Avaya Solution & Interoperability Test Lab

Application Notes for Configuring Avaya Communication Server 1000 R7.6 with Avaya Aura® Session Manager R6.3 and Avaya Session Border Controller for Enterprise R6.2 to support Telenor SIP Trunk Service - Issue 1.0

Abstract

These Application Notes describe the steps to configure Session Initiation Protocol (SIP) trunking between an Avaya SIP enabled enterprise solution and Telenor SIP Trunk service. The Avaya solution consists of Avaya Aura® Session Manager and Avaya Communication Server 1000 connected to an Avaya Session Border Controller for Enterprise. Telenor is a member of the Global SIP Service Provider program.

Readers should pay attention to Section 2, in particular the scope of testing as outlined in Section 2.1 as well as the observations noted in Section 2.2, to ensure that their own use cases are adequately covered by this scope and results.

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

1. Introduction

These Application Notes describe the necessary steps to configure Session Initiation Protocol (SIP) trunking between an Avaya SIP enabled enterprise solution and Telenor SIP Trunk service. The Avaya solution consists of Avaya Communication Server 1000 (CS1000), Avaya Aura® Session Manager and Avaya Session Border Controller for Enterprise (Avaya SBCE) connected to the Telenor SIP Trunk service. Customers using this Avaya SIP enabled enterprise solution with the Telenor SIP Trunk service are able to place and receive PSTN calls via a dedicated Internet connection using the SIP protocol. This converged network solution is an alternative to traditional PSTN trunks. The approach normally results in lower cost and a more flexible implementation for the enterprise customers.

2. General Test Approach and Test Results

The general test approach was to configure a simulated enterprise site using an Avaya SIP telephony solution consisting of CS1000, Session Manager, and the Avaya SBCE. The enterprise site was configured to use the SIP Trunk service provided by Telenor, with all PSTN traffic transiting via the Telenor SIP Trunk service.

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 calls to the enterprise site from the PSTN were routed to the DID numbers assigned by Telenor. Incoming PSTN calls were terminated on Digital, Analog, UNIStim and SIP telephones at the enterprise side.
- Outgoing calls from the enterprise site were completed via Telenor to PSTN telephones. Outgoing calls from the enterprise to the PSTN were made from Digital, Analog, UNIStim and SIP telephones.
- Calls were made using G.711A and G.711MU codec's.
- 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 IVR menu progression.
- User features such as hold and resume, transfer, conference, call forwarding, etc.
- Caller ID Presentation and Caller ID Restriction.
- Call coverage and call forwarding for endpoints at the enterprise site.
- Transmission and response of SIP OPTIONS messages sent by Telenor requiring Avaya response and sent by Avaya requiring Telenor response.

2.2. Test Results

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

- During testing it was observed that the CS1000 failed to respond to UPDATE sent from Telenor. This issue arose within a certain call scenario where an outbound call was placed from CS1000 to the Telenor platform where multiple call-forwarding on various phonesets within the Telenor platform was taking place. Telenor are sending 180 Ringing without SDP in response to the original CS1000 Invite. Telenor are then sending 180 Ringing with SDP on the second call forward, however this is ignored by CS1000 as 180 multi ringing is not supported by the CS1000 as the CS1000 expects 183 Session Progress with SDP. With the final call-forward on the Telenor platform, an UPDATE with SDP is sent to the CS1000 and the CS1000 fails to generate a response in offer to the UPDATE sent by Telenor. 500 Server Internal Error is then sent from Telenor due to the lack of response to the UPDATE and the call is torn down. As the CS1000 does not support 180 multi ringing, the second 180 Ringing with SDP is ignored hence the reason why UPDATE with SDP is rejected by the CS1000 resulting in the call failure. This issue has been raised with the CS1000 Design Team under **wi01200405** and a patch **VTRK SU version "cs1000-vtrk-7.65.16.23-58.i386.000.ntl"** is now available to resolve this issue. It is required that **VTRK SU version "cs1000-vtrk-7.65.16.23-58.i386.000.ntl"** or higher be used on all SSG signalling servers to ensure proper support of 180 multi ringing on the CS1000. For more information on how to obtain and apply this patch please visit http://support.avaya.com.
- The CS1000 default configuration will not allow a blind transfer to be executed (incoming SIP Service Provider trunk to outgoing SIP Service Provider trunk) if the SIP Service Provider in question does not support the SIP UPDATE method. With the installation of plugin 501 on the CS1000, the blind transfer will be allowed and the call will be completed. The limitation of this plugin is that no ringback is provided to the originator of the call for the duration that the destination set is ringing. In addition to plugin 501, it is required that **VTRK SU version "cs1000-vtrk-7.65.16.22.-4.i386.000.ntl"** or higher be used on all SSG signalling servers to ensure proper operation of the blind transfer feature. The use of plugin 501 does not restrict the use of the SIP UPDATE method of blind transfer to other parties that do happen to support the UPDATE method, but rather extends support to those parties that do not. Note that plugin 501 is independent of and does not require the Global Plugin Package 409.
- On outbound international calls from the CS1000, it was observed that the numbering format in the Contact Header contained "00" instead of "+". Telenor require all international numbering format to be E.164. A SigMa script was required on the Avaya SBCE to convert the "00" to "+" in the Contact Header. The details of this SigMa script are outlined in **Section 7.2.7**.
- Telenor required the removal of History-Info Headers from all messaging. The removal of all History-Info Headers was performed by creating a SigMa script on the Avaya SBCE. The details of this SigMa script are outlined in **Section 7.2.7**.
- 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.
- All unwanted MIME was stripped on outbound calls using the Adaptation Module in Session Manager.

2.3. Support

For technical support on the Avaya products described in these Application Notes visit http://support.avaya.com.

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 Telenor's SIP Trunk service. Located at the Enterprise site is an Avaya SBCE, Session Manager and CS1000. Endpoints are Avaya 1140 Series IP Deskphones, Avaya 1200 Series IP Deskphones (with UNIStim and SIP firmware), Avaya IP Softphones (Avaya 3456 IP Softphone, 2050 IP Softphone), Avaya Digital Deskphone, 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.

