1**
- **Local SIP port:** The local SIP port is the port to which the gateway listens. The default value is **5060**
- **Gateway endpoint name:** This field cannot be left blank so a value is needed here. This field is used when a Network Routing Server is used for registration of the endpoint. In this network a Session Manager is used so any value can be put in here and will not be used
- **Application node ID:** This is a unique value that can be alphanumeric and is for the new Node that is being created, in this case **100**
- **Under the heading Proxy or Redirect Server:** **Primary TLAN IP address** is the SIP signalling interface IP address of 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.

Node ID: 100 - Virtual Trunk Gateway Configuration Details

[General](#) | [SIP Gateway Settings](#) | [SIP Gateway Services](#)

Vtrk gateway application: ☒ Enable gateway service on this node

General

Vtrk gateway application: *
 SIP domain name: *
 Local SIP port: * (1 - 65535)
 Gateway endpoint name: *
 Gateway password: *
 Application node ID: * (0-9999)
 Enable failsafe NRS: ☐
 SIP ANAT: ☒ IPv4
☐ IPv6

Virtual Trunk Network Health Monitor

☐ Monitor IP addresses (listed below)
 Information will be captured for the IP addresses listed below.
 Monitor IP:
 Monitor addresses:

Proxy Or Redirect Server:

Proxy Server Route 1:

Primary TLAN IP address:
The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"
 Port: (1 - 65535)
 Transport protocol:
 Options: ☐ Support registration
☐ Primary CDS proxy

SIP URI Map:

Public E.164 domain names	Private domain names
National: <input type="text"/>	UDP: <input type="text" value="udp"/>
Subscriber: <input type="text" value="subscriber"/>	CDP: <input type="text" value="cdp.udp"/>
Special number: <input type="text" value="PublicSpecial"/>	Special number: <input type="text" value="PrivateSpecial"/>
Unknown: <input type="text" value="PublicUnknown"/>	Vacant number: <input type="text" value="PrivateUnknown"/>
	Unknown: <input type="text"/>

5.5. Configure Bandwidth Zones

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

Managing: 192.168.1.5 Username: admin
System » IP Network » Zones » Bandwidth Zones

Bandwidth Zones

Add... Edit... Import... Export Maintenance... Delete

Zone *	Intrazone Bandwidth	Intrazone Strategy	Interzone Bandwidth	Interzone Strategy	Resource Type	Zone Intent	Description
1 <input type="radio"/> 1	1000000	BQ	1000000	BQ	SHARED	VTRK	
2 <input type="radio"/> 2	1000000	BQ	1000000	BQ	SHARED	MO	

5.6. Configure Incoming Digit Conversion Table

A limited number of Direct Dial Inwards (DDI) numbers were available. The 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.

Digit Conversion Tree 0 Configuration

Regular IDC tree
Send calling party DID disabled

Add... Delete IDC Delete IDC tree

Incoming Digits *	Converted Digits	CPND Name	CPND language
1 <input type="radio"/> 22	5000		
2 <input type="radio"/> 22	5003		
3 <input type="radio"/> 22	5005		

5.7. Configure SIP Trunks

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

- Configure a D-Channel Handler (**DCH**); configure using the Communication Server 1000E system terminal and overlay 17
- Configure a SIP trunk Route Data Block (**RDB**); configure using the Communication Server 1000E system terminal and overlay 16
- Configure SIP trunk members; configure using the Communication Server 1000E system terminal and overlay 14
- Configure a Digit Manipulation Data Block (**DGT**), configure using the Communication Server 1000E system terminal and overlay 86
- Configure a Route List Block (**RLB**); configure using the Communication Server 1000E system terminal and overlay 86
- Configure Co-ordinated Dialling Plan(s) (**CDP**); configure using the Communication Server 1000E system terminal and overlay 87

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

```
Overlay 17
ADAN      DCH 1
CTYP DCIP
DES  VIR TRK
USR  ISLD
ISLM 4000
SSRC 3700
OTBF 32
NASA YES
IFC  SL1
CNEG 1
RLS  ID 4
RCAP ND2
MBGA NO
H323
OVLR NO
OVLS NO
```

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

Overlay 16 TYPE: RDB CUST 00 ROUT 1 TYPE RDB CUST 00 ROUT 1 DES VIR_TRK TKTP TIE NPID_TBL_NUM 0 ESN NO RPA NO CNVT NO SAT NO RCLS EXT VTRK YES ZONE 00001 PCID SIP CRID NO NODE 100 DTRK NO ISDN YES MODE ISLD DCH 1 IFC SL1 PNI 00000 NCNA YES NCRD YES TRO NO FALT NO CTYP UKWN INAC NO ISAR NO DAPC NO MBXR NO MBXOT NPA MBXT 0 PTYP ATT CNDP UKWN AUTO NO DNIS NO DCDR NO ICOG IAO SRCH LIN TRMB YES STEP	ACOD 1111 TCPP NO PII NO AUXP NO TARG CLEN 1 BILN NO OABS INST IDC YES DCNO 0 NDNO 0 * DEXT NO DNAM NO SIGO STD STYP SDAT MFC NO ICIS YES OGIS YES TIMR ICF 1920 OGF 1920 EOD 13952 LCT 256 DSI 34944 NRD 10112 DDL 70 ODT 4096 RGV 640 GTO 896 GTI 896 SFB 3 PRPS 800 NBS 2048 NBL 4096 IENB 5 TFD 0 VSS 0 VGD 6 EESD 1024 SST 5 0 DTD NO SCDT NO 2 DT NO NEDC ORG FEDC ORG	CPDC NO DLTN NO HOLD 02 02 40 SEIZ 02 02 SVFL 02 02 DRNG NO CDR NO NATL YES SSL CFWR NO IDOP NO VRAT NO MUS YES MRT 21 PANS YES RACD NO MANO NO FRL 0 0 FRL 1 0 FRL 2 0 FRL 3 0 FRL 4 0 FRL 5 0 FRL 6 0 FRL 7 0 OHQ NO OHQT 00 CBQ NO AUTH NO TTBL 0 ATAN NO OHTD NO PLEV 2 OPR NO ALRM NO ART 0 PECL NO DCTI 0 TIDY 1600 100 ATRR NO TRRL NO SGRP 0 ARDN NO CTBL 0 AACR NO
---	--	---

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

```

Overlay 14
TN    100 0 0 0
DATE
PAGE
DES   VIR_TRK
TN    100 0 00 00  VIRTUAL
TYPE IPTI
CDEN  8D
CUST  0
XTRK VTRK
ZONE  00001
TIMP  600
BIMP  600
AUTO_BIMP NO
NMUS  NO
TRK   ANLG
NCOS  0
RTMB 1 1
CHID  1
TGAR  1
STRI/STRO IMM IMM
SUPN  YES
AST   NO
IAPG  0
CLS   UNR DIP CND ECD WTA LPR APN THFD XREP SPCD MSBT
      P10 NTC
TKID
AACR  NO

```

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

Overlay 86

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

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

Overlay 86

```
CUST 0
FEAT rlb
RLI 10
ELC NO
ENTR 0
LTER NO
ROUT 1
TOD 0 ON 1 ON 2 ON 3 ON
    4 ON 5 ON 6 ON 7 ON
VNS NO
SCNV NO
CNV NO
EXP NO
FRL 0
DMI 10
CTBL 0
ISDM 0
```

```
FCI 0
FSNI 0
BNE NO
DORG NO
SBOC NRR
PROU 1
IDBB DBD
IOHQ NO
OHQ NO
CBQ NO
```

```
ISSET 0
NALT 5
MFRL 0
OVLL 0
```

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

```
TSC 00353
FLEN 0
RRPA NO
RLI 10
CCBA NO
```

```
TSC 18
FLEN 0
RRPA NO
RLI 10
CCBA NO
```

```
TSC 800
FLEN 0
RRPA NO
RLI 10
CCBA NO
```

```
TSC 08
FLEN 0
RRPA NO
RLI 10
CCBA NO
```


5.8. Configure Analog, Digital and IP Telephones

A variety of telephone types were used during the testing, the following is the configuration for the Avaya 1140e Unistim IP telephone. Load **Overlay 20** at the system terminal and enter the following values. A unique five digit number is entered for the **KEY 00** and **KEY 01** value. The value for **CFG_ZONE** is the same value used in **Section 5.5** for **VIRTUALSETS**.

Overlay 20 IP Telephone configuration

```
DES 1140
TN 100 0 01 0 VIRTUAL
TYPE 1140
CDEN 8D
CTYP XDLC
CUST 0
NUID
NHTN
CFG_ZONE 00002
CUR_ZONE 00002
ERL 0
ECL 0
FDN 0
TGAR 0
LDN NO
NCOS 0
SGRP 0
RNPG 1
SCI 0
SSU
LNRS 16
XLST
SCPW
SFLT NO
CAC_MFC 0
CLS UNR FBA WTA LPR PUA MTD FNA HTA TDD HFA CRPD
    MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
    POD SLKD CCSD SWD LNA CNDA
    CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBF
    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 CCBF RTDD RBDD RBHD PGND OCBF FLXD FTTC DNDY DNO3 MCBN
    FDSF 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 5000 0      MARP
      CPND
        CPND_LANG ROMAN
        NAME IP1140
        XPLN 10
        DISPLAY_FMT FIRST, LAST
01 MCR 5000 0
      CPND
        CPND_LANG ROMAN
        NAME IP1140
        XPLN 10
        DISPLAY_FMT FIRST, LAST
02
03 BSY
04 DSP
05
06
07
08
09
10
11
12
13
14
15
16
17 TRN
18 AO6
19 CFW 16
20 RGA
21 PRK
22 RNP
23
24 PRS
25 CHG
26 CPN
```

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

Overlay 20 - Digital Set configuration

```
TYPE: 3904
DES 3904
TN 04 0 02 00 VIRTUAL
TYPE 3904
CDEN 8D
CTYP XDLC
CUST 0
MRT
ERL 0
FDN 0
TGAR 0
LDN NO
NCOS 0
SGRP 0
RNPG 1
SCI 0
SSU
LNRS 16
XLST
SCPW
SFLT NO
CAC_MFC 0
CLS UNR FBD WTA LPR PUA MTD FND HTD TDD HFA GRLD CRPA STSD
    MWA LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
    POD SLKD CCSD SWD LNA CNDA
    CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBF
    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 HBTB AHA IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
    DRDD EXR0
    USMD USRD ULAD CCBF RTDD RBDD RBHD PGND OCBD FLXD FTTC DNDY DNO3 MCBN
    FDSD NOVD CDMR PRED RECA MCDD T87D SBMD PKCH CROD CROD
CPND_LANG ENG
RCO 0
HUNT
PLEV 02
PUID
DANI NO
SPID NONE
AST
IAPG 1
AACS
ACQ
ASID
SFNB
SFRB
USFB
CALB
FCTB
ITNA NO
DGRP
PRI 01
MLWU_LANG 0
```

---continued on next page---

---continued from previous page----

MLNG ENG

DNDR 0

KEY 00 MCR 5008 0 MARP

CPND

CPND_LANG ROMAN

NAME Digital Set

XPLN 10

DISPLAY_FMT FIRST, LAST

01 MCR 5008 0

CPND

CPND_LANG ROMAN

NAME Digital Set

XPLN 10

DISPLAY_FMT FIRST, LAST

02

03

04

05

06

07

08

09

10

11

12

13

14

15

16

17 TRN

18 AO6

19 CFW 16

20 RGA

21 PRK

22 RNP

23

24 PRS

25 CHG

26 CPN

27 CLT

28 RLT

29

30

31

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

Overlay 20 - Analog Telephone Configuration

```
DES 500
TN 04 0 03 00
TYPE 500
CDEN 4D
CUST 0
MRT

ERL 00000
WRLS NO
DN 5015
AST NO
IAPG 0
HUNT
TGAR 0
LDN NO
NCOS 0
SGRP 0
RNPG 0
XLST
SCI 0
SCPW
SFLT NO
CAC_MFC 0
CLS UNR DTN FBD XFD WTA THFD FND HTD ONS
LPR XRD AGRD CWD SWD MWD RMMD SMWD LPD XHD SLKD CCSD LND TVD
CFTD SFD MRD C6D CNID CLBD AUTU
ICDD CDMD LLCN EHTD MCTD
GPUD DPUD CFXD ARHD OVDD AGTD CLTD LDTD ASCD SDND
MBXD CPFA CPTA UDI RCC HBTD IRGD DDGA NAMA MIND
NRWD NRCD NROD SPKD CRD PRSD MCRD
EXR0 SHL SMSD ABDD CFHD DNDY DNO3
CWND USMD USRD CCB D BNRD OCB D 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
```

5.9. 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.

