



## **Avaya Solution & Interoperability Test Lab**

---

# **Application Notes for Configuring Avaya Communication Server 1000E R7.5, Avaya Network Routing Server, Avaya Session Border Controller Advanced for Enterprise R4.0.5 to support Phonect SIP Trunk Service – Issue 1.0**

## **Abstract**

These Application Notes describes the steps to configure Session Initiation Protocol (SIP) Trunking between Phonect SIP Trunk Service and an Avaya SIP enabled Enterprise Solution. The Avaya solution consists of Avaya Network Routing Server, Avaya Session Border Controller Advanced for Enterprise and Avaya Communication Server 1000E.

Phonect 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 Lab.

**NOTE:** This Application Note focused on the SIP Trunking aspect of the Avaya Session Border Controller Advanced for Enterprise. Advanced enterprise capabilities such as Remote Worker “a.k.a. Remote SIP Endpoints”, dual forking, and TLS/SRTP were not tested. As a result, the Avaya Session Border Controller for Enterprise is also considered Compliance Tested for this solution.

## 1. Introduction

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between Phonect SIP Trunk Service and an Avaya SIP enabled Enterprise Solution. The Avaya solution consists of Avaya Network Routing Server (NRS), Avaya Communication Server 1000E (CS1000E) connected to Phonect SIP Trunk Service via an Avaya Session Border Controller Advanced for Enterprise (ASBCAE). Customers using this Avaya SIP-enabled Enterprise Solution with Phonect 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 NRS, ASBCAE and CS1000E. The enterprise site was configured to use the SIP Trunk to Phonect SIP Trunk Service.

### 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 Phonect
- 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 Phonect to PSTN destinations
- Calls using the G.711A, G.711U and G.729 codec supported by Phonect
- 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
- Caller ID Presentation and Caller ID Restriction
- Call coverage and call forwarding for endpoints at the enterprise site
- Mobile-X call features were not tested

### 2.2. Test Results

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

- When making an outbound call, the ASBCAE has to send 5 INVITES before the Service Providers SIP Trunk Network replies with 100 Trying and 183 Session Progress messaging. This may result in a 7-8 second delay on outbound calls. All unwanted MIME was stripped on outbound calls. Service Provider has now passed this issue to their developers to be resolved

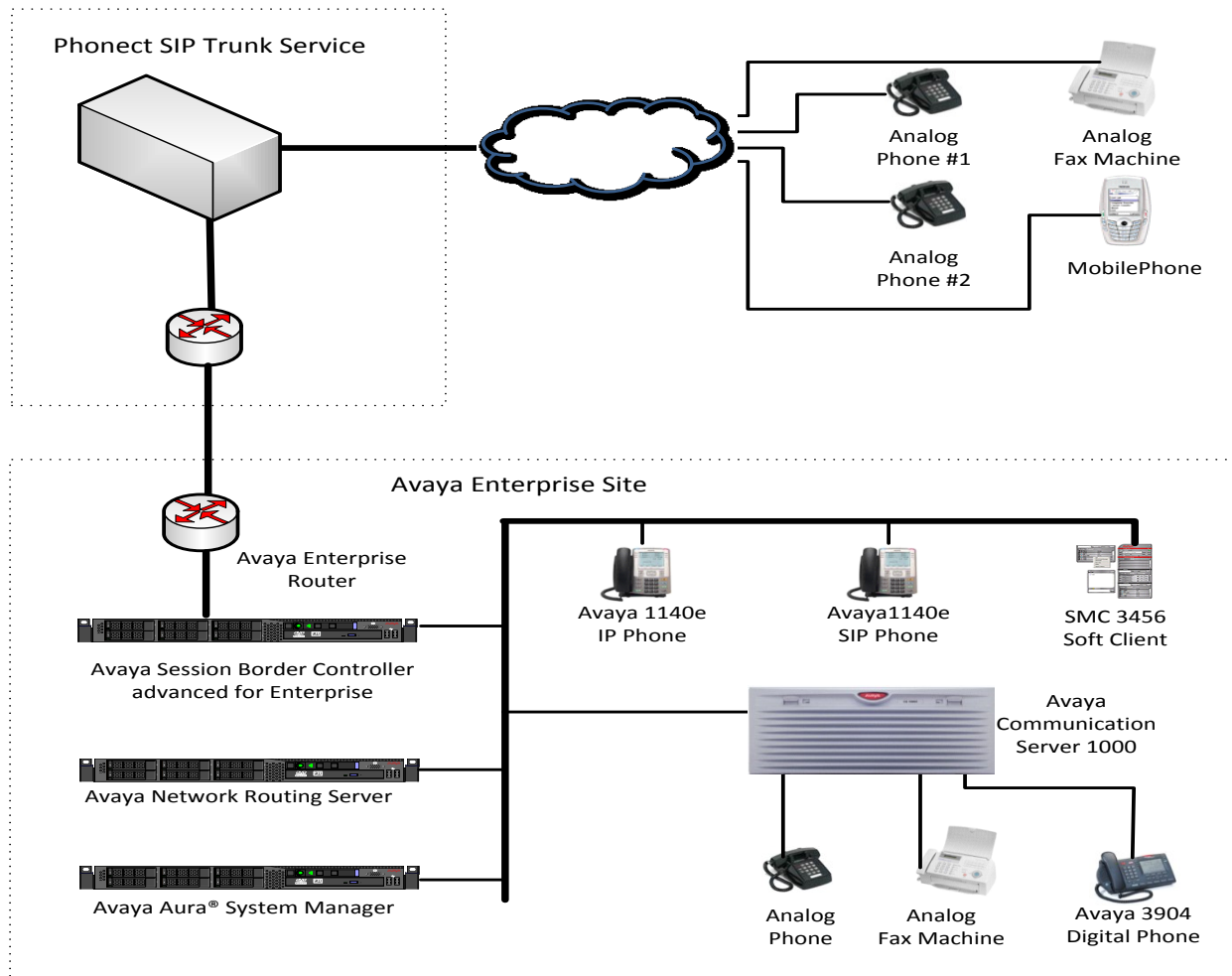
- No inbound toll free numbers were tested as none were available from the Service Provider
- No Emergency Services numbers tested as test calls to these numbers should be pre-arranged with the Operator

## **2.3. Support**

For initial setup for your Avaya solution please contact [leveranse@phonect.no](mailto:leveranse@phonect.no). For technical support send email to [bedriftsupport@phonect.no](mailto:bedriftsupport@phonect.no).