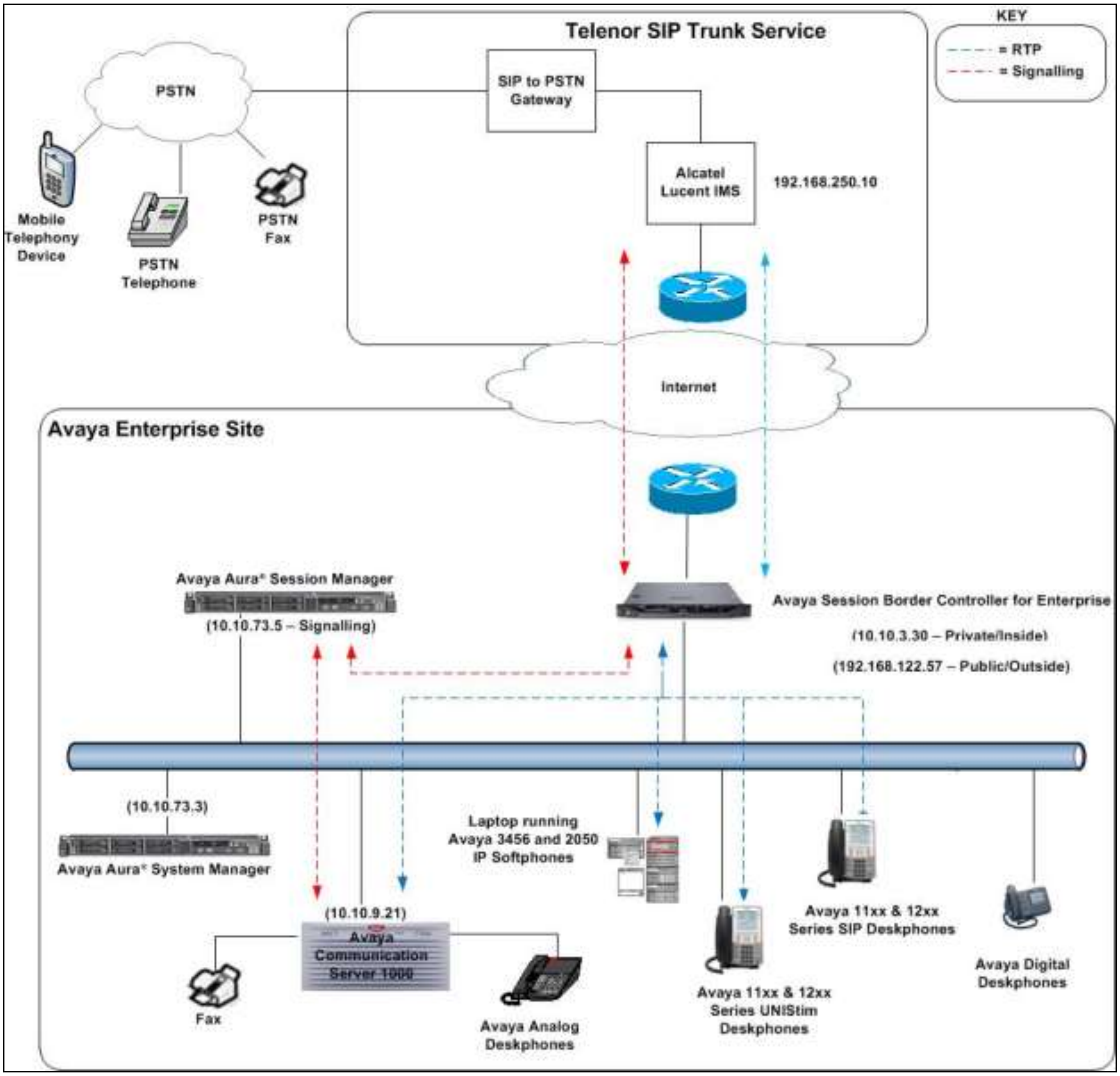

Telenor SIP Trunk Service
KEY
= RTP
= Signalling
PSTN
SIP to PSTN Gateway
Alcatel Lucent IMS
192.168.250.10
Mobile Telephony Device
PSTN Telephone
PSTN Fax
Internet
Avaya Enterprise Site
Avaya Aura® Session Manager
(10.10.73.5 – Signalling)
Avaya Session Border Controller for Enterprise
(10.10.3.30 – Private/Inside)
(192.168.122.57 – Public/Outside)
(10.10.73.3)
Avaya Aura® System Manager
Laptop running Avaya 3456 and 2050 IP Softphones
(10.10.9.21)
Avaya Communication Server 1000
Fax
Avaya Analog Deskphones
Avaya 11xx & 12xx Series UNIStim Deskphones
Avaya 11xx & 12xx Series SIP Deskphones
Avaya Digital Deskphones

Figure 1: Test Setup Telenor SIP Trunk Service to Avaya Enterprise

4. Equipment and Software Validated

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

Equipment	Software
Dell PowerEdge R620 running Avaya Aura® Session Manager on VM Version 8	R6.3.11 - 6.3.11.0.631103
Dell PowerEdge R620 running Avaya Aura® System Manager on VM Version 8	R6.3.11 - Build No. - 6.3.0.8.5682-6.3.8.4411 Software Update Revision No: 6.3.11.8.1.2871
Avaya Session Border Controller for Enterprise	Version 6.2.1.Q18
Avaya Communication Server 1000 running on CP+PM server as co-resident configuration	Avaya Communication Server 1000 R7.6 Version 7.65.P Deplist: CPL_X21_07_65P All CS1000 patches listed in **Appendix A**
Avaya Communication Server 1000 Media Gateway	CSP Version: MGCC DC01 MSP Version: MGCM AB02 APP Version: MGCA BA18 FPGA Version: MGCF AA22 BOOT Version: MGCB BA18 DBL1 Version: DSP2 AB07
Avaya 1140e and 1230 UNIStim Deskphones	FW: 0625C8A
Avaya 1140e and 1230 SIP Deskphones	FW: 04.04.18.00.bin
Avaya IP Softphone 3456	Version 2.6 build 53715
Avaya 2050 IP Softphone	Release 4.3.0081
Avaya Analogue Telephone	N/A
Avaya Digital Deskphone	N/A
Telenor Equipment	**Software**
Telenor SIP Trunk Service	Telenor IPT Version 11.0.138

5. Configure Avaya Communication Server 1000

This section describes the steps required to configure CS1000 for SIP trunking and also the basic configuration for telephones (analog, SIP and IP phones). SIP trunks are established between CS1000 and Session Manager. SIP trunks are also established between Session Manager and the Avaya SBCE private interface. The Avaya SBCE public interface connects to the Telenor's SIP trunks. Incoming PSTN calls from the Telenor SIP Trunk service traverse the Avaya SBCE and are directed to the Session Manager, which directs the calls to CS1000 (see **Figure 1**).