- **SIP Line Gateway Application:** Enable the SIP line service on the node, check the box to enable
- **SIP Domain Name:** This value must match that configured in **Section 6.1**
- **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**

The screenshot shows the AVAYA CS1000 Element Manager interface. The left sidebar contains a tree view with categories like UCM Network Services, Home, Links, System, Alarms, Maintenance, Core Equipment, Peripheral Equipment, IP Network, Nodes, Servers, Media Cards, Maintenance and Reports, Media Gateways, Zones, Host and Route Tables, Network Address Translation (NAT), QoS Thresholds, Personal Directories, Unicode Name Directory, Interfaces, Engineered Values, and Emergency Services. The main content area is titled 'CS1000 Element Manager' and has a 'Help' button. It features a tabbed interface with 'General', 'SIP Line Gateway Settings', and 'SIP Line Gateway Service' tabs. The 'General' tab is selected, displaying the 'SIP Line Gateway Settings' page. At the top, there's a checkbox for 'SIP Line Gateway Application' which is checked, with the text 'Enable gateway service on this node'. Below this, the 'General' section contains several input fields: 'SIP domain name' (avaya.com), 'SLG endpoint name' (cs1kv3), 'SLG Group ID' (empty), 'SLG Local Sip port' (5070), and 'SLG Local Tls port' (5071). To the right of the 'SLG Local Sip port' and 'SLG Local Tls port' fields, there are small text labels '(1 - 65535)'. On the far right, there's a 'Virtual Trunk Network Health Monitor' section with a checkbox for 'Monitor IP addresses (listed below)' and a text box for 'Monitor addresses' with 'Add' and 'Remove' buttons.

5.10. 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 5.5**. A unique telephone number is entered for value **KEY 00**. The value for **KEY 01** is comprised of the **UAPR** value and the telephone number used in **KEY 00**.

Overlay 20 - SIP Telephone Configuration

```
DES SIPD
TN 100 0 01 10 VIRTUAL
TYPE UEXT
CDEN 8D
CTYP XDLC
CUST 0
UXTY SIPL
MCCL YES
SIPN 1
SIP3 0
FMCL 0
TLSV 0
SIPU 5003
NDID 100
SUPR NO
SUBR DFLT MWI RGA CWI MSB
UXID
NUID 100
NHTN 100 0 01 10
CFG_ZONE 00002
CUR_ZONE 00002
ERL 0
ECL 0
VSIT NO
FDN
TGAR 0
LDN NO
NCOS 0
SGRP 0
RNPG 0
SCI 0
SSU
XLST
SCPW 1234
SFLT NO
CAC MFC 0
CLS UNR FBD WTA LPR MTD FNA HTA TDD HFD CRPD
MWD LMPN RMMD SMWD AAD IMD XHD IRD NID OLD VCE DRG1
POD SLKD CCSD SWD LND CNDA
CFTD SFD MRD DDV CNID CDCA MSID DAPA BFED RCBF
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 OCB D FLXD FTTC DNDY DNO3 MCBN
FDSD NOVD VOLA VOUD CDMR PRED RECD MCDD T87D SBMD ELMD MSNV FRA PKCH MWTD DVLD
CROD CROD
CPND_LANG ENG
RCO 0
HUNT
LHK 0
PLEV 02
PUID
DANI NO
AST
IAPG 0 *

AACS NO
ITNA NO
DGRP
MLWU_LANG 0
MLNG ENG
DNDR 0
KEY 00 SCR 5003 0 MARP
CPND
CPND_LANG ROMAN
NAME Sigma 1140
XPLN 11
DISPLAY_FMT FIRST, LAST*
01 HOT U 115003 MARP 0
02
03
04
05
06
07
08
09
10
11
12
13
14
15
16
17 TRN
18 AO6
19 CFW 16
20 RGA
21 PRK
22 RNP
23 *
24 PRS
25 CHG
26 CPN
27
28
29
30
31
```


5.11. Save Configuration

Expand **Tools** → **Backup and Restore** on the left navigation panel and select **Call Server**. Select **Backup** and click **Submit** to save configuration changes as shown below.

The screenshot shows the AVAYA CS1000 Element Manager web interface. On the left is a navigation tree with categories like 'Host and Route Tables', 'Network Address Translation', 'QoS Thresholds', 'Personal Directories', 'Unicode Name Directory', 'Interfaces', 'Engineered Values', 'Emergency Services', 'Software', 'Customers', 'Routes and Trunks', 'Dialing and Numbering Plans', 'Phones', and 'Tools'. The 'Tools' category is expanded, showing 'Backup and Restore' and 'Call Server'. The main content area is titled 'Call Server Backup'. At the top, it says 'Managing: 192.168.1.5 Username: admin' and 'Tools » Backup and Restore » Call Server Backup and Restore » Call Server Backup'. Below the title, there is an 'Action' dropdown menu set to 'Backup', and two buttons: 'Submit' (highlighted with a red box) and 'Cancel'.

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.

```
Backing up reten.bkp to "/var/opt/nortel/cs/fs/cf2/backup/single"  
Database backup Complete!  
TEMU207  
Backup process to local Removable Media Device ended successfully.
```

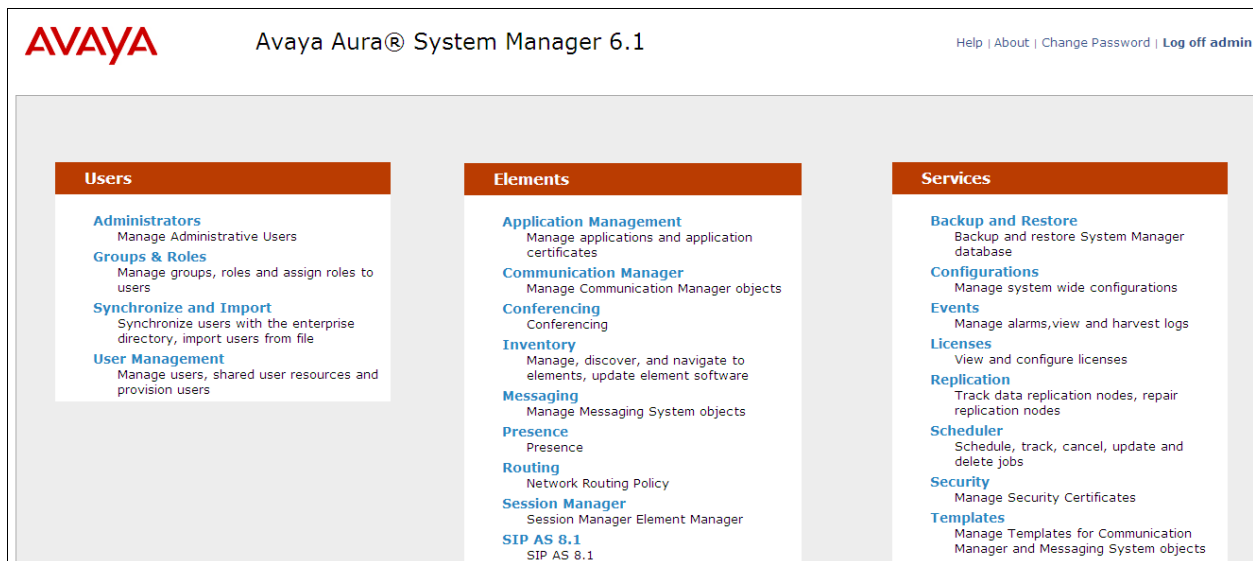
Configuration of Communication Server 1000E is complete.

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 Locations
- Configure Adaptation Module
- Define SIP Entities
- Define Entity Links
- Define Routing Policy
- Define Dial Pattern

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 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.

The screenshot shows the Avaya Aura System Manager 6.1 interface. The top header includes the Avaya logo, the title 'Avaya Aura™ System Manager 6.1', and links for 'Help', 'About', 'Change Password', and 'Log off admin'. The left navigation menu is expanded to 'Routing', and 'Domains' is selected. The main area is titled 'Domain Management' and contains a table with one item: 'avaya.com'. The table has columns for 'Name', 'Type', 'Default', and 'Notes'. The 'Name' column contains 'avaya.com', the 'Type' column contains 'sip', the 'Default' column has a checkbox, and the 'Notes' column is empty. There are 'Commit' and 'Cancel' buttons at the top right of the main area.

Name	Type	Default	Notes
* avaya.com	sip	<input type="checkbox"/>	

6.2. Define Locations

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, **10.10.3.*** was used
- **Notes** Add a brief description [Optional]

Click **Commit** to save. The screenshot below shows the Location defined in the sample configuration.

Routing / Home / Elements / Routing / Locations- Location Details

Location Details

Commit

General

* Name: SMGRVL3

Notes:

Overall Managed Bandwidth

Managed Bandwidth Units: Kbit/sec

Total Bandwidth:

Multimedia Bandwidth:

Audio Calls Can Take Multimedia Bandwidth: ☒

Per-Call Bandwidth Parameters

Maximum Multimedia Bandwidth (Intra-Location): 1000 Kbit/Sec

Maximum Multimedia Bandwidth (Inter-Location): 1000 Kbit/Sec

Minimum Multimedia Bandwidth: 64 Kbit/Sec

* Default Audio Bandwidth: 80 Kbit/sec

Location Pattern

Add Remove

3 Items Refresh Filter: Enable

IP Address Pattern	Notes
* 10.10.3.*	
* 10.10.9.*	
* 10.10.8.*	

Select : All, None

* Input Required

Commit Cancel

6.3. Configure Adaptation Module

To enable calls to be routed to stations on Communication Server 1000E, the Session Manager should be configured to use an Adaptation Module designed to remove digits before sending on to the Communication Server 1000E. As the number being sent from Telenor contained a + at the beginning of the calling id, the Communication Server 1000E cannot handle this and therefore this needs removing. Expand **Elements** → **Routing** and select **Adaptations** from the left navigational menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.