### 3. Reference Configuration

**Figure 1** illustrates the test configuration. The test configuration shows an enterprise site connected to the Phonet SIP Trunks Service. Located at the enterprise site are NRS, ASBCAE and a 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: Phonet SIP Trunk Topology**

## 4. Equipment and Software Validated

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

Equipment	Software
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 Network Routing Server	Avaya Network Routing Server R7.50
Avaya S8800 server	Avaya Session Border Controller Advanced 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	one-X® Communicator -Version cs6.1.0.10
Avaya Analogue Telephone	N/A
Avaya M3904 Digital Telephone	N/A
Phonect SIP Trunk Service	MC22

## 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 NRS. These SIP trunks carry SIP Signaling associated with Phonect SIP Trunk Service. For incoming calls, the NRS receives SIP messages from the ASBCAE; through which Phonect 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 NRS. The NRS directs the outbound SIP messages to the ASBCAE and on to Phonect'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 NRS is presumed to have been previously completed and is not discussed here.

## 5.1. Log in to 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 Phonect'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 customer is setup to use **ISDN** trunks (see below).

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

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

### 5.3. Configure Codec's for Voice and FAX Operation

Phonect SIP Trunk service supports G.711A, G.711U and G.729 voice codec's and T.38 FAX transmissions. Using the Communication Server 1000E element manager sidebar, 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 (squelch 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.

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

### 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)

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

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

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

General | **Voice Codecs** | Fax

**Voice Codecs**

Codec G729: ☒ 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.

☐ Voice Activity Detection (VAD)



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

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

### 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)

## 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 NRS.

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

Add Remove Make Leader Print Refresh

<input type="checkbox"/> Hostname ▲	Type	Deployed Applications	ELAN IP	TLAN IPv4	Role
<input type="checkbox"/> cs1kv13	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**.
- **SIP domain name:** The SIP Domain Name is the SIP Service Domain. The SIP Domain Name configured in the Signaling Server properties must match the Service Domain name configured in the NRS.
- **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 is used when a Network Routing Server is used for registration of the endpoint.
- **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**
- **Proxy or Redirect Server:** Primary TLAN ip address is the Security Module ip address of the NRS. 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.

Managing: 192.168.1.5 Username: admin  
System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration

### 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 Gateway (SIPGw) ▼

SIP domain name: avaya.com \*

Local SIP port: 5060 \* (1 - 65535)

Gateway endpoint name: cs1kv3 \*

Gateway password: \*

Application node ID: 100 \* (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:  Add

Monitor addresses:

Remove

**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" value=""/>	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" value=""/>

## 5.5. Configure Bandwidth Zones

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

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"/>	1000000	BQ	1000000	BQ	SHARED	VTRK	
2 <input type="radio"/>	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 four 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.

Managing: 192.168.1.5 Username: admin  
Dialing and Numbering Plans » Incoming Digit Translation » Customer 00 » Digit Conversion Tree 0 Configuration

### 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
1 <input type="radio"/>	472	5000	
2 <input type="radio"/>	472	5000	
3 <input type="radio"/>	472	5001	
4 <input type="radio"/>	472	5003	
5 <input type="radio"/>	472	5004	
6 <input type="radio"/>	472	5005	
7 <input type="radio"/>	472	5006	
8 <input type="radio"/>	472	5009	

## 5.7. Configure SIP Trunks

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

- Configure a D-Channel Handler (**DCH**); configure using the Communication Server 1000E system terminal and overlay 17
- Configure a SIP trunk Route Data Block (**RDB**); configure using the Communication Server 1000E system terminal and overlay 16
- Configure SIP trunk members; configure using the Communication Server 1000E system terminal and overlay 14
- Configure a 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
OVLN 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.

<b>Overlay 16</b> TYPE: <b>RDB</b> CUST 00 ROUT 1 TYPE RDB CUST 00 <b>ROUT 1</b> DES VIR_TRK <b>TKTP TIE</b> NPID_TBL_NUM 0 ESN NO RPA NO CNVT NO SAT NO RCLS EXT <b>VTRK YES</b> <b>ZONE 00001</b> <b>PCID SIP</b> CRID NO <b>NODE 100</b> DTRK NO <b>ISDN YES</b> <b>MODE ISLD</b> <b>DCH 1</b> <b>IFC SL1</b> 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 <b>ICOG IAO</b> SRCH LIN TRMB YES STEP	<b>ACOD 1111</b> TCPP NO PII NO AUXP NO TARG CLEN 1 BILN NO OABS INST <b>IDC YES</b> 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
OVL 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 CCBD RTDD RBDD RBHD PGND OCBD FLXD FTTC DNDY DNO3 MCBN
    FDSD NOVD CDMR PRED RECA MCDD T87D SBMD PKCH CROD CROD
CPND_LANG ENG
RCO 0
HUNT
PLEV 02
PUID
DANI NO
SPID NONE
AST
IAPG 1
AACS
ACQ
ASID
SFNB
SFRB
USFB
CALB
FCTB
ITNA NO
DGRP
PRI 01
MLWU_LANG 0
```

---continued on next page---

---continued from previous page----

MLNG ENG

DNDR 0

**KEY 00** MCR 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 RMD 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 DNRD OCB DRTD 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:** The 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**

**AVAYA CS1000 Element Manager**

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

**Node ID: 100 - SIP Line Configuration Details**

**General | SIP Line Gateway Settings | SIP Line Gateway Service**

SIP Line Gateway Application: ☒ Enable gateway service on this node

**General**

SIP domain name:  \*

SLG endpoint name:

SLG Group ID:

SLG Local Sip port:  (1 - 65535)

SLG Local Tls port:  (1 - 65535)

**Virtual Trunk Network Health Monitor**

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

Monitor IP:

Monitor addresses:

**SIP Line Gateway Settings**

Security policy:

Number of byte re-negotiation:

Options: ☐ Client authentication

## 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---



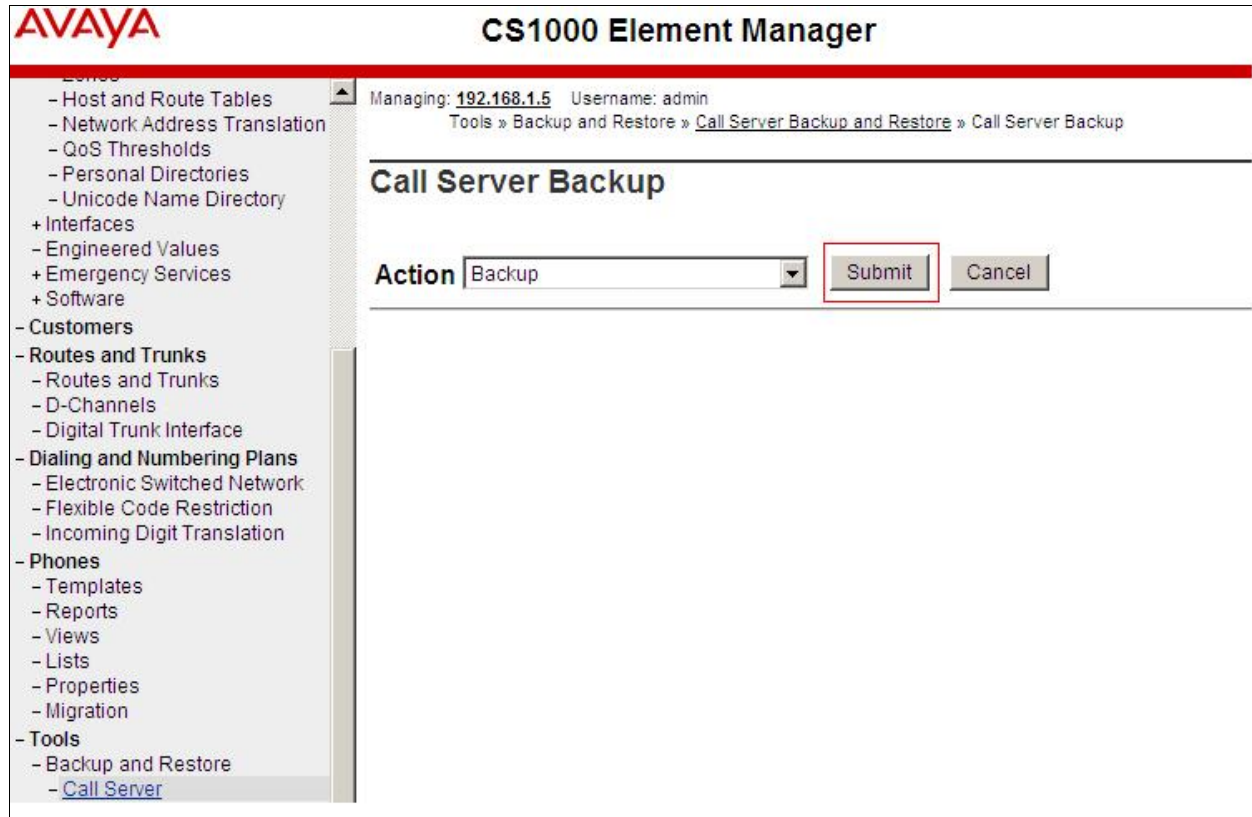
---continued from previous page---