When a SIP message arrives at CS1000, 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 CS1000 and may be first subject to outbound features such as route selection, digit manipulation and class of service restrictions. When CS1000 selects a SIP trunk for outgoing PSTN calls, SIP signalling is directed to Session Manager. Session Manager directs the outbound SIP messages to the Avaya SBCE private interface. The Avaya SBCE public interface manages outgoing SIP sessions onwards to Telenor's SIP trunks.

Specific CS1000 configuration was performed using Element Manager and the system terminal interface. The general installation of the CS1000, System Manager, Session Manager and Avaya SBCE is presumed to have been previously completed and is not discussed here. Configuration details will be provided as required to draw attention to changes in default system configurations.

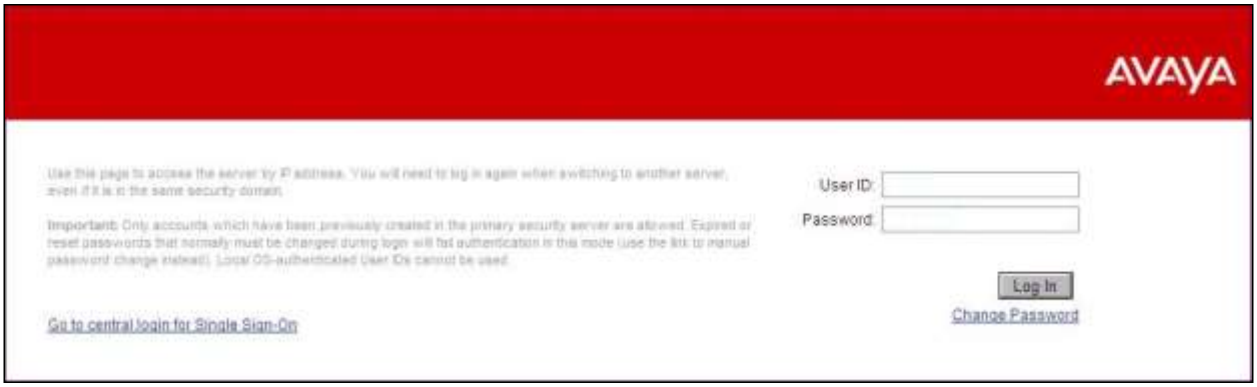
5.1. Logging into the Avaya Communication Server 1000

Configuration on the CS1000 will be performed by using both SSH Putty session and Avaya Unified Communications Management GUI.

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

Log in using the web based Avaya Unified Communications Management GUI. Avaya Unified Communications Management GUI may be launched directly via http://<ipaddress> where the relevant <ipaddress> is the TLAN IP address of the CS1000. Avaya Unified Communications Management can also be implemented on System Manager.

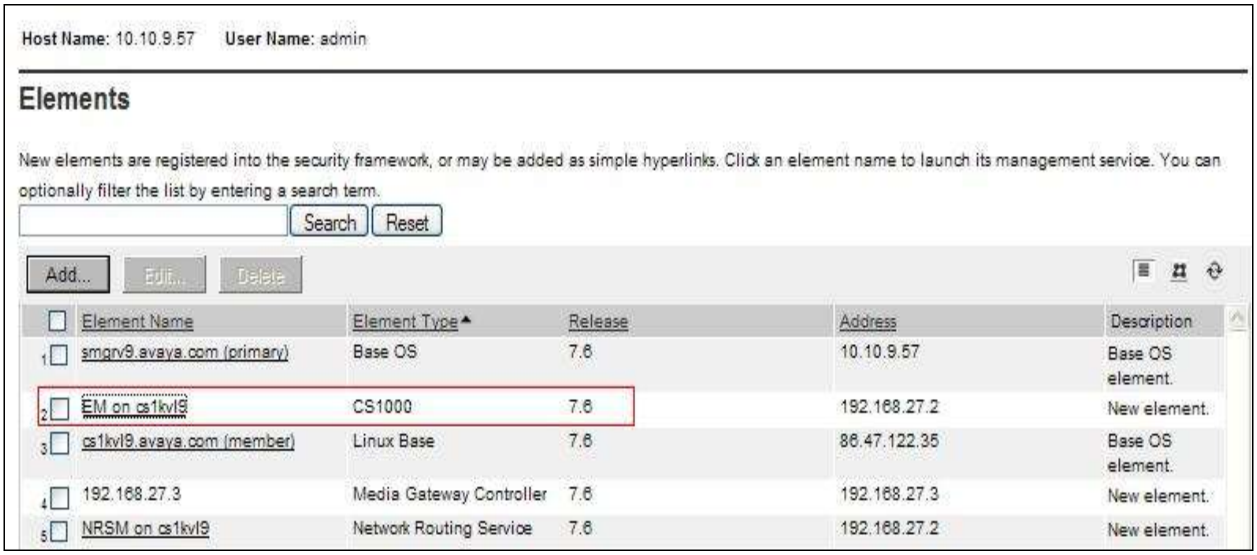
The following screen shows the login screen. Login with the appropriate credentials.



Use this page to access the server by IP address. You will need to log in again when switching to another server, even if it is in the same security domain.

Important: Only accounts which have been previously created in the primary security server are allowed. Expired or reset passwords that normally must be changed during login will fail authentication in this mode (use the link to manual password change instead). Local OS-authenticated User IDs cannot be used.

The Avaya Unified Communications Management **Elements** page will be used for configuration. Click on the element name corresponding to **CS1000** in the **Element Type** column. In the abridged screen below, the user would click on the element name **EM on cs1kvl9**.