- **Adaptation name** Enter an identifier for the Adaptation Module
- **Module name** Select **DigitConversionAdapter** from drop-down menu
- **Module parameter** **MIME=no** → Strips MIME message bodies on egress from Session Manager

The screenshot shows the 'Adaptation Details' configuration page in the Session Manager. The left sidebar contains a navigation menu with 'Routing' selected. The main content area is titled 'Adaptation Details' and has a 'Commit' button in the top right. Under the 'General' tab, the following fields are visible: 'Adaptation name' (text input with value 'remove'), 'Module name' (drop-down menu with 'DigitConversionAdapter' selected), and 'Module parameter' (text input with value 'MIME=no'). Below these are 'Egress URI Parameters' and 'Notes' text input fields. A red rectangular box highlights the 'Adaptation name', 'Module name', and 'Module parameter' fields.

In the **Digit Conversion for Incoming Calls to SM** section, click **Add** and enter the following values.

- **Matching Pattern** Enter dialed prefix for calls to SIP endpoints registered to Session Manager. In the sample configuration, **+47** was used
- **Min** Enter minimum number of digits that must be dialed
- **Max** Enter maximum number of digits that may be dialed. In the sample configuration **16** was used
- **Delete Digits** Enter **3** to strip off +47
- **Address to modify** Select **both**

In the **Digit Conversion for Outgoing Calls to SM** section, click **Add** and enter the following values.

- **Matching Pattern** Enter dialed prefix for calls to SIP endpoints registered to Session Manager. In the sample configuration, **5** was used
- **Min** Enter minimum number of digits that must be dialed
- **Max** Enter maximum number of digits that may be dialed. In the sample configuration **16** was used
- **Delete Digits** Enter number of digits that may be deleted. In the sample configuration, **4** was used
- **Insert Digits** Enter number of digits to be added before the dialed number
+4722xxxxxx was used as this number required to be presented as CLID on outgoing calls
- **Address to Modify** Select **Both**

The following screenshot shows the Digit Conversion for incoming and outgoing calls defined in the sample configuration.

Digit Conversion for Incoming Calls to SM

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	* +47	* 3	* 16		* 3		both	

Select : All, None

Digit Conversion for Outgoing Calls from SM

Add Remove

1 Item Refresh Filter: Enable

<input type="checkbox"/>	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Notes
<input type="checkbox"/>	* 5	* 2	* 16		* 4	+4722xxxxxx	both	

Select : All, None

* Input Required

Commit Cancel

6.4. Define SIP Entities

A SIP Entity must be added for Communication Server 1000E and also for the Avaya SBCE. Expand **Elements** → **Routing** and select **SIP Entities** from the left navigation menu. Two 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 Avaya SBCE enter the private interface IP address
- **Type** Select **Other** for the Communication Server 1000E and **gateway** for the Avaya SBCE
- **Notes** Enter a brief description [Optional]
- **Adaptations** For the Avaya SBCE select the remove adaptor that was created in **Section 6.3**
- **Location** Select the Location defined for Communication Server 1000E in **Section 5.2** and also apply this same location to the Avaya SBCE

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 screenshot displays the 'SIP Entity Details' configuration page. The left navigation pane shows 'SIP Entities' selected. The main content area is titled 'SIP Entity Details' and includes a 'Commit' button in the top right. The 'General' tab is active, showing the following fields:

- Name:** CS1K
- FQDN or IP Address:** 10.10.3.6
- Type:** Other (dropdown)
- Notes:** (text area with a note: 'Additional notes with max. 255 characters.')
- Adaptation:** (dropdown)
- Location:** SMGRVL3 (dropdown)
- Time Zone:** Europe/Dublin (dropdown)

Below these fields, there are checkboxes for 'Override Port & Transport with DNS SRV' (unchecked) and 'SIP Timer B/F (in seconds):' (4). There is also a 'Credential name:' text field and a 'Call Detail Recording:' dropdown set to 'none'.

The 'SIP Link Monitoring' section at the bottom shows the 'SIP Link Monitoring:' dropdown set to 'Use Session Manager Configuration'.

The following screenshot shows the SIP Entity defined for Avaya SBCE in the sample configuration, note the adaption created in **Section 6.3** is associated with this entity link.

The screenshot displays the 'SIP Entity Details' configuration page for an entity named 'Sipera'. The page is part of a larger application with a sidebar menu on the left containing options like 'Routing', 'Domains', 'Locations', 'Adaptations', 'SIP Entities' (highlighted), 'Entity Links', 'Time Ranges', 'Routing Policies', 'Dial Patterns', 'Regular Expressions', and 'Defaults'. The main content area has a breadcrumb trail 'Home / Elements / Routing / SIP Entities- SIP Entity Details' and a 'Commit' button in the top right. The 'General' tab is active, showing fields for 'Name' (Sipera), 'FQDN or IP Address' (10.10.3.30), 'Type' (Gateway), 'Notes', 'Adaptation' (remove), 'Location' (SMGRVL3), and 'Time Zone' (Europe/Dublin). Below these fields are checkboxes for 'Override Port & Transport with DNS SRV' and 'SIP Timer B/F (in seconds)' (4), a 'Credential name' field, and a 'Call Detail Recording' dropdown (none). A 'SIP Link Monitoring' section at the bottom shows a dropdown set to 'Use Session Manager Configuration'. A red box highlights the 'Name', 'FQDN or IP Address', 'Type', 'Notes', 'Adaptation', 'Location', and 'Time Zone' fields.

Routing / Elements / Routing / SIP Entities- SIP Entity Details

SIP Entity Details

Commit

General

* Name: Sipera

* FQDN or IP Address: 10.10.3.30

Type: Gateway

Notes:

Adaptation: remove

Location: SMGRVL3

Time Zone: Europe/Dublin

Override Port & Transport with DNS SRV: ☐

* SIP Timer B/F (in seconds): 4

Credential name:

Call Detail Recording: none

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

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

6.5. 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 Avaya SBCE.

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/ Avaya SBCE in **Section 6.4**
- **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 Avaya Communication Server 1000E.

The screenshot shows the 'Entity Links' configuration page. The left navigation menu has 'Entity Links' selected. The main area displays a table with one entry. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Trusted, and Notes. The entry is for 'CS1K' with SIP Entity 1 as 'Session Manager', Protocol as 'TCP', Port as '5060', SIP Entity 2 as 'CS1K', Port as '5060', and Notes as 'toCS1K'. The 'Trusted' checkbox is checked.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Trusted	Notes
* CS1K	* Session Manager	TCP	* 5060	* CS1K	* 5060	<input checked="" type="checkbox"/>	toCS1K

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

The screenshot shows the 'Entity Links' configuration page. The left navigation menu has 'Entity Links' selected. The main area displays a table with one entry. The table has columns: Name, SIP Entity 1, Protocol, Port, SIP Entity 2, Port, Connection Policy, and Notes. The entry is for 'Sipera' with SIP Entity 1 as 'Session Manager', Protocol as 'TCP', Port as '5060', SIP Entity 2 as 'Sipera', Port as '5060', and Notes as 'toSipera'. The 'Connection Policy' is 'Trusted'. There is a red asterisk and the text 'Input Required' at the bottom left.

Name	SIP Entity 1	Protocol	Port	SIP Entity 2	Port	Connection Policy	Notes
* Sipera	* Session Manager	TCP	* 5060	* Sipera	* 5060	Trusted	toSipera

* Input Required

6.6. 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 policies for which calls will be routed to the Avaya SBCE and therefore to Telenor 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 Avaya Communication Server 1000E, select the SIP Entity associated with Communication Server 1000E defined in **Section 6.5** 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 Communication Server 1000E:

Routing Policy Details

Commit

General

* Name: toCS1K

Disabled: ☐

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Type	Notes
CS1K	10.10.3.6	Other	

For routing policy to the Avaya SBCE – Telenor SIP Trunk, select the SIP Entity associated with Avaya SBCE defined in **Section 6.5** 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 Avaya SBCE – Telenor SIP Trunk:

Routing Policy Details

General

* Name:

Disabled: ☐

Notes:

SIP Entity as Destination

Select

Name	FQDN or IP Address	Additional notes with max. 255 characters.	Type	Notes
Sipera	10.10.3.30		Gateway	

Commit

6.7. Define Dial Pattern

Dial Patterns are needed to route calls through Session Manager. For the compliance test, dial patterns were needed to route calls from Communication Server 1000E to Telenor and vice versa.

Dial Patterns define which route policy will be selected for a particular call based on the dialed digits, destination domain and originating location.

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 that will be matched against the Request URI of a call
- **Min** Enter the minimum number of digits that must to be dialed
- **Max** Enter the maximum number of digits that may be dialed
- **SIP Domain** Select the SIP domain from the 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 6.6**

Click **Select** to save these changes and return to **Dial Pattern Details** page. Click **Commit** to save. The following screen shows that minimum **2** digit dialed numbers that begin with **22** originating from **SMGRVL3** uses route policy **toCS1K**. This will allow DID numbers assigned to the enterprise from Swisscom SIP Trunk Service to route to Communication Server 1000E.

Home / Elements / Routing / Dial Patterns- Dial Pattern Details

Dial Pattern Details Commit

General

* Pattern: 22

* Min: 2

* Max: 16

Emergency Call: ☐

SIP Domain: ALL

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	SMGRVL3		toCS1K	0	<input type="checkbox"/>	CS1K	

Select : All, None

Repeat the above steps to add the Dial Pattern to the Avaya SBCE, select the routing policy defined in **Section 6.6**. The following screenshot shows that a minimum **5** digit dialed numbers that begin with **00353** originating from **SMGRVL3** uses route policy **toSipera**. This will allow outbound calls to route from the Communication Server 1000E to PSTN test numbers in the Avaya enterprise lab.

Routing | Home / Elements / Routing / Dial Patterns- Dial Pattern Details

Dial Pattern Details Commit

General

* Pattern: 00353

* Min: 5

* Max: 16

Emergency Call: ☐

SIP Domain: -ALL-

Notes:

Originating Locations and Routing Policies

Add Remove

1 Item Refresh

<input type="checkbox"/>	Originating Location Name 1 ▲	Originating Location Notes	Routing Policy Name	Rank 2 ▲	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
<input type="checkbox"/>	-ALL-	Any Locations	toSipera	0	<input type="checkbox"/>	Sipera	

Select : All, None

7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya SBCE. The Avaya SBCE is administered using the UC-Sec Control Center.

7.1. Access Avaya Session Border Controller for Enterprise

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



Enter the appropriate **Login ID** and **Password**.



7.2. Define Network Information

To define the network information for the Avaya SBCE, click on the **Device Specific Settings** to expand the options, then select **Network Management**.

- Click on **Add IP**
- Define the internal IP address with subnet mask and assign to interface **A1**
- Select **Save** (not shown) to save the information
- Click on **Add IP**
- Define the external IP address with subnet mask and assign to interface **B1**
- Select **Save** (not shown) to save the information
- Select the **Interface Configuration** tab and change the state of interfaces A1 and B1 to **Enabled**

To activate the changes click on **System Management** in the main menu and select **Restart Application** indicated by an icon in the status bar (not shown).