```
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** (not shown) 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', a 'Submit' button (highlighted with a red box), and a 'Cancel' button.

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 Network Routing Server

This section provides the procedure for configuring the NRS to receive and route calls over the SIP trunk between the ASBCAE and the CS1000E. These instructions assume other administration activities have already been completed such as defining system wide settings. The following administration activities will be described.

- Define SIP Domain
- Define Endpoints
- Define Routes

Configuration is accomplished by accessing the browser-based GUI of the Unified Communications Manager (UCM), using the URL **https://<ip-address>/network-login**, where **<ip-address>** is the IP address of UCM. Once logged on click on the NRS Manager link on the UCM front page and log in with the appropriate credentials.

### 6.1. Define SIP Domain

Create a SIP Domain by clicking on **Numbering Plans → Domains**, click **Add** (not shown). Enter a name for your Domain name and click on **Save**. In the test configuration **avaya.com** was used and this is the same domain that is configured on the CS1000E as per **Section 5.4**.

The screenshot displays the Avaya Network Routing Service Manager interface. On the left is a navigation tree with categories like «UCM Network Services», System, and Tools. Under «UCM Network Services», the 'Numbering Plans' section is expanded, and 'Domains' is selected. The main area is titled 'Edit Service Domain'. It contains a 'Domain name' field with 'avaya.com' entered, marked with a red asterisk to indicate it is a required field. Below it is a 'Domain description' field. At the top right, there are radio buttons for 'Active database' and 'Standby database', and the IP address '192.168.1.5'. A breadcrumb trail shows 'Numbering Plans > Domains > Service Domains'. A 'Save' button is located at the bottom right of the form area.

Use the same procedure as above to add a **UDP** and a **CDP** domain for **avaya.com**. These domains are sub-domains to avaya.com. This is the UDP domain created for avaya.com.

**AVAYA Network Routing Service Manager**

Managing: ☐ Active database 192.168.1.5  
☒ Standby database [Numbering Plans » Domains](#)

**Domains**  
 Domains establish the basic structure of your converged network, defined by Service domains, L1 (UDP) and L0 (CDP) domains.

Service Domains (1) | **L1 Domains (UDP) (1)** | L0 Domains (CDP) (1)

Filter by Domain: All service domains

[Add...](#) [Delete](#)

ID	Description	# of L0 Domains	# of Gateway Endpoints	# of Routing Entries	Context
1	udp	1	2	4	avaya.com

1 - 1 of 1 L1 Domain(s) Page 1 of 1 First| Previous|

This is the CDP domain created for avaya.com/udp domain.

**AVAYA Network Routing Service Manager**

Managing: ☐ Active database 192.168.1.5  
☒ Standby database [Numbering Plans » Endpoints](#)

**Search for Endpoints**

Enter an endpoint ID (use \* for all) and click Search. You may narrow the search by specifying a particular domain.

Endpoint ID: \*

Limit results to Domain: avaya.com / udp / cdp

Results per page: 50

**Gateway Endpoints (2)** | **User Endpoints (0)**

[Add...](#) [Delete](#) [SIP phone context...](#)

## 6.2. Define Endpoints

For this test configuration two endpoints were configured on the NRS. A static endpoint was configured for the ASBCAE and a dynamic endpoint for the CS1000E. Create an Endpoint by clicking on **Numbering Plans** → **Endpoints**. Select the domain and sub-domains (e.g. **avaya.com/udp/cdp**) where you want to create the endpoint and click **Add**.

The screenshot displays the Avaya Network Routing Service Manager (NRS) web interface. The left sidebar shows the navigation menu with 'Numbering Plans' and 'Endpoints' highlighted. The main content area is titled 'Search for Endpoints' and includes a search bar with the placeholder text 'Enter an endpoint ID (use \* for all) and click Search. You may narrow the search by specifying a particular domain.' Below the search bar, there are dropdown menus for 'Limit results to Domain' set to 'avaya.com', and 'udp' and 'cdp' sub-domains. At the bottom, there are tabs for 'Gateway Endpoints (2)' and 'User Endpoints (0)', with an 'Add...' button highlighted under the Gateway Endpoints tab.

## 6.2.1. Configure Static Endpoint for Avaya Session Border Controller Advanced for Enterprise

This section shows how to add a static endpoint for the ASBCAE. Enter the following values and use default values for remaining fields.