Host Name: 10.10.9.57 **User Name:** admin

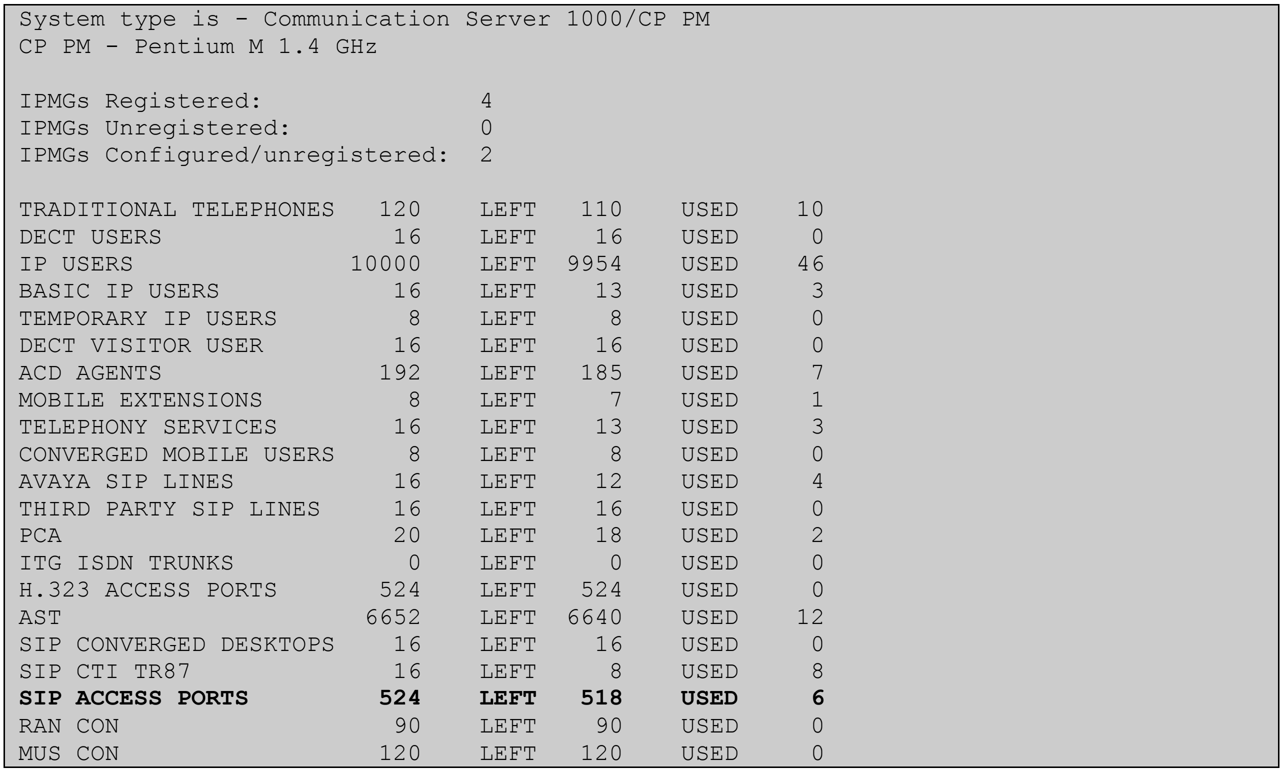
Elements

New elements are registered into the security framework, or may be added as simple hyperlinks. Click an element name to launch its management service. You can optionally filter the list by entering a search term.

	□	Element Name	Element Type ▲	Release	Address	Description
1	□	smgrv9.avaya.com (primary)	Base OS	7.6	10.10.9.57	Base OS element.
2	□	EM on cs1kvl9	CS1000	7.6	192.168.27.2	New element.
3	□	cs1kvl9.avaya.com (member)	Linux Base	7.6	86.47.122.35	Base OS element.
4	□	192.168.27.3	Media Gateway Controller	7.6	192.168.27.3	New element.
5	□	NRSM on cs1kvl9	Network Routing Service	7.6	192.168.27.2	New element.

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 CS1000 system terminal and manually load overlay 22 to print the System Limits (the required command is **slt**), and verify that the number of SIP access ports reported by the system is sufficient for the combination of trunks to the Telenor 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 CS1000.

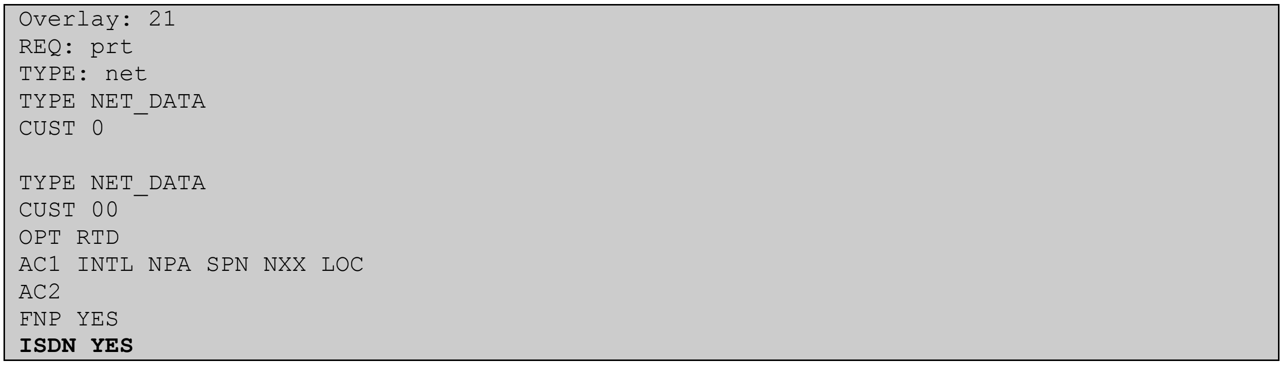


```
System type is - Communication Server 1000/CP PM
CP PM - Pentium M 1.4 GHz

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

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

Load Overlay 21 and confirm the customer is setup to use **ISDN** trunks by typing the **PRT** and **NET_DATA** commands as shown below.

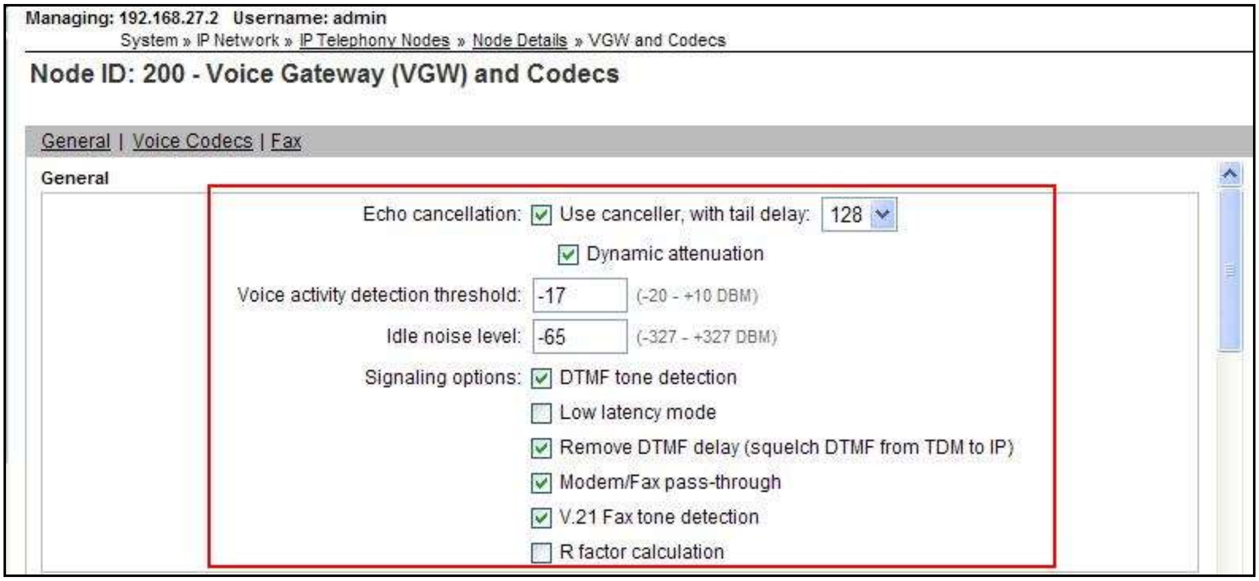