IP Address	Public IP	Gateway	Interface
10.10.3.30		10.10.3.1	A1
86.x.x.x.x		86.x.x.x.x	B1

7.3. Define Interfaces

To define the signaling and media interfaces for the Avaya SBCE, click on the **Device Specific Settings** to expand the options.

7.3.1. Signalling Interfaces

Select **Signalling Interface** from the menu options.

- Select **Add Signalling Interface**
- In the **Name** field enter a descriptive name for the internal signalling interface
- Select the **internal** interface IP address defined in **Section 7.2**
- Select **UDP** and **TCP** port numbers, **5060** is the default port number used for this test configuration
- Select **Add Signalling Interface**
- In the **Name** field enter a descriptive name for the external signalling interface
- Select the **external** interface IP address defined in **Section 7.2**
- Select **UDP** and **TCP** port numbers, **5075** is used by Telenor

The screenshot shows the UC-Sec Control Center web interface. The top navigation bar includes links for Alarms, Incidents, Statistics, Logs, Diagnostics, and Users. The left sidebar shows a tree view of the system configuration, with 'Signaling Interface' selected under 'Device Specific Settings'. The main content area displays the 'Signaling Interface' configuration for device 'GSSCP_03'. It includes a table with two rows: 'Int_Sig' and 'Ext_Sig'. The 'Int_Sig' row has a Signaling IP of 10.10.3.30, TCP Port 5060, and UDP Port 5060. The 'Ext_Sig' row has a Signaling IP of xxx.xxx.xxx.xxx, TCP Port 5075, and UDP Port 5075. Both rows have TLS Port set to --- and TLS Profile set to None. There are edit and delete icons for each row. An 'Add Signaling Interface' button is located above the table.

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile		
Int_Sig	10.10.3.30	5060	5060	---	None		
Ext_Sig	xxx.xxx.xxx.xxx	5075	5075	---	None		

7.3.2. Media Interfaces

Select **Media Interface** from the menu options. The IP addresses for media can be the same as those used for signalling.

- Select **Add Media Interface**
- In the **Name** field enter a descriptive name for the internal media interface
- Select the **internal** interface IP address defined in **Section 7.2**
- Select RTP port ranges for the media path with the enterprise end-points
- Select **Add Media Interface**
- In the **Name** field enter a descriptive name for the external media interface
- Select the **external** interface IP address defined in **Section 7.2**
- Select RTP port ranges for the media path with the Telenor SIP Trunk Service

The screenshot shows the UC-Sec Control Center web interface. The top header includes the title 'UC-Sec Control Center', a welcome message, the user 'Admin', and the server time '2:04:48 PM GMT'. The Siper Systems logo is in the top right. A navigation bar contains links for Alarms, Incidents, Statistics, Logs, Diagnostics, Users, Logout, and Help. A left sidebar lists various system management options, with 'Media Interface' highlighted under 'Device Specific Settings'. The main content area is titled 'Device Specific Settings > Media Interface: GSSCP_03'. It features a 'Media Interface' tab, a warning message about application restarts, an 'Add Media Interface' button, and a table listing existing interfaces.

Name	Media IP	Port Range		
Int_Media	10.10.3.30	35000 - 40000		
Ext_Media	xxx xxx xxx xxx	35000 - 40000		

7.4 Define Server Interworking

Server interworking is defined for the Telenor SIP Trunk Service and the Session Manager. To define server interworking, first click on **Global Profiles** to expand the menu options.

- Highlight the **avaya-ru** profile and select **Clone Profile**
- In the **Name** field enter a descriptive name for server interworking profile from the Session Manager to the Telenor SIP Trunk Service
- Click on **Finish**
- Select **Edit** and check the T.38 box, then **Next** and **Finish**
- Select **Add Profile**
- In the **Name** field enter a descriptive name for server interworking profile from the Telenor SIP Trunk Service to the Session Manager
- Select **Edit** and check the T.38 box
- Change the **Hold Support RFC** to **RFC2543**
- Select **Next** three times and **Finish**

The screenshot shows the UC-Sec Control Center interface. The left sidebar contains a tree view with 'Server Interworking' selected. The main panel displays the configuration for the 'SM3_CS' profile. The 'General' tab is active, showing various settings. The 'Hold Support' is set to 'RFC2543', 'T.38 Support' is set to 'Yes', and 'Privacy Enabled' is set to 'No'.

Global Profiles > Server Interworking: SM3_CS	
Click here to add a description.	
General Timers URI Manipulation Header Manipulation Advanced	
General	
Hold Support	RFC2543
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
T.38 Support	Yes
URI Scheme	SIP
Via Header Format	RFC3261
Privacy	
Privacy Enabled	No

7.4. Define Servers

To define the servers and add the additional IP address for the Telenor SIP Trunk Service, click on **Global Profiles** to expand the menu. Select **Server Configuration** to add the Call Server which is the Session Manager.

- Select **Add Profile**
- In the **Name** field enter a descriptive name for the Session Manager
- Enter the Session Manager SIP Signalling interface IP address in the IP address field
- Select **TCP** and **UDP** ports for SIP signaling

The screenshot shows the UC-Sec Control Center interface. The left sidebar has 'Server Configuration' highlighted. The main area shows the 'Global Profiles > Server Configuration: SM3_Call_Server' page. The 'General' tab is selected, displaying a table with the following data:

General	
Server Type	Trunk Server
IP Addresses / FQDNs	10.10.3.5
Supported Transports	TCP, UDP
TCP Port	5060
UDP Port	5060

Buttons for 'Add Profile', 'Rename Profile', 'Clone Profile', 'Delete Profile', and 'Edit' are visible.

Select the server **Interworking Profile** for the call server defined in Section 7.4.

The screenshot shows the UC-Sec Control Center interface. The left sidebar has 'Server Configuration' highlighted. The main area shows the 'Global Profiles > Server Configuration: SM3_Call_Server' page. The 'Advanced' tab is selected, displaying a table with the following data:

Advanced	
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	SM3_CS
Signaling Manipulation Script	None
TCP Connection Type	SUBID
UDP Connection Type	SUBID

Buttons for 'Add Profile', 'Rename Profile', 'Clone Profile', 'Delete Profile', and 'Edit' are visible.

Select **Server Configuration** to add the Trunk Server which is the Telenor SIP Trunk Service.

- Select **Add Profile**
- In the **Name** field enter a descriptive name for the Telenor SIP Trunk Service
- Enter the Telenor SIP Trunk Service IP address in the IP address field
- Select a **UDP** port for SIP signaling **5075** is used by Telenor

The screenshot shows the UC-Sec Control Center interface. The left sidebar has 'Server Configuration' highlighted. The main area shows 'Global Profiles > Server Configuration: SP_Trunk_Server'. A table lists profiles: 'SM3_Call_Server' and 'SP_Trunk_Server' (highlighted). The 'General' tab is active, showing fields for 'Server Type' (Trunk Server), 'IP Addresses / FQDNs' (XXX.XXX.XXX.XXX), 'Supported Transports' (UDP), and 'UDP Port' (5075). Buttons for 'Add Profile', 'Rename Profile', 'Clone Profile', 'Delete Profile', and 'Edit' are visible.

Select the server **Interworking Profile** for the trunk server defined in **Section 7.4**.

The screenshot shows the UC-Sec Control Center interface. The left sidebar has 'Server Configuration' highlighted. The main area shows 'Global Profiles > Server Configuration: SP_Trunk_Server'. The 'Advanced' tab is active, showing fields for 'Enable DoS Protection' (checkbox), 'Enable Grooming' (checkbox), 'Interworking Profile' (SP_Trunk), 'Signaling Manipulation Script' (None), and 'UDP Connection Type' (SUBID). Buttons for 'Add Profile', 'Rename Profile', 'Clone Profile', 'Delete Profile', and 'Edit' are visible.

7.5. Define Routing

To define routing to the Session Manager, click on **Global Profiles** to expand the menu. Select **Routing**.

- Select **Add Profile**
- In the **Name** field enter a descriptive name for the Session Manager
- Enter the Session Manager SIP Signalling interface IP address in the **Next Hop Server 1** field
- Check the **Next Hop in Dialog** box
- Select **TCP** for the **Outgoing Transport**

Note: The **Next Hop in Dialog** is required to ensure that messages are sent to the next hop address regardless of the original destination. This is necessary where the Trunk Server sends messages to the address specified in the Contact header in the original INVITE message.

The screenshot shows the UC-Sec Control Center interface. The left sidebar has a tree view with 'Routing' selected. The main area is titled 'Global Profiles > Routing: Call Server'. It includes buttons for 'Add Profile', 'Rename Profile', 'Clone Profile', and 'Delete Profile'. Below these is a 'Routing Profiles' list with 'default' and 'Call Server' (highlighted). The 'Call Server' profile is expanded, showing a 'Routing Profile' section with a table of routing rules. The table has columns: Priority, URI Group, Next Hop Server 1, Next Hop Server 2, Next Hop Priority, NAPTR, SRV, Next Hop in Dialog, Ignore Route Header, and Outgoing Transport. A single rule is shown with Priority 1, URI Group *, Next Hop Server 1 10.10.3.55, Next Hop Priority checked, and Outgoing Transport TCP.

Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport
1	*	10.10.3.55	---	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	TCP

To define routing to the Telenor Trunk Server, create an additional profile

- Select **Add Profile**
- In the **Name** field enter a descriptive name for the Telenor SIP Trunk Service
- Enter the Telenor SIP Trunk Service IP address and port **5075** in the **Next Hop Server 1** field
- Check the **Next Hop in Dialog** box
- Select **UDP** for the **Outgoing Transport**

The screenshot shows the UC-Sec Control Center interface. The left sidebar has a tree view with 'Routing' selected. The main area is titled 'Global Profiles > Routing: Trunk Server'. It includes buttons for 'Add Profile', 'Rename Profile', 'Clone Profile', and 'Delete Profile'. Below these is a 'Routing Profiles' list with 'default' and 'Trunk Server' (highlighted). The 'Trunk Server' profile is expanded, showing a 'Routing Profile' section with a table of routing rules. The table has columns: Priority, URI Group, Next Hop Server 1, Next Hop Server 2, Next Hop Priority, NAPTR, SRV, Next Hop in Dialog, Ignore Route Header, and Outgoing Transport. A single rule is shown with Priority 1, URI Group *, Next Hop Server 1 XXX.XXX.XXX.XXX:5075, Next Hop Priority checked, and Outgoing Transport UDP.