- **End point name:** **Sipera** was used in this configuration
- **Description:** Enter a descriptive name
- **Static endpoint address:** This is the ip address of ASBCAE. This has been hidden for security purposes.
- **SIP support:** Set this to **Static SIP endpoint**
- **SIP mode:** Set this to **Proxy mode**
- **SIP TCP transport enabled:** Click the box to enable
- **SIP UDP transport enabled:** Click the box to enable

Click on **Save** (not shown). The two screenshots below show the ASBCAE Endpoint configuration used for the testing.

AVAYA Network Routing Service Manager

Managing: ☐ Active database 192.168.1.5  
☒ Standby database

Numbering Plans > Endpoints > Gateway Endpoint

Edit Gateway Endpoint avaya.com / udp / cdp

End point name: Sipera \*

Description:

Trust Node: ☒

Tandem gateway endpoint name: Not Applicable

Endpoint authentication enabled: Authentication off

Authentication password:

E.164 country code:

E.164 area code:

AVAYA Network Routing Service Manager

Managing: ☐ Active database 192.168.1.5  
☒ Standby database

Numbering Plans > Endpoints > Gateway Endpoint

Edit Gateway Endpoint avaya.com / udp / cdp

Private Special number Z training code length: (0-31)

Static endpoint address type: IP version 4

Static endpoint address:

H.323 support: H.323 not supported

SIP support: Static SIP endpoint

SIP mode: ☒ Proxy Mode  
☐ Redirect Mode

SIP TCP transport enabled: ☒

SIP TCP port: 5060

SIP UDP transport enabled: ☒

SIP UDP port: 5060

## 6.2.2. Configure Dynamic Endpoint for Avaya Communication Server 1000E

This section shows how to add a dynamic endpoint for the CS1000E. Enter the following values and use default values for remaining fields.

- **End point name:** cs1kvl3 was used in this configuration
- **Description:** Enter a descriptive name
- **SIP support:** Set this to **Dynamic SIP endpoint**
- **SIP mode:** Set this to **Proxy mode**
- **SIP TCP transport enabled:** Click the box to enable
- **SIP UDP transport enabled:** Click the box to enable

Click on **Save** (not shown). The two screenshots below show the CS1000E Endpoint configuration used for the testing.

AVAYA Network Routing Service Manager

Managing: ☐ Active database 192.168.1.5  
☒ Standby database

Numbering Plans » Endpoints » Gateway Endpoint

Edit Gateway Endpoint avaya.com / udp / cdp )

End point name: cs1kvl3 \*

Description:

Trust Node: ☒

Tandem gateway endpoint name: Not Applicable

Endpoint authentication enabled: Authentication off

Authentication password:

E.164 country code:

E.164 area code:

E.164 international dialing access code:

AVAYA Network Routing Service Manager

Managing: ☐ Active database 192.168.1.5  
☒ Standby database

Numbering Plans » Endpoints » Gateway Endpoint

Edit Gateway Endpoint avaya.com / udp / cdp )

Static endpoint address type: IP version 4

Static endpoint address:

H.323 support: H.323 not supported

SIP support: Dynamic SIP endpoint

SIP mode: ☒ Proxy Mode  
☐ Redirect Mode

SIP TCP transport enabled: ☒

SIP TCP port: 5060

SIP UDP transport enabled: ☒

SIP UDP port: 5060

SIP TLS transport enabled: ☐



## 6.3. Define Routes

Routes need to be defined for each endpoint. Routes are how the NRS routes out calls to an endpoint based on digits it receives.

### 6.3.1. Configure Route to the Avaya Communication Server 1000E

This section shows how to add routes to the CS1000E. This is incoming calls from the PSTN to the CS1000E. Create a Route by clicking on **Numbering Plans** → **Routes**. Select the domain and sub-domains (e.g. **avaya.com/udp/cdp**) and endpoint where you want to create the route (e.g. **cs1kv13**) and click **Add**.

The screenshot shows the Avaya Network Routing Service Manager interface. On the left is a navigation tree with 'Numbering Plans' and 'Routes' highlighted. The main area shows 'Managing: Standby database' and '192.168.1.5'. Below is a 'Search for Routing Entries' section with a search bar and filters. The 'Limit results to Domain' is set to 'avaya.com / udp / cdp' and 'Endpoint Name' is 'cs1kv13'. At the bottom, there are three tabs: 'Routing Entries (1)', 'Default Routes (0)', and 'Emergency Fallback Routes (0)'. The 'Add...' button in the 'Routing Entries' tab is highlighted with a red box.

Enter the following values

- **DN type:** Select **Private level 0 regional (CDP steering code)**
- **DN prefix:** **47** prefix matches the DN extensions on the test sets on the CS1000E. This also matches the first 2 digits of the DDI range given for the test
- **Route cost:** **1** is used as this is the only route available

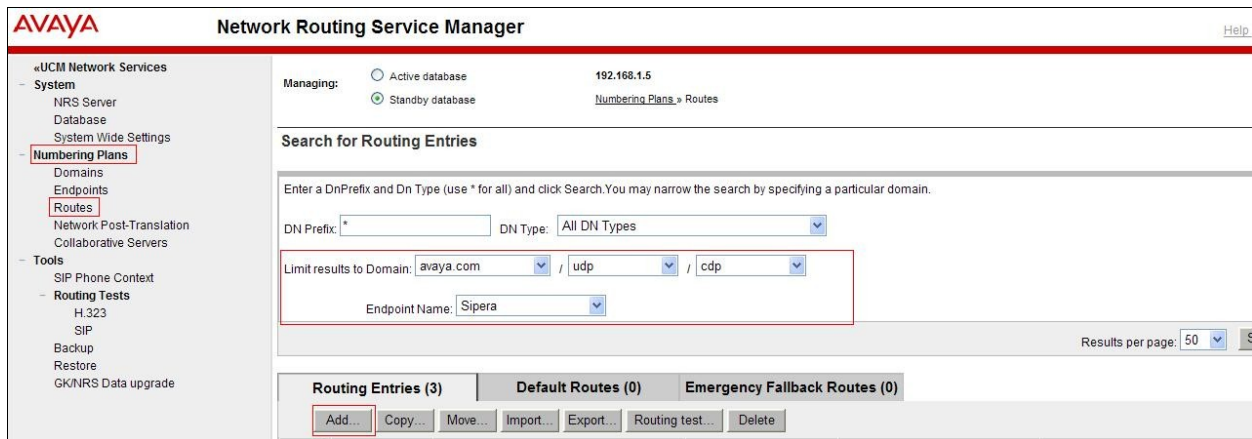
Click on **Save**.