```
Overlay: 21
REQ: prt
TYPE: net
TYPE NET_DATA
CUST 0

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's SIP Trunk service supports G.711 voice codecs. Using the CS1000 Element Manager sidebar, select **Nodes, Servers, Media Cards** (not shown). Navigate to the **IP Network → IP Telephony Nodes → Node Details → VGW and Codecs** property page and configure the CS1000 **General** codec settings as in the following screenshots. The values highlighted are required for correct operation. The following screenshot shows the necessary **General** settings.



Managing: 192.168.27.2 Username: admin
System » IP Network » IP Telephony Nodes » Node Details » VGW and Codecs

Node ID: 200 - Voice Gateway (VGW) and Codecs

General | Voice Codecs | Fax

General

Echo cancellation: ☑ Use canceller, with tail delay: 128

☑ Dynamic attenuation

Voice activity detection threshold: -17 (-20 - +10 DBM)

Idle noise level: -65 (-327 - +327 DBM)

Signaling options: ☑ DTMF tone detection

□ Low latency mode

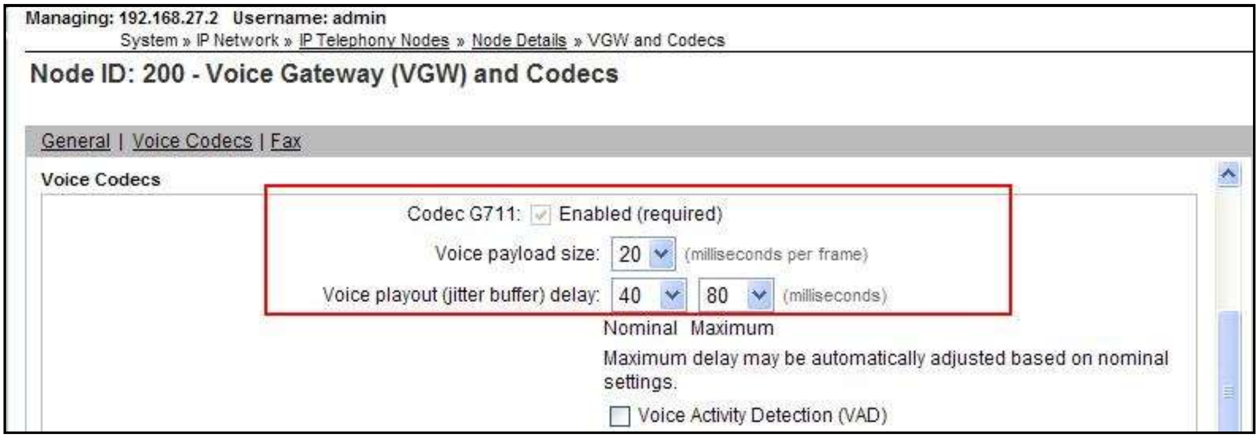
☑ Remove DTMF delay (squelch DTMF from TDM to IP)

☑ Modem/Fax pass-through

☑ V.21 Fax tone detection

□ R factor calculation

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



Managing: 192.168.27.2 Username: admin
System » IP Network » IP Telephony Nodes » Node Details » VGW and Codecs

Node ID: 200 - Voice Gateway (VGW) and Codecs

General | Voice Codecs | Fax

Voice Codecs

Codec G711: ☑ Enabled (required)

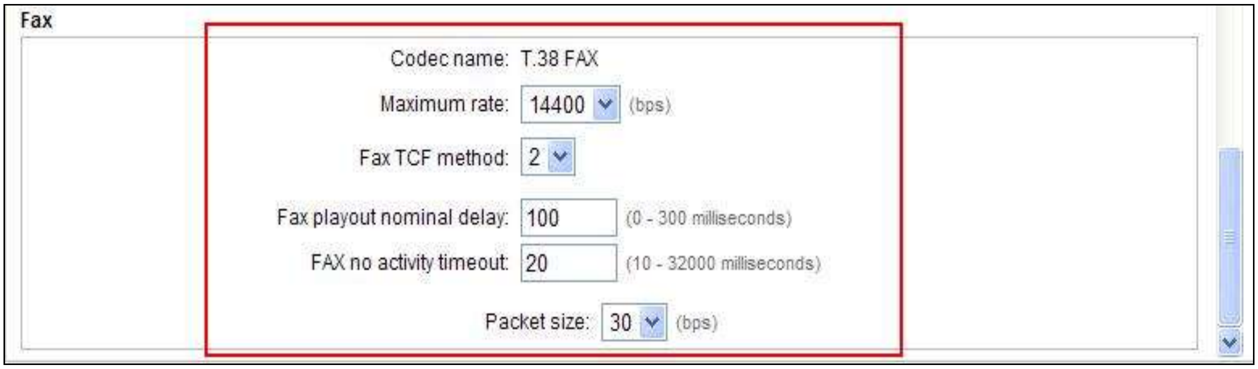
Voice payload size: 20 (milliseconds per frame)

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

Maximum delay may be automatically adjusted based on nominal settings.