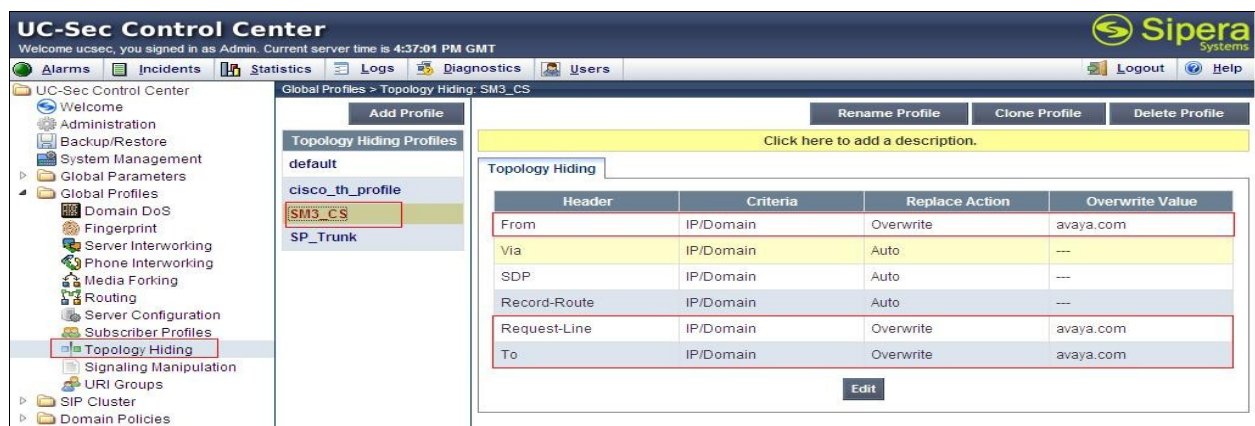
Priority	URI Group	Next Hop Server 1	Next Hop Server 2	Next Hop Priority	NAPTR	SRV	Next Hop in Dialog	Ignore Route Header	Outgoing Transport
1	*	XXX.XXX.XXX.XXX:5075	---	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	UDP

7.6. Topology Hiding

Topology hiding is used to hide local information such as private IP addresses and local domain names. To define Topology Hiding for the Session Manager, click on **Global Profiles** to expand the menu and select **Topology Hiding**

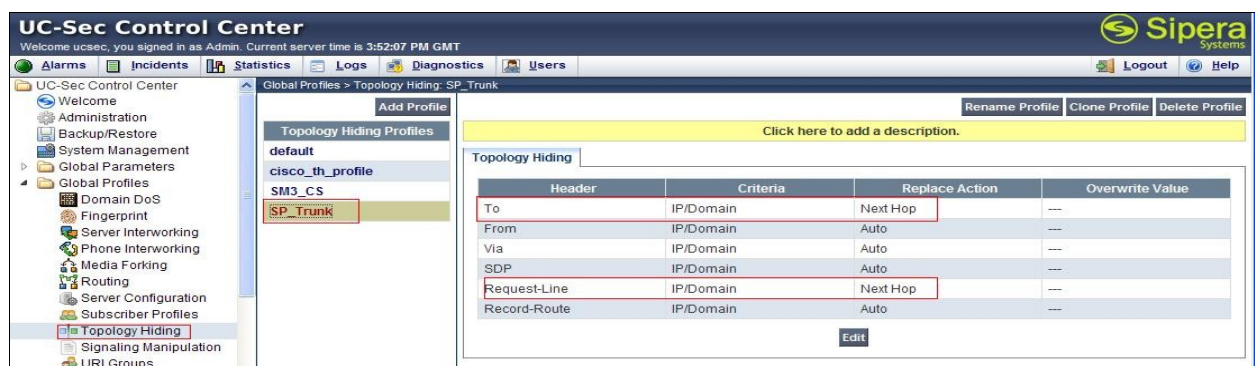
- Select **Add Profile**
- In the **Name** field enter a descriptive name for the Session Manager
- **Overwrite** the **From** field with a domain name for the Trunk Server, in test **avaya.com** was used
- **Overwrite** the **Request-Line** field and **To** field with a local domain name, in test **avaya.com** was used

Note: Different domain names could be used for the enterprise and Telenor network.



To define Topology Hiding for the Telenor SIP Trunk Service, create an additional profile

- Select **Add Profile**
- In the **Name** field enter a descriptive name for the Telenor SIP Trunk Service
- **Overwrite** the **From** field with a Replace Action Next Hop selection
- **Overwrite** the **Request-Line** field and **To** field with Replace Action Next Hop selection



7.7. Signalling Rules

Signalling rules are a mechanism on the Avaya SBCE to handle any unusual signalling scenarios that may be encountered for a particular Service Provider. When the Entity Link described in **Section 6.6** is established, it initiates OPTIONS messages from the Session Manager to the Avaya SBCE. This prompts the Avaya SBCE to initiate OPTIONS messages to the Service Provider. If it doesn't receive a valid response from the Service Provider, it will not respond to the Session Manager. The 407 "Proxy Authentication Required" is not treated as a valid response. When this happens, the Entity Links will not be established and will be indicated as "DOWN" on the Session Manager

A signalling rule must be defined on the Avaya SBCE to treat the 407 "Proxy Authentication Required" response from Telenor and change it to a valid 200 "OK" response for Session Manager. To define the signalling rule, click on **Domain Policies** to expand the menu and select **Signalling Rules**.

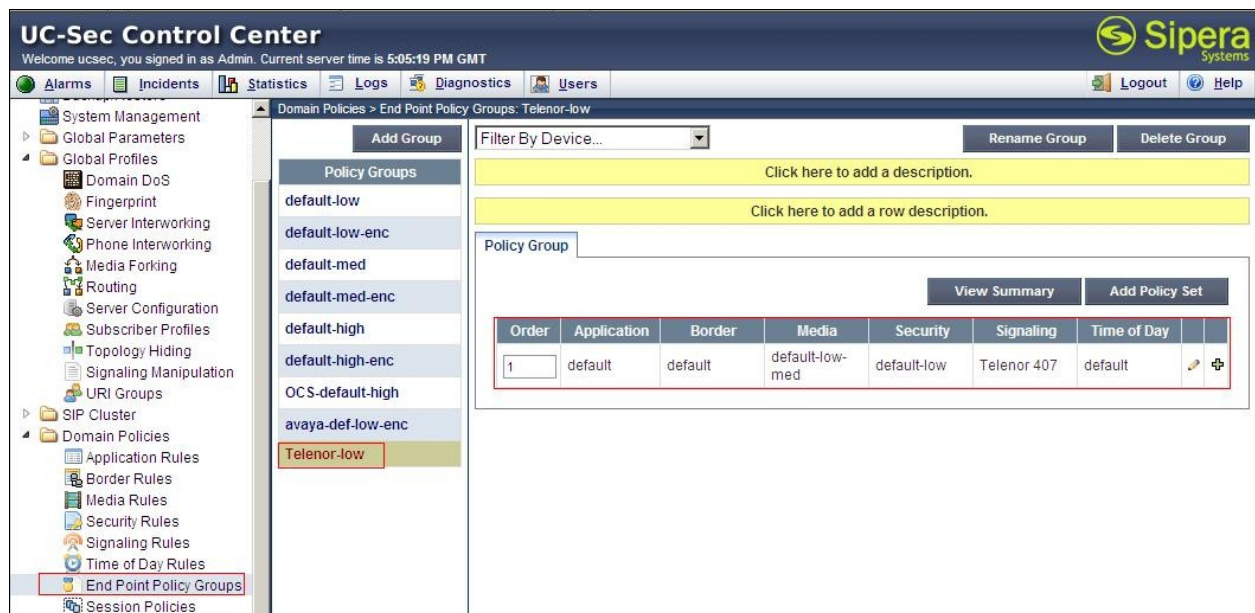
- Select **Add Rule**
- In the **Name** field enter a descriptive name for the Telenor signalling rule
- Click on the **Responses** tab
- Click on the **Add in Response Control**
- Select **Response Code 407**
- Select **Change response** in the **In Dialog Action** field
- Define the response code as **200** and the text field as **OK**

The screenshot shows the UC-Sec Control Center interface. The left sidebar contains a tree view with categories like Administration, Global Profiles, SIP Cluster, and Domain Policies. Under Domain Policies, 'Signalling Rules' is selected. The main area displays the configuration for a rule named 'Telenor 407'. The 'Responses' tab is active, showing a table with one row: Row 1, Response Code 407, Method Name ALL, In Dialog Action 'Change response to "200 OK"', Proprietary No, and Direction IN. Above the table are buttons for 'Add In Response Control' and 'Add Out Response Control'. The top of the interface shows the user is logged in as Admin and the server time is 4:52:57 PM GMT.

Row	Response Code	Method Name	In Dialog Action	Proprietary	Direction	
1	407	ALL	Change response to "200 OK"	No	IN	

An End Point Policy Group is required to implement the signalling rule. To define this, click on **Domain Policies** to expand the menu and select **End Point Policy Groups**.

- Select **Add Group**
- In the **Name** field enter a descriptive name for the Telenor Policy Group
- In the **Application** field, select **default**
- In the **Border** field, select **default**
- In the **Media** field, select **default-low-med**
- In the **Security** field, select **default-low**
- In the **Signalling** field, select the recently added signalling rule for Telenor
- In the **Time of Day** field, select **default**



7.8. Server Flows

Server Flows combine the previously defined profiles into an outgoing flow from the Session Manager to the Telenor SIP Trunk Service and an incoming flow from the Telenor SIP Trunk Service to the Session Manager. To define an outgoing Server Flow, click on **Device Specific Settings** to expand the menu and select **End Point Flows**.

- Click on the **Server Flows** tab
- Select **Add Flow**
- In the **Name** field enter a descriptive name for the outgoing server flow
- In the **Received Interface** field, select the SIP signalling interface for the Telenor SIP Trunk Service
- In the **Signalling Interface** field, select the SIP signalling interface for the Session Manager
- In the **Media Interface** field, select the media interface for the Session Manager
- In the **Routing Profile** field, select the routing profile of the Telenor SIP Trunk Service
- In the **Topology Hiding Profile** field, select the topology hiding profile of the Session Manager

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

- Select **Add Flow**
- In the **Name** field enter a descriptive name for the incoming server flow
- In the **Received Interface** field, select the SIP signalling interface for the Session Manager
- In the **Signalling Interface** field, select the SIP signalling interface for the Telenor SIP Trunk Service
- In the **Media Interface** field, select the media interface for the Telenor SIP Trunk Service
- In the **End Point Policy Group** field, select the End Point Policy Group defined in **Section 7.8**
- In the **Routing Profile** field, select the routing profile of the Session Manager
- In the **Topology Hiding Profile** field, select the topology hiding profile of the Telenor SIP Trunk Service

The screenshot shows the UC-Sec Control Center web interface. The left sidebar contains a navigation tree with categories like Administration, System Management, Global Profiles, SIP Cluster, Domain Policies, and Device Specific Settings. The 'End Point Flows' option under 'Device Specific Settings' is highlighted. The main content area is titled 'Device Specific Settings > End Point Flows: GSSCP_03'. It features two tabs: 'Subscriber Flows' and 'Server Flows'. The 'Server Flows' tab is active, displaying a table with the following data:

Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile		
1	SM3_Call_Server	*	*	*	Ext_Sig	Int_Sig	Int_Media	default-low	Trunk Server	SM3_CS	None		

Below the table, there is a section titled 'Server Configuration: SP_Trunk_Server' which contains another table:

Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signaling Interface	Media Interface	End Point Policy Group	Routing Profile	Topology Hiding Profile	File Transfer Profile		
1	SP_Trunk_Server	*	*	*	Int_Sig	Ext_Sig	Ext_Media	Telenor-low	Call Server	SP_Trunk	None		

8. Telenor SIP Service Provider Configuration

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

9. Verification

This section provides verification steps that may be performed in the field to verify that the solution is configured properly. This section also provides a list of useful troubleshooting commands that can be used to troubleshoot the solution.