The screenshot shows the 'Edit Routing Entry' form in the Avaya Network Routing Service Manager. The breadcrumb trail is 'Numbering Plans > Routes > Routing Entry'. The form title is 'Edit Routing Entry ( avaya.com / udp / cdp / cs1kv13 )'. The form contains three fields: 'DN type' set to 'Private level 0 regional (CDP steering code)', 'DN prefix' set to '47', and 'Route cost' set to '1'. A red box highlights these three fields. At the bottom right, there is a 'Save' button highlighted with a red box. A note at the bottom left says '\* Required value.'.



## 6.3.2. Configure Route to the Avaya Session Border Controller Advanced for Enterprise

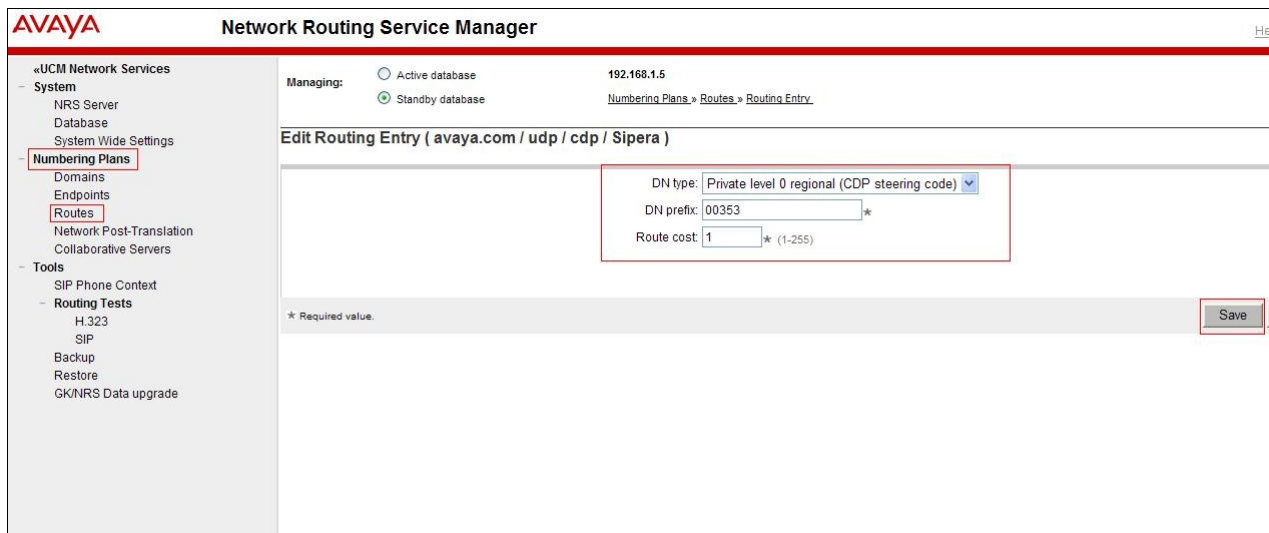
This section shows how to add routes to the ASBCAE. This is outgoing calls from the CS1000E to the PSTN. Create a Route by clicking on **Numbering Plans** → **Routes**. Select the domain and sub-domains (e.g. **avaya.com/udp/cdp**) and endpoint where you want to create the route (e.g. **Sipera**) and click **Add**.



Enter the following values; this is an example of E.164 International call.

- **DN type:** Select **Private level 0 regional (CDP steering code)**
- **DN prefix:** **00353** prefix matches the digits going to be dialed for an international call
- **Route cost:** **1** is used as this is the only route available

Click on **Save**.



This is an example of a local call using CDP dial plan, only CDP dialling worked for local calls.

- **DN type:** Select **Private level 0 regional (CDP steering code)**
- **DN prefix:** **800** prefix matches the digits going to be dialed for a local call
- **Route cost:** **1** is used as this is the only route available

Click on **Save**.

The screenshot shows the Avaya Network Routing Service Manager web interface. The left sidebar contains a navigation menu with categories like «UCM Network Services», System, Numbering Plans, and Tools. The 'Numbering Plans' section is expanded, showing 'Routes' as the selected option. The main content area is titled 'Edit Routing Entry ( avaya.com / udp / cdp / Sipera )'. It features a 'Managing:' section with radio buttons for 'Active database' and 'Standby database'. Below this, the 'DN type' is set to 'Private level 0 regional (CDP steering code)', the 'DN prefix' is '800', and the 'Route cost' is '1'. A 'Save' button is located at the bottom right of the form. A red box highlights the 'DN type', 'DN prefix', and 'Route cost' fields. Another red box highlights the 'Save' button.

AVAYA Network Routing Service Manager

Managing: ☐ Active database 192.168.1.5  
☒ Standby database [Numbering Plans > Routes > Routing Entry](#)

Edit Routing Entry ( avaya.com / udp / cdp / Sipera )

DN type: Private level 0 regional (CDP steering code) ▼  
DN prefix: 800 \*  
Route cost: 1 \* (1-255)

\* Required value.

Save

## 7. Configure Avaya Session Border Controller Advanced for Enterprise

This section describes the configuration of the Session Border Controller. The ASBCAE is administered using the E-SBC Control Center.

### 7.1. Access Avaya Session Border Controller Advanced for Enterprise

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



Select **UC-Sec Control Center** and enter the **Login ID** and **Password**.



## 7.2. Define Network Information

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

- Click on **Add IP**
- Define the internal IP address with screening mask and assign to interface **A1**
- Select Save (not shown) to save the information
- Click on **Add IP**
- Define the external IP address (not shown) with screening mask and assign to interface **B1**
- Select Save (not shown) to save the information
- Select the **Network Configuration** tab and change the state of interfaces A1 and B1 to **Enabled**
- Click on **System Management** in the main menu
- Select **Restart Application** indicated by an icon in the status bar

The screenshot shows the UC-Sec Control Center interface. The left sidebar contains a tree view with categories like Backup/Restore, System Management, Global Parameters, Global Profiles, and Device Specific Settings. Under Device Specific Settings, 'Network Management' is selected. The main panel is titled 'Device Specific Settings > Network Management: GSSCP\_03'. It has two tabs: 'Network Configuration' (active) and 'Interface Configuration'. A warning message states: 'Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management.' Below this, there are fields for 'A1 Netmask' (255.255.255.0), 'A2 Netmask', 'B1 Netmask' (255.255.255.128), and 'B2 Netmask'. An 'Add IP' button is present. Below the buttons is a table with columns: IP Address, Public IP, Gateway, and Interface. The table contains two rows: one for interface A1 with IP 10.10.3.30 and gateway 10.10.3.1, and another for interface B1 with IP xxx.xxx.xxx.xxx and gateway xxx.xxx.xxx.xxx. Each row has a red 'X' icon in the interface column.