□ Voice Activity Detection (VAD)

Finally, configure the **Fax** settings as in the highlighted section of the next screenshot. Click on the **Save** button when finished (not shown).



Fax

Codec name: T.38 FAX

Maximum rate: 14400 (bps)

Fax TCF method: 2

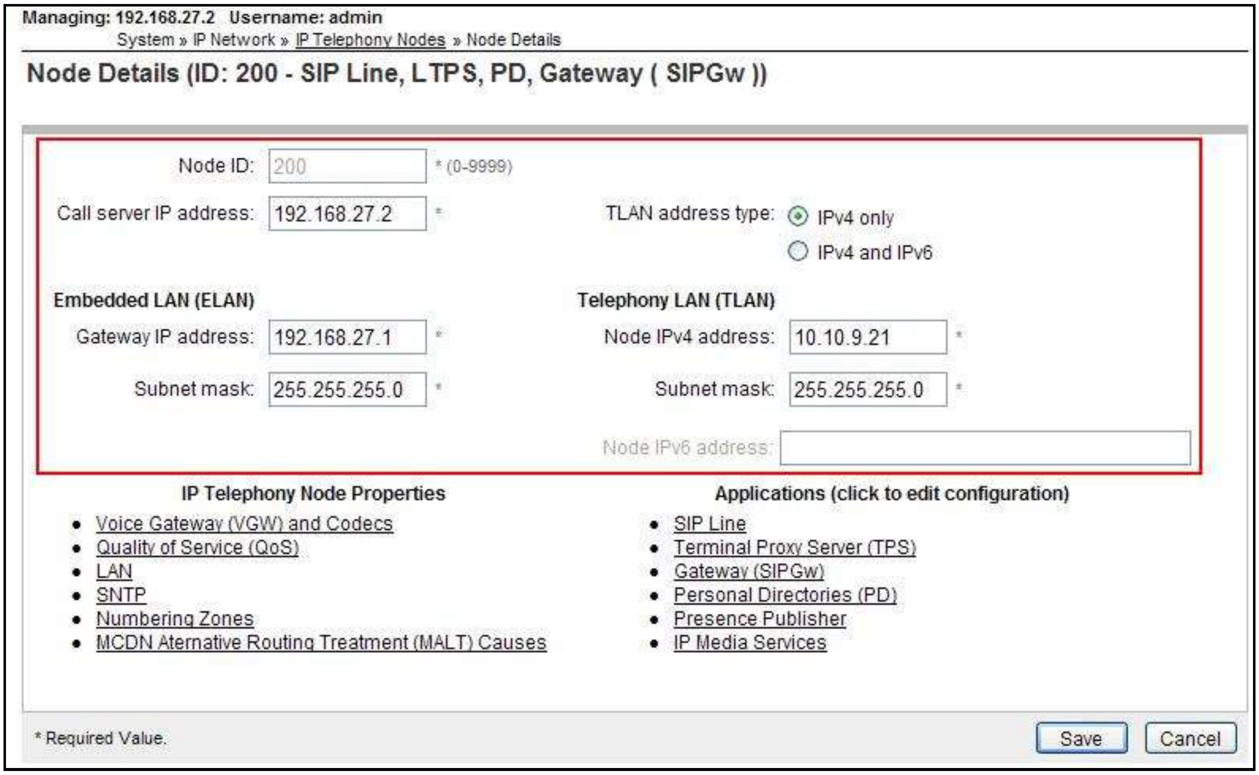
Fax playout nominal delay: 100 (0 - 300 milliseconds)

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

Packet size: 30 (bps)

5.4. Virtual Trunk Gateway Configuration

Use CS1000 Element Manager to configure the system node properties. Navigate to the **System → IP Network → IP Telephony Nodes → Node Details** and verify the highlighted section is completed with the correct IP addresses and subnet masks of the Node. The CS1000 call server and signaling server have previously been configured with IP addresses. The **Node IPv4 address** is the IP address that the IP phones use to register. This is also where the SIP trunk connection is made to Session Manager. When an entity link is added in Session Manager for the CS1000, it is the **Node IPv4 address** that is used (see **Section 6.5** – Administer SIP Entities for more details).



Managing: 192.168.27.2 Username: admin

System » IP Network » IP Telephony Nodes » Node Details

Node Details (ID: 200 - SIP Line, LTPS, PD, Gateway (SIPGw))

Node ID: 200 * (0-9999)

Call server IP address: 192.168.27.2 *

TLAN address type: ● IPv4 only ○ IPv4 and IPv6

Embedded LAN (ELAN)

Gateway IP address: 192.168.27.1 *

Subnet mask: 255.255.255.0 *

Telephony LAN (TLAN)

Node IPv4 address: 10.10.9.21 *

Subnet mask: 255.255.255.0 *

Node IPv6 address:

IP Telephony Node Properties

- Voice Gateway (VGW) and Codecs
- Quality of Service (QoS)
- LAN
- SNTP
- Numbering Zones
- MCDN Aternative Routing Treatment (MALT) Causes