9.1. Verify Avaya Communication Server 1000E Operational Status

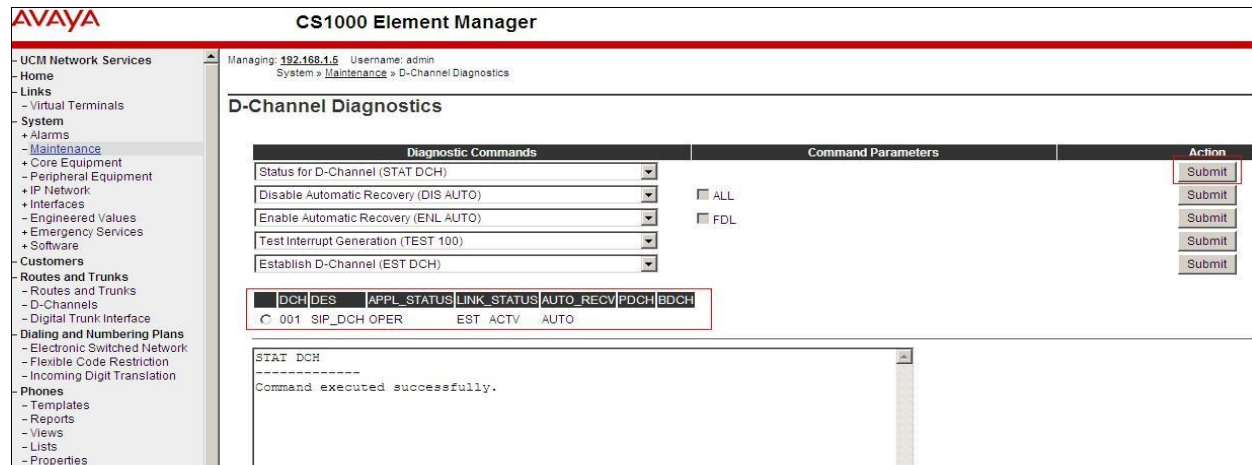
Expand **System** on the left navigation panel and select **Maintenance**. Select **LD 96 - D-Channel** from the **Select by Overlay** table and the **D-Channel Diagnostics** function from the **Select Group** table as shown below.

The screenshot displays the AVAYA CS1000 Element Manager web interface. The top header shows the AVAYA logo and the title "CS1000 Element Manager". Below the header, the left navigation pane lists various system components, with "System" expanded to show "Maintenance". The main content area is titled "Maintenance" and contains two tables. The "Select by Overlay" table lists various LDs (LD 30, LD 32, LD 34, LD 36, LD 37, LD 38, LD 39, LD 45, LD 46, LD 48, LD 54, LD 60, LD 75, LD 80, LD 96, LD 117, LD 135, LD 137, LD 143). The "Select Group" table lists "D-Channel Diagnostics", "MSDL Diagnostics", and "TMDI Diagnostics". The "LD 96 - D-Channel" entry is highlighted in the "Select by Overlay" table, and the "D-Channel Diagnostics" entry is highlighted in the "Select Group" table.

AVAYA CS1000 Element Manager	
<ul style="list-style-type: none">- UCM Network Services- Home- Links- Virtual Terminals- System<ul style="list-style-type: none">- Alarms- Maintenance+ Core Equipment- Peripheral Equipment+ IP Network+ Interfaces- Engineered Values+ Emergency Services+ Software- Customers<ul style="list-style-type: none">- Routes and Trunks- Routes and Trunks- D-Channels- Digital Trunk Interface- Dialing and Numbering Plans<ul style="list-style-type: none">- Electronic Switched Network- Flexible Code Restriction- Incoming Digit Translation- Phones<ul style="list-style-type: none">- Templates- Reports- Views- Lists- Properties- Migration	Managing: 192.168.1.5 Username: admin System > Maintenance Maintenance <div><input checked="" type="radio"/> Select by Overlay <div><Select by Overlay> LD 30 - Network and Signaling LD 32 - Network and Peripheral Equipment LD 34 - Tone and Digit Switch LD 36 - Trunk LD 37 - Input/Output LD 38 - Conference Circuit LD 39 - Intergroup Switch and System Clock LD 45 - Background Signaling and Switching LD 46 - Multifrequency Sender LD 48 - Link LD 54 - Multifrequency Signaling LD 60 - Digital Trunk Interface and Primary Rate Interface LD 75 - Digital Trunk LD 80 - Call Trace LD 96 - D-Channel LD 117 - Ethernet and Alarm Management LD 135 - Core Common Equipment LD 137 - Core Input/Output LD 143 - Centralized Software Upgrade</div><div><input type="radio"/> Select by Functionality <div><Select Group> D-Channel Diagnostics MSDL Diagnostics TMDI Diagnostics</div></div></div>

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**



Managing: 192.168.1.5 Username: admin
System > Maintenance > D-Channel Diagnostics

D-Channel Diagnostics

Diagnostic Commands	Command Parameters	Action
Status for D-Channel (STAT DCH)		<input type="button" value="Submit"/>
Disable Automatic Recovery (DIS AUTO)	<input type="checkbox"/> ALL	<input type="button" value="Submit"/>
Enable Automatic Recovery (ENL AUTO)	<input type="checkbox"/> FDL	<input type="button" value="Submit"/>
Test Interrupt Generation (TEST 100)		<input type="button" value="Submit"/>
Establish D-Channel (EST DCH)		<input type="button" value="Submit"/>

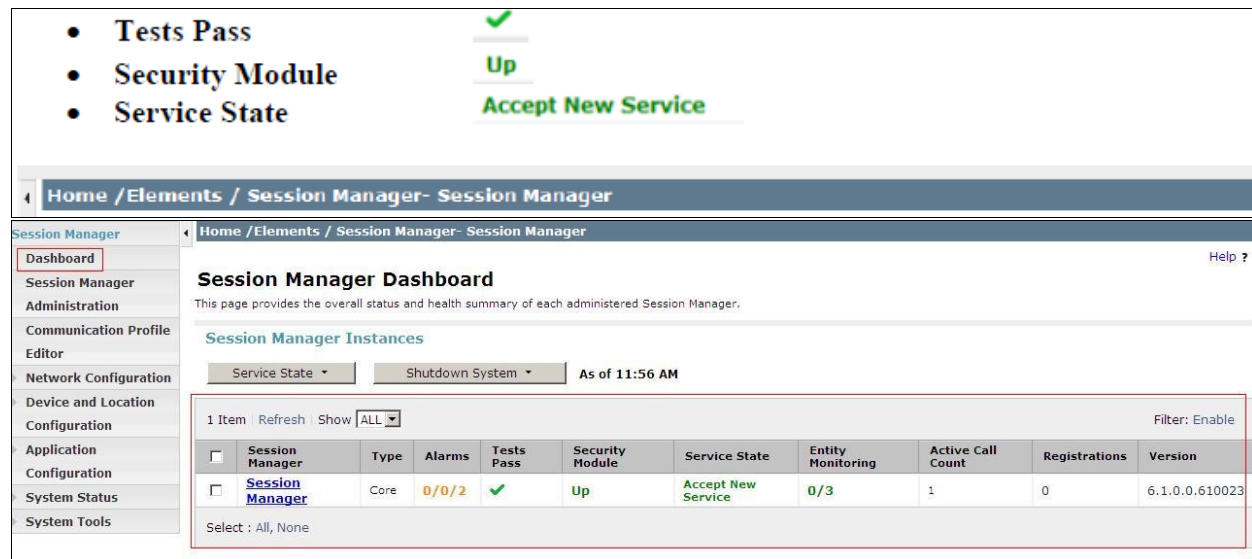
DCH	DES	APPL_STATUS	LINK_STATUS	AUTO_REC	PDCH	BDCH
C 001	SIP_DCH	OPER	EST ACTV	AUTO		

```

STAT DCH
-----
Command executed successfully.
  
```

9.2. Verify Avaya Aura® Session Manager Operational Status

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** Up
- **Service State** Accept New Service

Home / Elements / Session Manager - Session Manager

Session Manager Dashboard

This page provides the overall status and health summary of each administered Session Manager.

Session Manager Instances

Service State: [Dropdown] Shutdown System: [Dropdown] As of 11:56 AM

Session Manager	Type	Alarms	Tests Pass	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Version
<input type="checkbox"/> Session Manager	Core	0/0/2	✓	Up	Accept New Service	0/3	1	0	6.1.0.0.610023

Select: All, None

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.

Reset

Synchronize

Certificate Management ▾

Connection Status

1 Item

Refresh

Show

ALL ▾

Filter: Enable

	Details	Session Manager	Type	Status	Connections	IP Address	VLAN	Default Gateway	NIC Bonding	Entity Links (expected / actual)	Certificate Used
<div>C</div>	<div>► Show</div>	Session Manager	SM	Up	6	10.10.3.55/24	---	10.10.3.1	Disabled	3/3	SIP CA

Select : None

9.3. 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: Communication Server 1000E** table, verify the **Conn. Status** for the link is **Up** as shown below.

SIP Entity, Entity Link Connection Status							
This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.							
All Entity Links to SIP Entity: CS1K							
Summary View							
1 Item Refresh Filter: Enable							
Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
► Show	Session Manager	10.10.3.6	5060	TCP	Up	200 OK	Up

Verify the status of the SIP link is up between the Session Manager and the Avaya SBCE by going through the same process as outlined above but selecting the SIP Entity for the Avaya SBCE in the **All Monitored SIP Entity:** table.

SIP Entity, Entity Link Connection Status							
This page displays detailed connection status for all entity links from all Session Manager instances to a single SIP entity.							
All Entity Links to SIP Entity: Sipera							
Summary View							
1 Item Refresh Filter: Enable							
Details	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Conn. Status	Reason Code	Link Status
► Show	Session Manager	10.10.3.30	5060	TCP	Up	200 OK	Up

10. Conclusion

These Application Notes describe the configuration necessary to connect the Avaya Communication Server 1000E, Avaya Aura® Session Manager and Avaya Session Border Controller for Enterprise to Telenor SIP Service. Interoperability testing of the sample configuration was completed with successful results for the Telenor SIP Trunk with observations which are detailed in **Section 2.2**.