IP Address	Public IP	Gateway	Interface
10.10.3.30		10.10.3.1	A1
xxx.xxx.xxx.xxx		xxx.xxx.xxx.xxx	B1

## 7.3. Define Interfaces

To define the signaling and media interfaces for the ASBCAE, 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 an **internal** interface IP address defined in **Section 7.2**
- Select **UDP** and **TCP** port numbers, **5060** is used internally in the lab
- Select **Add Signalling Interface**
- In the **Name** field enter a descriptive name for the external signalling interface
- Select an **external** interface IP address (not shown) defined in **Section 7.2**
- Select **UDP** and **TCP** port numbers

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 contains a tree view of the system's configuration options, with 'Signaling Interface' highlighted under 'Device Specific Settings'. The main content area displays the 'Signaling Interface' configuration for device 'GSSCP\_03'. It features a table with columns for Name, Signaling IP, TCP Port, UDP Port, TLS Port, and TLS Profile. Two entries are listed: 'Int\_Sig' and 'Ext\_Sig'. An 'Add Signaling Interface' button is located in the top right corner of the table area.





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	5060	5060	---	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 an **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 an **external** interface IP address (not shown) defined in **Section 7.2**
- Select RTP port ranges for the media path with the Phonect SIP Trunk Service

The screenshot shows the UC-Sec Control Center web interface. The top navigation bar includes tabs for Alarms, Incidents, Statistics, Logs, Diagnostics, and Users. The left sidebar contains a tree view of configuration options, with 'Media Interface' selected under 'Device Specific Settings'. The main content area is titled 'Media Interface' and displays a table of configured interfaces. A warning message states: 'Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.' An 'Add Media Interface' button is located above the table.

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 Phonect SIP Trunk Service and the NRS. 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 NRS to the Phonect 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 Phonect SIP Trunk Service to the NRS
- 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 area displays the configuration for the 'SM3\_CS' profile. The 'General' tab is active, showing a table of settings.

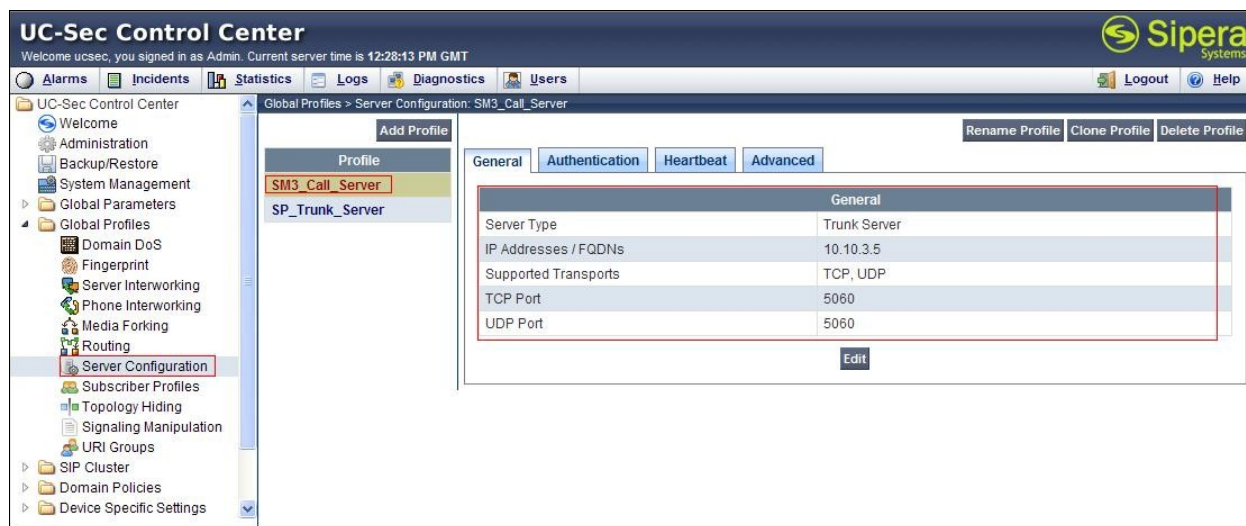
General	
Hold Support	RFC2543
180 Handling	None
181 Handling	None
182 Handling	None
183 Handling	None
Refer Handling	No
3xx Handling	No
Diversion Header Support	No
Delayed SDP Handling	No
T.38 Support	Yes
URI Scheme	SIP



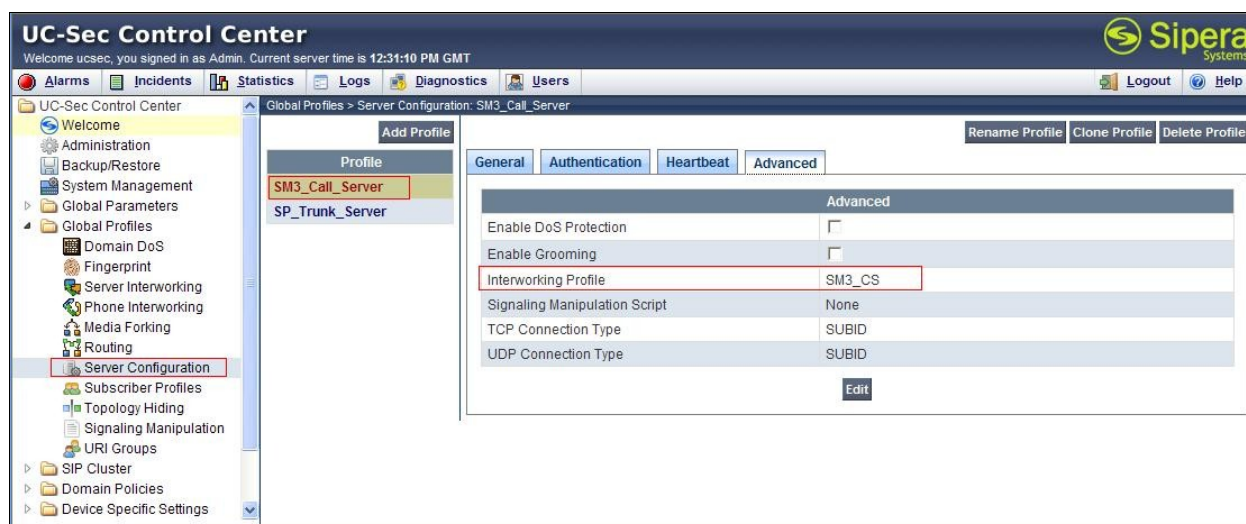
## 7.5. Define Servers

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

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



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





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

- Select **Add Profile**
- In the **Name** field enter a descriptive name for the Phonect SIP Trunk Service
- Select the Phonect SIP Trunk Service IP address in the IP address field
- Select a **UDP** port for SIP signaling

The screenshot shows the UC-Sec Control Center interface. The left sidebar contains a tree view with 'Server Configuration' highlighted. The main area displays the 'Global Profiles > Server Configuration: SP\_Trunk\_Server' page. The 'Add Profile' button is visible. The 'General' tab is selected, showing the following configuration:

General	
Server Type	Trunk Server
IP Addresses / FQDNs	xxx.xxx.xxx.xxx
Supported Transports	UDP
UDP Port	5060

An 'Edit' button is located at the bottom right of the configuration table.