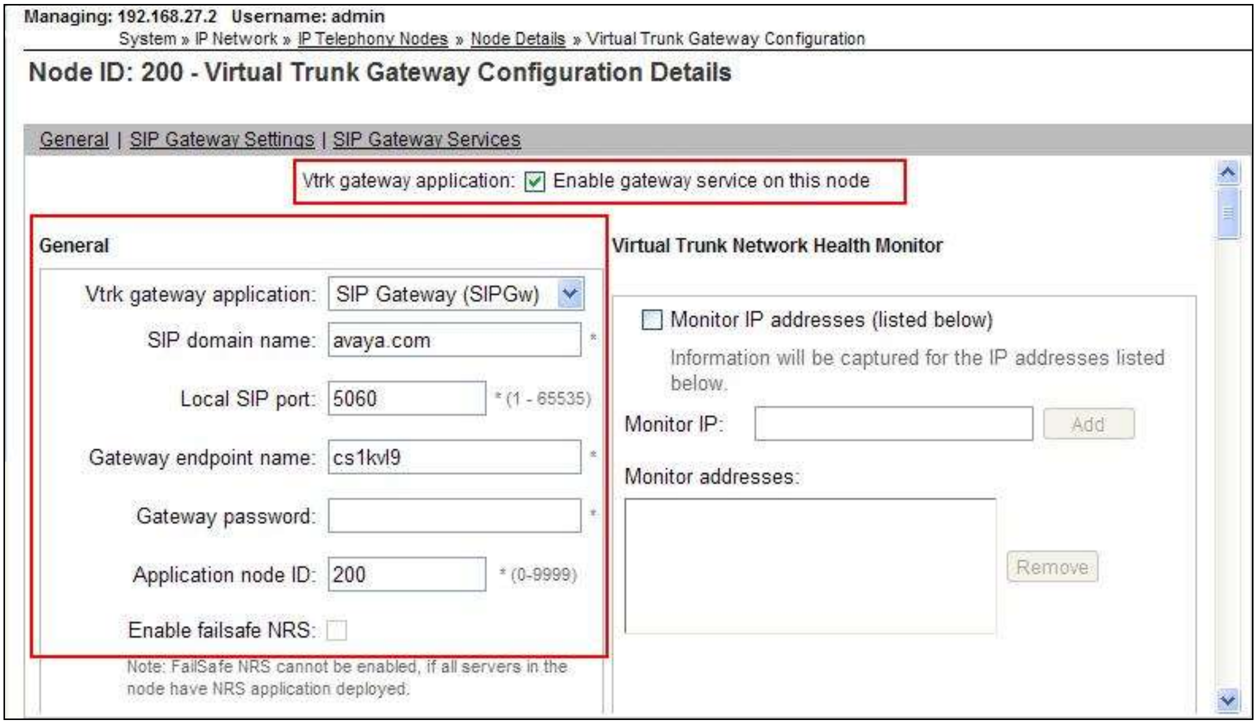
Applications (click to edit configuration)

- SIP Line
- Terminal Proxy Server (TPS)
- Gateway (SIPGw)
- Personal Directories (PD)
- Presence Publisher
- IP Media Services

* Required Value.

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

- **Vtrk gateway application:** Provides option to select Gateway applications. The three supported modes are **SIP Gateway (SIPGw)**, **H.323Gw**, and **SIPGw and H.323Gw**. **SIP Gateway (SIPGw)** was used in the test configuration.
- **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 Session Manager; in this case **avaya.com**.
- **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 **200**.
- **Proxy Or Redirect Server:** Primary TLAN IP address is the Security Module IP address of Session Manager. The **Transport protocol** used for SIP, in this case is **TCP**.
- **SIP URI Map: Public E.164 - National** and **Private - Unknown** are left blank. All other fields in the SIP URI Map are left with default values.



Managing: 192.168.27.2 Username: admin

System » IP Network » IP Telephony Nodes » Node Details » Virtual Trunk Gateway Configuration

Node ID: 200 - 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: cs1kvl9 *

Gateway password: *

Application node ID: 200 * (0-9999)

Enable failsafe NRS: □

Note: FailSafe NRS cannot be enabled, if all servers in the node have NRS application deployed.

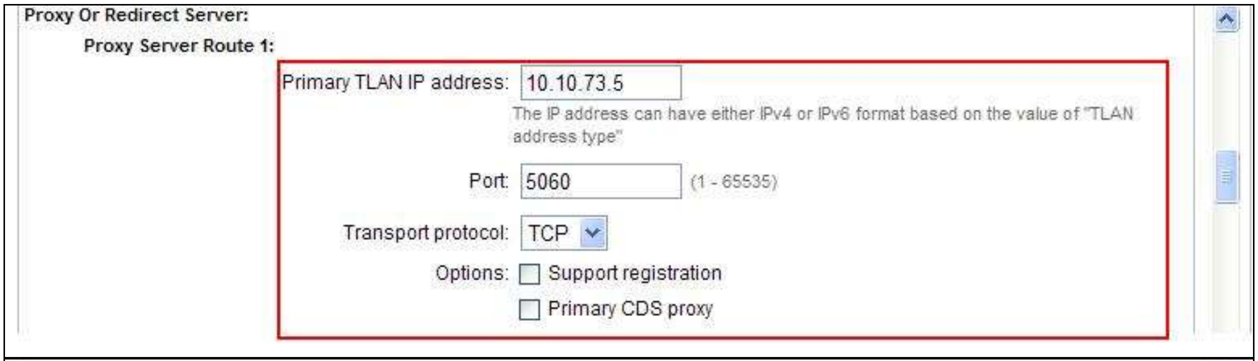
Virtual Trunk Network Health Monitor

□ 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: 10.10.73.5

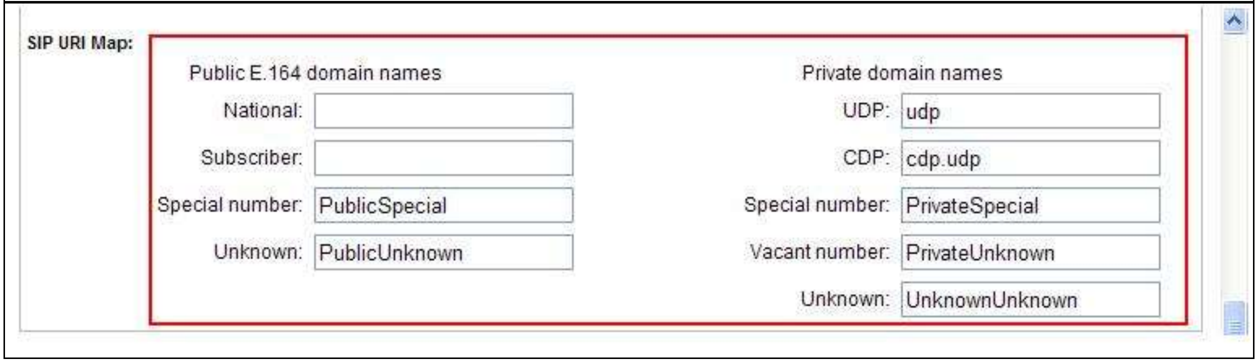
The IP address can have either IPv4 or IPv6 format based on the value of "TLAN address type"