11. Additional References

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

- [1] 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] Network Routing Service Fundamentals, Release 7.5, Document Number NN43001-130, Issue 03.02, available at <http://support.avaya.com>
- [8] 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>
- [9] Signaling Server and IP Line Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-125, available at <http://support.avaya.com>
- [10] E-SBC (Avaya Session Border Controller Advanced for Enterprise) Administration Guide, November 2011
- [11] RFC 3261 SIP: Session Initiation Protocol, <http://www.ietf.org/>

Appendix A – Avaya Communication Server 1000E Software

Avaya Communication Server 1000E call server patches and plug ins

TID: 46379

VERSION 4121

System type is - Communication Server 1000E/CP PM Linux

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: 01(created: 2012-01-10 16:47:54 (est))

MDP>LAST SUCCESSFUL MDP REFRESH :2012-01-24 11:17:37(Local Time)
MDP>USING DEPLIST ZIP FILE DOWNLOADED :2012-01-11 11:07:13(est)
SYSTEM HAS NO USER SELECTED PEPs IN-SERVICE

LOADWARE VERSION: PSWV 100
INSTALLED LOADWARE PEPs : 0
ENABLED PLUGINS : 0

Avaya Communication Server 1000E call server deplists

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

IN-SERVICE PEPs

PAT#	CR #	PATCH REF #	NAME	DATE	FILENAME	SPECINS
000	wi00891626	ISS1:10F1	p31051_1	01/02/2012	p31051_1.cpl	YES
001	wi00951837	ISS1:10F1	p31485_1	01/02/2012	p31485_1.cpl	NO
002	wi00946477	ISS1:10F1	p31426_1	01/02/2012	p31426_1.cpl	NO
003	wi00906163	ISS1:10F1	p31205_1	01/02/2012	p31205_1.cpl	NO
004	wi00962211	ISS1:10F1	p31580_1	01/02/2012	p31580_1.cpl	NO
005	wi00877592	ISS1:10F1	p30880_1	01/02/2012	p30880_1.cpl	NO
006	wi00839134	ISS1:10F1	p30698_1	01/02/2012	p30698_1.cpl	YES
007	wi00958682	ISS1:10F1	p31540_1	01/02/2012	p31540_1.cpl	NO
008	wi00868729	ISS1:10F1	p31163_1	01/02/2012	p31163_1.cpl	NO
009	wi00886321	ISS1:10F1	p31009_1	01/02/2012	p31009_1.cpl	NO
010	wi00946282	ISS1:10F1	p31204_1	01/02/2012	p31204_1.cpl	NO
011	wi00841980	ISS1:10F1	p30618_1	01/02/2012	p30618_1.cpl	NO
012	wi00946681	ISS1:10F1	p31428_1	01/02/2012	p31428_1.cpl	NO
013	wi00945533	ISS1:10F1	p31421_1	01/02/2012	p31421_1.cpl	YES
014	wi00843623	ISS1:10F1	p30731_1	01/02/2012	p30731_1.cpl	YES
015	wi00958776	ISS1:10F1	p31542_1	01/02/2012	p31542_1.cpl	YES
016	wi00857362	ISS1:10F1	p30782_1	01/02/2012	p30782_1.cpl	NO
017	wi00865477	ISS1:10F1	p30893_1	01/02/2012	p30893_1.cpl	YES
018	wi00879526	ISS1:10F1	p31007_1	01/02/2012	p31007_1.cpl	NO
019	wi00894243	ISS1:10F1	p31087_1	01/02/2012	p31087_1.cpl	NO
020	wi00890475	p30952	p31048_1	01/02/2012	p31048_1.cpl	NO
021	WI00927300	ISS1:10F1	p30999_1	01/02/2012	p30999_1.cpl	NO
022	wi00856991	ISS1:10F1	p17588_1	01/02/2012	p17588_1.cpl	NO
023	wi00688381	ISS1:10F1	p30104_1	01/02/2012	p30104_1.cpl	NO
024	wi00881777	ISS1:10F1	p25747_1	01/02/2012	p25747_1.cpl	NO
025	WI00853473	ISS1:10F1	p30625_1	01/02/2012	p30625_1.cpl	NO
026	wi00855423	ISS1:10F1	p31328_1	01/02/2012	p31328_1.cpl	YES
027	wi00943172	ISS1:10F1	p31402_1	01/02/2012	p31402_1.cpl	NO

028	wi00865477	ISS1:10F1	p30898_1	01/02/2012	p30898_1.cpl	YES
029	wi00850521	ISS1:10F1	p30709_1	01/02/2012	p30709_1.cpl	YES
030	wi00898327	ISS1:10F1	p31136_1	01/02/2012	p31136_1.cpl	NO
031	wi00871739	ISS1:10F1	p30856_1	01/02/2012	p30856_1.cpl	NO
032	wi00853031	ISS1:10F1	p30531_1	01/02/2012	p30531_1.cpl	NO
033	wi00839821	ISS1:10F1	p30619_1	01/02/2012	p30619_1.cpl	NO
034	wi00854130	ISS1:10F1	p30443_1	01/02/2012	p30443_1.cpl	NO
035	wi00871969	ISS1:10F1	p30768_1	01/02/2012	p30768_1.cpl	NO
036	wi00952381	ISS1:10F1	p31410_1	01/02/2012	p31410_1.cpl	NO
037	wi00946876	ISS1:10F1	p31430_1	01/02/2012	p31430_1.cpl	NO
038	wi00962557	ISS1:10F1	p31581_1	01/02/2012	p31581_1.cpl	NO
039	wi00833910	ISS2:10F1	p30492_2	01/02/2012	p30492_2.cpl	NO
040	wi00903085	ISS1:10F1	p31164_1	01/02/2012	p31164_1.cpl	NO
041	wi00875425	ISS1:10F1	p30943_1	01/02/2012	p30943_1.cpl	NO
042	wi00862574	iss1:10f1	p30870_1	01/02/2012	p30870_1.cpl	NO
043	wi00859499	ISS1:10F1	p30694_1	01/02/2012	p30694_1.cpl	NO
044	wi00925208	ISS1:10F1	p30986_1	01/02/2012	p30986_1.cpl	NO
045	wi00877442	ISS1:10F1	p30844_1	01/02/2012	p30844_1.cpl	NO
046	wi00900668	ISS1:10F1	p30456_1	01/02/2012	p30456_1.cpl	NO
047	wi00867905	ISS1:10F1	p30640_1	01/02/2012	p30640_1.cpl	NO
048	wi00879322	ISS1:10F1	p30954_1	01/02/2012	p30954_1.cpl	NO
049	wi00865477	ISS1:10F1	p30895_1	01/02/2012	p30895_1.cpl	YES
050	wi00951925	ISS1:10F1	p31486_1	01/02/2012	p31486_1.cpl	NO
051	wi00865477	ISS1:10F1	p30894_1	01/02/2012	p30894_1.cpl	YES
052	wi00865477	ISS1:10F1	p30897_1	01/02/2012	p30897_1.cpl	YES
053	wi00865477	ISS1:10F1	p30892_1	01/02/2012	p30892_1.cpl	YES
054	wi00908933	ISS1:10F1	p31239_1	01/02/2012	p31239_1.cpl	NO
055	wi00931028	ISS1:10F1	p31354_1	01/02/2012	p31354_1.cpl	YES
056	wi00932948	ISS1:10F1	p31077_1	01/02/2012	p31077_1.cpl	NO
057	wi00869695	ISS1:10F1	p30654_1	01/02/2012	p30654_1.cpl	NO
058	wi00838073	ISS1:10F1	p30588_1	01/02/2012	p30588_1.cpl	NO
059	wi00852365	ISS1:10F1	p30707_1	01/02/2012	p30707_1.cpl	NO
060	wi00927321	ISS1:10F1	p31286_1	01/02/2012	p31286_1.cpl	YES
061	wi00937114	ISS1:10F1	p31310_1	01/02/2012	p31310_1.cpl	NO
062	wi00877367	ISS1:10F1	p30534_1	01/02/2012	p30534_1.cpl	NO
063	wi00900096	ISS1:10F1	p31006_1	01/02/2012	p31006_1.cpl	NO
064	wi00905660	ISS1:10F1	p27968_1	01/02/2012	p27968_1.cpl	NO
065	wi00925141	ISS1:10F1	p30802_1	01/02/2012	p30802_1.cpl	NO
066	wi00943748	ISS1:10F1	p31516_1	01/02/2012	p31516_1.cpl	NO
067	wi00827950	ISS2:10F1	p30471_2	01/02/2012	p30471_2.cpl	NO
068	wi00937119	ISS1:10F1	p28005_1	01/02/2012	p28005_1.cpl	NO
069	wi00836981	ISS1:10F1	p30613_1	01/02/2012	p30613_1.cpl	NO
070	wi00961267	ISS1:10F1	p30288_1	01/02/2012	p30288_1.cpl	NO
071	wi00936714	ISS1:10F1	p31379_1	01/02/2012	p31379_1.cpl	NO
072	wi00906022	ISS1:10F1	p31202_1	01/02/2012	p31202_1.cpl	NO
073	wi00852389	ISS1:10F1	p30641_1	01/02/2012	p30641_1.cpl	NO
074	wi00857566	ISS1:10F1	p30766_1	01/02/2012	p30766_1.cpl	NO
075	wi00932204	ISS2:10F1	p31305_2	01/02/2012	p31305_2.cpl	NO
077	wi00865477	ISS1:10F1	p30890_1	01/02/2012	p30890_1.cpl	YES
078	wi00873382	ISS1:10F1	p30832_1	01/02/2012	p30832_1.cpl	NO
079	wi00948274	ISS1:10F1	p31365_1	01/02/2012	p31365_1.cpl	NO
080	wi00923899	ISS1:10F1	p31270_1	01/02/2012	p31270_1.cpl	NO
081	wi00856410	ISS1:10F1	p30749_1	01/02/2012	p30749_1.cpl	NO
082	wi00854415	ISS1:10F1	p30593_1	01/02/2012	p30593_1.cpl	NO
083	wi00896394	ISS1:10F1	p30807_1	01/02/2012	p30807_1.cpl	NO
084	wi00826075	ISS1:10F1	p30452_1	01/02/2012	p30452_1.cpl	NO
085	wi00863876	ISS1:10F1	p30787_1	01/02/2012	p30787_1.cpl	NO
086	wi00880386	ISS1:10F1	p30977_1	01/02/2012	p30977_1.cpl	NO
087	wi00840590	ISS1:10F1	p30767_1	01/02/2012	p30767_1.cpl	NO
088	wi00949627	ISS1:10F1	p31462_1	01/02/2012	p31462_1.cpl	NO
089	wi00842409	ISS1:10F1	p30621_1	01/02/2012	p30621_1.cpl	NO
090	wi00865477	ISS1:10F1	p30896_1	01/02/2012	p30896_1.cpl	YES
091	wi00897096	ISS1:10F1	p30676_1	01/02/2012	p30676_1.cpl	NO
092	wi00899584	ISS1:10F1	p30809_1	01/02/2012	p30809_1.cpl	NO
093	wi00907707	ISS1:10F1	p31228_1	01/02/2012	p31228_1.cpl	NO
094	wi00949273	ISS1:10F1	p31411_1	01/02/2012	p31411_1.cpl	NO
095	wi00839255	ISS1:10F1	p30591_1	01/02/2012	p30591_1.cpl	NO
096	wi00921340	ISS1:10F1	p31266_1	01/02/2012	p31266_1.cpl	NO
097	wi00903369	ISS1:10F1	p31165_1	01/02/2012	p31165_1.cpl	NO
098	wi00875701	ISS1:10F1	p30942_1	01/02/2012	p30942_1.cpl	NO