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

- Select **MIME new** for **Signaling Manipulation Script**, this will be discussed in **Section 7.8**

The screenshot shows the same UC-Sec Control Center interface, but with the 'Advanced' tab selected. The configuration is as follows:

Advanced	
Enable DoS Protection	<input type="checkbox"/>
Enable Grooming	<input type="checkbox"/>
Interworking Profile	SP_Trunk
Signaling Manipulation Script	MIME new
UDP Connection Type	SUBID

An 'Edit' button is located at the bottom right of the configuration table.

## 7.6. Define Routing

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

- Select **Add Profile**
- In the **Name** field enter a descriptive name for the NRS
- Enter the NRS TLAN IP address and port in the **Next Hop Server 1** field
- Check the **Next Hop in Dialog** box
- Select TCP for the **Outgoing Transport**

**Note:** Unless default port 5060 is used, this must be included in the next hop IP address.

**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.

UC-Sec Control Center

Welcome ucsec, you signed in as Admin. Current server time is 10:32:08 AM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

Global Profiles > Routing: Call Server

Add Profile Rename Profile Clone Profile Delete Profile

Routing Profiles

default

Call Server

Trunk Server

Click here to add a description.

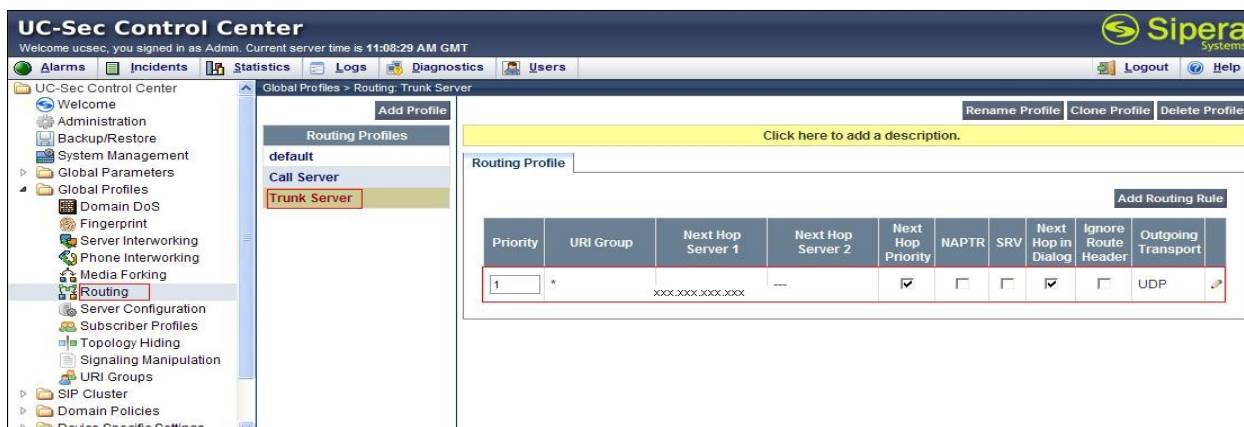
Routing Profile

Add Routing Rule

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	*	10.10.3.5	---	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	TCP

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

- Select **Add Profile**
- In the **Name** field enter a descriptive name for the Phonect SIP Trunk Service
- Enter the Phonect IP address (not shown) in the **Next Hop Server 1** field
- Select **UDP** for the **Outgoing Transport**

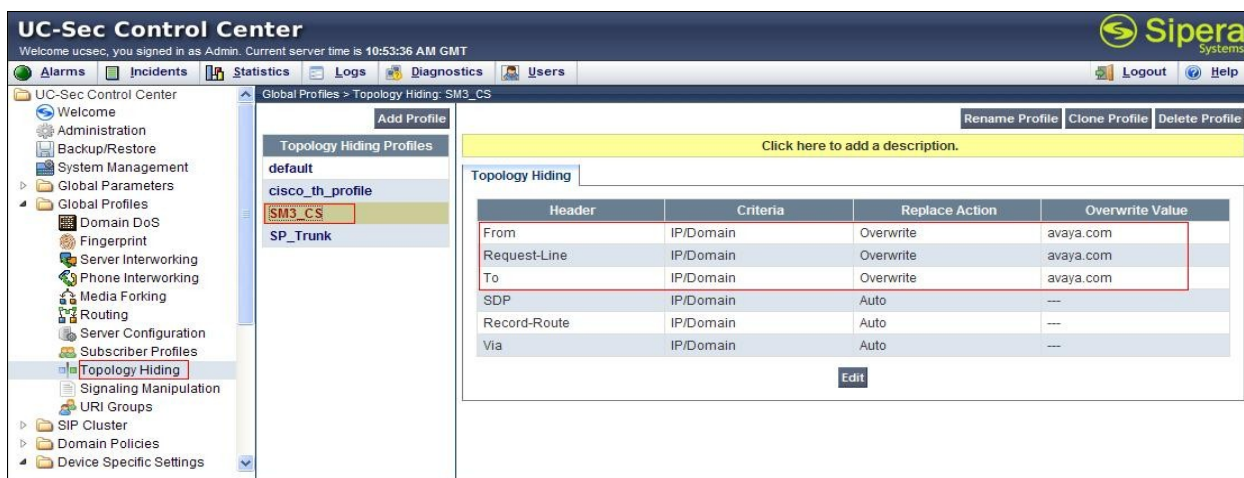


## 7.7. Topology Hiding

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

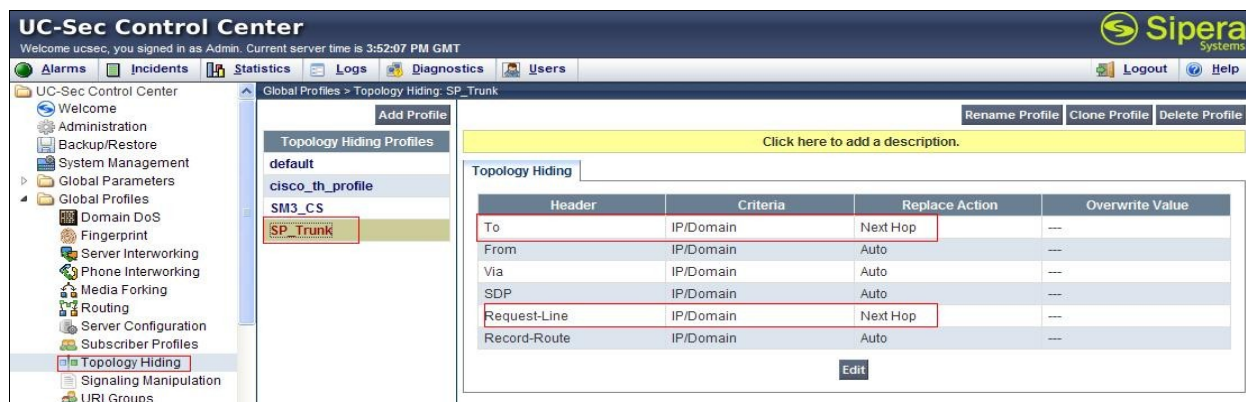
- Select **Add Profile**
- In the **Name** field enter a descriptive name for the NRS
- **Overwrite** the **From** field with a domain name for the Trunk Server, in test **avaya.com** was used
- **Overwrite** the **Request-Line** field and **To** field with a local domain name, in test **avaya.com**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

**Note:** The different domain names could be used for the enterprise and the Phonect network.



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

- Select **Add Profile**
- In the **Name** field enter a descriptive name for the Phonect 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



## 7.8. Signaling Manipulation Scripts

This feature adds the ability to add, change and delete any of the headers and other information in a SIP message. During test, a script was written to remove unwanted MIME from INVITES on outbound calls.

From the lefthand menu select **Global Profiles → Signaling Manipulation** and click on **Add Script**. The script shown below was used for this test:



This script was then associated with **Server Configuration – Phonect side** defined in **Section 7.5** under Signaling Manipulation Script.

## 7.9. Server Flows

Server Flows combine the previously defined profiles into an outgoing flow from the NRS to the Phonect SIP Trunk Service and an incoming flow from the Phonect SIP Trunk Service to the NRS. 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 Phonect SIP Trunk Service
- In the **Signalling Interface** field, select the SIP signalling interface for the NRS
- In the **Media Interface** field, select the media interface for the NRS
- In the **End Point Policy Group** field, select the default-low End Point Policy Group
- In the **Routing Profile** field, select the routing profile of the Phonect SIP Trunk Service
- In the **Topology Hiding Profile** field, select the topology hiding profile of the NRS

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 NRS
- In the **Signalling Interface** field, select the SIP signalling interface for the Phonect SIP Trunk Service
- In the **Media Interface** field, select the media interface for the Phonect SIP Trunk Service
- In the **End Point Policy Group** field, select the default-low End Point Policy Group
- In the **Routing Profile** field, select the routing profile of the NRS
- In the **Topology Hiding Profile** field, select the topology hiding profile of the Phonect SIP Trunk Service

**UC-Sec Control Center**  
Welcome ucsec, you signed in as Admin. Current server time is 11:16:32 AM GMT

Alarms Incidents Statistics Logs Diagnostics Users Logout Help

Device Specific Settings > End Point Flows: GSSCP\_03

**Subscriber Flows** **Server Flows**

Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signalling 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		

Server Configuration: SP\_Trunk\_Server

Priority	Flow Name	URI Group	Transport	Remote Subnet	Received Interface	Signalling 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	default-low	Call Server	SP_Trunk	None		



## 8. Phonect SIP Service Provider Configuration

The setup for the use of Phonect is by using the SIP trunk with an authenticated service. The configuration of Phonect's authentication service 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 Phonect's equipment and system configuration please contact an authorised Phonect representative.

## 9. Verification

### 9.1. Verify Avaya Communication Server 1000E Operational Status

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

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 navigation pane on the left lists various system components, with "System" expanded and "Maintenance" selected. The main content area is titled "Maintenance" and contains two tabs: "Select by Overlay" (active) and "Select by Functionality". The "Select by Overlay" tab displays a table of LDs (Line Drivers) with "LD 96 - D-Channel" highlighted. The "Select by Functionality" tab displays a table of functions with "D-Channel Diagnostics" highlighted.

<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
<b>LD 96 - D-Channel</b>
LD 117 - Ethernet and Alarm Management
LD 135 - Core Common Equipment
LD 137 - Core Input/Output
LD 143 - Centralized Software Upgrade

<Select Group>
<b>D-Channel Diagnostics</b>
MSDL Diagnostics
TMDI Diagnostics

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**

The screenshot shows the Avaya CS1000 Element Manager interface. The top header displays the Avaya logo and the title 'CS1000 Element Manager'. Below the header, the user is logged in as 'admin' with IP '192.168.1.5'. The main content area is titled 'D-Channel Diagnostics'. It features a table with three columns: 'Diagnostic Commands', 'Command Parameters', and 'Action'. The 'Diagnostic Commands' column lists several commands, including 'Status for D-Channel (STAT DCH)', 'Disable Automatic Recovery (DIS AUTO)', 'Enable Automatic Recovery (ENL AUTO)', 'Test Interrupt Generation (TEST 100)', and 'Establish D-Channel (EST DCH)'. The 'Command Parameters' column has checkboxes for 'ALL' and 'FDL'. The 'Action' column contains 'Submit' buttons for each command. Below the table, there is a status table with columns: DCH, DES, APPL\_STATUS, LINK\_STATUS, AUTO\_REC, PDCH, and BDCH. The first row shows values: C, 001, SIP\_DCH, OPER, EST, ACTV, and AUTO. At the bottom, there is a text area showing the command 'STAT DCH' and the message 'Command executed successfully.'

## 10. Conclusion

These Application Notes describe the configuration necessary to connect the Avaya Communication Server 1000E, Avaya Network Routing Server and Avaya Session Border Controller Advanced for Enterprise to Phonect SIP Service. Interoperability testing of the sample configuration was completed with successful results for the Phonect 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] IP Peer Networking Installation and Commissioning, Release 7.5, Document Number NN43001-313, available at <http://support.avaya.com>
- [2] Network Routing Service Fundamentals, Release 7.5, Document Number NN43001-130, Issue 03.02, available at <http://support.avaya.com>
- [3] 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>
- [4] Signaling Server and IP Line Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-125, available at <http://support.avaya.com>
- [5] Unified Communications Management Common Services Fundamentals, Avaya Communication Server 1000E Release 7.5, Document Number NN43001-116, available at <http://support.avaya.com>
- [6] E-SBC (Avaya Session Border Controller Advanced for Enterprise) Administration Guide, November 2011
- [7] 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](mailto:devconnect@avaya.com).