099	wi00884699	ISS1:10F1	p31000_1	01/02/2012	p31000_1.cpl	YES
100	wi00834382	ISS1:10F1	p30548_1	01/02/2012	p30548_1.cpl	NO
101	wi00960133	ISS2:10F1	p31557_2	01/02/2012	p31557_2.cpl	NO
102	wi00929140	ISS1:10F1	p31284_1	01/02/2012	p31284_1.cpl	NO
103	wi00948931	ISS1:10F1	p31407_1	01/02/2012	p31407_1.cpl	NO
104	wi00887744	ISS2:10F1	p31026_2	01/02/2012	p31026_2.cpl	NO
105	wi00905600	ISS1:10F1	p31201_1	01/02/2012	p31201_1.cpl	NO
106	wi00869243	ISS1:10F1	p30848_1	01/02/2012	p30848_1.cpl	NO
107	WI00854150	ISS1:10F1	p30468_1	01/02/2012	p30468_1.cpl	NO
108	wi00897176	ISS1:10F1	p30418_1	01/02/2012	p30418_1.cpl	NO
109	wi00903381	ISS1:10F1	p30421_1	01/02/2012	p30421_1.cpl	NO
110	wi00959854	ISS1:10F1	p31556_1	01/02/2012	p31556_1.cpl	NO
111	wi00908598	ISS1:10F1	p31235_1	01/02/2012	p31235_1.cpl	NO
112	wi00903437	ISS1:10F1	p31167_1	01/02/2012	p31167_1.cpl	NO
113	wi00900766	ISS1:10F1	p31159_1	01/02/2012	p31159_1.cpl	NO
114	wi00946558	ISS1:10F1	p31358_1	01/02/2012	p31358_1.cpl	NO
115	wi00932958	ISS1:10F1	p31115_1	01/02/2012	p31115_1.cpl	NO
116	wi00895090	ISS1:10F1	p31105_1	01/02/2012	p31105_1.cpl	NO
117	wi00824257	ISS1:10F1	p30447_1	01/02/2012	p30447_1.cpl	NO
118	wi00895181	ISS1:10F1	p31106_1	01/02/2012	p31106_1.cpl	NO
119	WI00928455	ISS1:10F1	p31297_1	01/02/2012	p31297_1.cpl	NO
120	wi00832106	ISS1:10F1	p30550_1	01/02/2012	p30550_1.cpl	NO
121	wi00953900	ISS1:10F1	p31494_1	01/02/2012	p31494_1.cpl	NO
122	wi00942734	ISS1:10F1	p31409_1	01/02/2012	p31409_1.cpl	NO
123	wi00898200	ISS1:10F1	p31274_1	01/02/2012	p31274_1.cpl	NO
124	wi00882293	ISS1:10F1	p31010_1	01/02/2012	p31010_1.cpl	NO
125	WI00843571	ISS1:10F1	p30627_1	01/02/2012	p30627_1.cpl	NO
126	wi00835294	ISS1:10F1	p30565_1	01/02/2012	p30565_1.cpl	NO
127	WI00836292	ISS1:10F1	p30554_1	01/02/2012	p30554_1.cpl	NO
128	WI00900213	ISS1:10F1	p30656_1	01/02/2012	p30656_1.cpl	NO
129	wi00921295	ISS1:10F1	p31265_1	01/02/2012	p31265_1.cpl	NO
130	wi00957141	ISS1:10F1	p31579_1	01/02/2012	p31579_1.cpl	NO
131	WI00836334	ISS1:10F1	p30481_1	01/02/2012	p30481_1.cpl	NO
132	wi00858335	ISS1:10F1	p30819_1	01/02/2012	p30819_1.cpl	NO
133	wi00859123	ISS1:10F1	p30648_1	01/02/2012	p30648_1.cpl	NO
134	wi00959820	ISS1:10F1	p31562_1	01/02/2012	p31562_1.cpl	NO
135	wi00905297	ISS1:10F1	p31195_1	01/02/2012	p31195_1.cpl	NO
136	wi00907697	ISS1:10F1	p31227_1	01/02/2012	p31227_1.cpl	NO
137	wi00951427	ISS1:10F1	p31478_1	01/02/2012	p31478_1.cpl	NO
138	wi00883604	ISS1:10F1	p30973_1	01/02/2012	p30973_1.cpl	NO
139	wi00962955	ISS1:10F1	p31585_1	01/02/2012	p31585_1.cpl	NO
140	wi00860279	ISS1:10F1	p30789_1	01/02/2012	p30789_1.cpl	NO
141	wi00909476	ISS1:10F1	p31340_1	01/02/2012	p31340_1.cpl	NO
142	wi00925218	ISS1:10F1	p30675_1	01/02/2012	p30675_1.cpl	NO
143	wi00836182	ISS1:10F1	p30450_1	01/02/2012	p30450_1.cpl	NO
144	wi00841273	ISS1:10F1	p30713_1	01/02/2012	p30713_1.cpl	NO
145	WI00889786	ISS1:10F1	p30750_1	01/02/2012	p30750_1.cpl	NO
146	wi00894443	ISS1:10F1	p31093_1	01/02/2012	p31093_1.cpl	NO
147	wi00896420	ISS1:10F1	p30867_1	01/02/2012	p30867_1.cpl	NO
148	wi00941500	ISS1:10F1	p31394_1	01/02/2012	p31394_1.cpl	NO
149	wi00950592	ISS1:10F1	p31499_1	01/02/2012	p31499_1.cpl	NO
150	wi00927678	ISS1:10F1	p31399_1	01/02/2012	p31399_1.cpl	NO
151	wi00930864	ISS1:10F1	p31325_1	01/02/2012	p31325_1.cpl	NO
152	wi00957252	ISS1:10F1	p31530_1	01/02/2012	p31530_1.cpl	NO
153	wi00880836	ISS1:10F1	p30976_1	01/02/2012	p30976_1.cpl	NO
154	wi00865477	ISS1:10F1	p30891_1	01/02/2012	p30891_1.cpl	YES
155	wi00896680	ISS1:10F1	p30357_1	01/02/2012	p30357_1.cpl	NO
156	wi00856702	ISS1:10F1	p30573_1	01/02/2012	p30573_1.cpl	NO
157	wi00897082	ISS1:10F1	p31124_1	01/02/2012	p31124_1.cpl	NO
158	wi00853178	ISS1:10F1	p30719_1	01/02/2012	p30719_1.cpl	NO
159	wi00938555	ISS1:10F1	p30881_1	01/02/2012	p30881_1.cpl	YES
160	WI00839794	ISS1:10F1	p28647_1	01/02/2012	p28647_1.cpl	NO

MDP>LAST SUCCESSFUL MDP REFRESH :2012-01-24 11:17:37 (Local Time)

MDP>USING DEPLIST ZIP FILE DOWNLOADED :2012-01-11 11:07:13 (est)

Avaya Communication Server 1000E signaling server service updates

Product Release: 7.50.17.00

In system patches: 1

PATCH#	NAME	IN_SERVICE	DATE	SPECINS	TYPE	RPM
20	p30260_1	Yes	31/01/12	NO	FRU	cs1000-pi-control-1.00.00.00-00.noarch

In System service updates: 21

PATCH#	IN_SERVICE	DATE	SPECINS	REMOVABLE	NAME
0	Yes	20/01/12	NO	YES	cs1000-linuxbase-7.50.17.16-5.i386.000
1	Yes	20/01/12	NO	YES	cs1000-baseWeb-7.50.17.16-1.i386.001
2	Yes	20/01/12	NO	YES	cs1000-patchWeb-7.50.17.16-2.i386.000
3	Yes	20/01/12	NO	YES	cs1000-dbcom-7.50.17-02.i386.000
4	Yes	20/01/12	NO	yes	cs1000-sps-7.50.17.16-01.i386.000
5	Yes	20/01/12	NO	YES	cs1000-shared-pbx-7.50.17.16-1.i386.000
6	Yes	20/01/12	NO	YES	cs1000-kcv-7.50.17.16-1.i386.000
7	Yes	20/01/12	NO	YES	cs1000-nrsmWebService-7.50.17.16-1.i386.000
8	Yes	20/01/12	NO	YES	cs1000-dmWeb-7.50.17.16-1.i386.000
9	Yes	20/01/12	NO	YES	cs1000-nrsm-7.50.17.16-2.i386.000
10	Yes	20/01/12	NO	YES	cs1000-ipsec-7.50.17.16-1.i386.000
11	Yes	20/01/12	NO	YES	cs1000-ftrpkg-7.50.17.16-5.i386.000
12	Yes	20/01/12	NO	YES	cs1000-tps-7.50.17.16-8.i386.000
13	Yes	20/01/12	NO	YES	cs1000-csmWeb-7.50.17.16-2.i386.000
14	Yes	20/01/12	NO	YES	ipsec-tools-0.6.5-14.el5.3 avaya 1.i386.000
15	Yes	20/01/12	NO	YES	spiritAgent-6.1-1.0.0.108.208.i386.000
16	Yes	20/01/12	NO	YES	cs1000-EmCentralLogic-7.50.17.16-1.i386.000
17	Yes	20/01/12	NO	YES	cs1000-Jboss-Quantum-7.50.17.16-8.i386.000
18	Yes	20/01/12	NO	YES	cs1000-bcc-7.50.17.16-31.i386.000
19	Yes	20/01/12	NO	YES	cs1000-emWeb_6-0-7.50.17.16-9.i386.000
21	Yes	31/01/12	NO	YES	cs1000-vtrk-7.50.17.16-36TMP.i386.000

Avaya Communication Server 1000E system software

Product Release: 7.50.17.00

Base Applications

base	7.50.17	[patched]
NTAFS	7.50.17	
sm	7.50.17	
cs1000-Auth	7.50.17	
Jboss-Quantum	7.50.17	[patched]
lhmonitor	7.50.17	
baseAppUtils	7.50.17	[patched]
dfoTools	7.50.17	
nnnm	7.50.17	
cppmUtil	7.50.17	
oam-logging	7.50.17	[patched]
dmWeb	n/a	[patched]
baseWeb	n/a	[patched]
ipsec	n/a	[patched]
Snmp-Daemon-TrapLib	7.50.17	
ISECSH	7.50.17	
patchWeb	n/a	[patched]
EmCentralLogic	n/a	[patched]

Application configuration: CS+SS+NRS+EM

Packages:

CS+SS+NRS+EM

Configuration version:	7.50.17-00	
cs	7.50.17	
dbcom	7.50.17	[patched]
cslogin	7.50.17	
sigServerShare	7.50.17	[patched]
csv	7.50.17	
tps	7.50.17.16	[patched]
vtrk	7.50.17.16	[patched]
pd	7.50.17	
sps	7.50.17.16	[patched]
ncs	7.50.17	
gk	7.50.17	
nrsm	7.50.17	[patched]

nrsmWebService	7.50.17	[patched]
managedElementWebService	7.50.17	
EmConfig	7.50.17	
emWeb_6-0	7.50.17	[patched]
emWebLocal_6-0	7.50.17	
csmWeb	7.50.17	[patched]
bcc	7.50.17	[patched]
ftrpkg	7.50.17	[patched]
cs1000WebService_6-0	7.50.17	
mscAnnc	7.50.17	
mscAttn	7.50.17	
mscConf	7.50.17	
mscMusc	7.50.17	
mscTone	7.50.17	

©2012 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

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.