Port: 5060 (1 - 65535)

Transport protocol: TCP

Options: □ Support registration

□ Primary CDS proxy



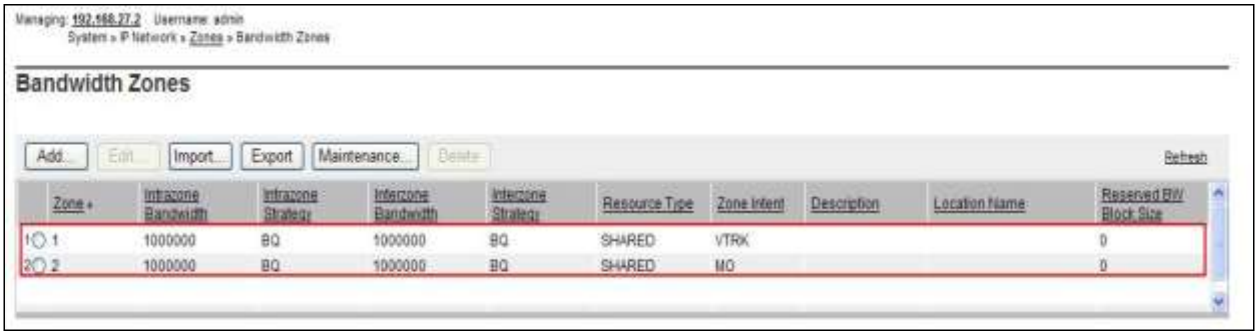
SIP URI Map:

Public E.164 domain names		Private domain names	
National:		UDP:	udp
Subscriber:		CDP:	cdp.udp
Special number:	PublicSpecial	Special number:	PrivateSpecial
Unknown:	PublicUnknown	Vacant number:	PrivateUnknown
		Unknown:	UnknownUnknown

5.5. Configure Bandwidth Zones

Bandwidth Zones are used for alternate call routing between IP telephones 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. In the sample configuration SIP trunks use zone 1 and IP and SIP telephones use zone 2; system defaults were used for each zone other than the parameter configured for **Zone Intent**. For SIP trunks (zone 1), **VTRK** is configured for **Zone Intent**. For IP and SIP telephones (zone 2), **MO** (Main Office) is configured for **Zone Intent**.

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.



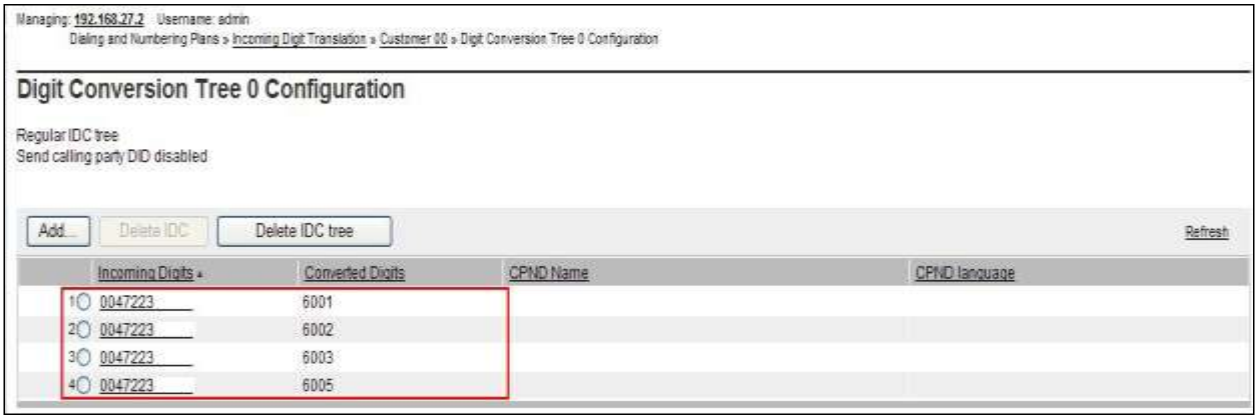
Managing: 192.168.27.2 Username: admin
System » IP Network » Zones » Bandwidth Zones

Bandwidth Zones

	Zone	Intrazone Bandwidth	Intrazone Strategy	Interzone Bandwidth	Interzone Strategy	Resource Type	Zone Intent	Description	Location Name	Reserved BW Block Size
1○	1	1000000	BQ	1000000	BQ	SHARED	VTRK			0
2○	2	1000000	BQ	1000000	BQ	SHARED	MO			0

5.6. Configure Incoming Digit Conversion Table

A limited number of Direct Dial Inwards (DDI) numbers were available. The Incoming Digit Conversion (IDC) table was configured to translate incoming PSTN numbers to four digit local telephone extension numbers. The 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: 192.168.27.2 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

	Incoming Digits	Converted Digits	CPND Name	CPND language
1○	0047223[redacted]	6001		
2○	0047223[redacted]	6002		
3○	0047223[redacted]	6003		
4○	0047223[redacted]	6005		

5.7. Configure SIP Trunks

Communication Server 1000 virtual trunks will be used for all inbound and outbound PSTN calls to the Telenor SIP Trunk service. Six separate steps are required to configure Communication Server 1000 virtual trunks:

- Configure a D-Channel Handler (**DCH**); configure using the CS1000 system terminal and overlay 17.
- Configure a SIP trunk Route Data Block (**RDB**); configure using the CS1000 system terminal and overlay 16.
- Configure SIP trunk members; configure using the CS1000 system terminal and overlay 14.
- Configure a Digit Manipulation Data Block (**DGT**), configure using the CS1000 system terminal and overlay 86.
- Configure a Route List Block (**RLB**); configure using the CS1000 system terminal and overlay 86.
- Configure Co-ordinated Dialling Plan(s) (**CDP**); configure using the CS1000 system terminal and overlay 87.

The following is an example DCH configuration for SIP trunks. Load **Overlay 17** at the CS1000 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 CS1000 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 **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 200
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 CS1000 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 Digit Manipulation Index (**DMI)** is the same as 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

ISET 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 CS1000 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        TSC  18           TSC  800          TSC  08
FLEN 0            FLEN 0            FLEN 0            FLEN 0
RRPA NO           RRPA NO           RRPA NO           RRPA NO
RLI  10           RLI  10           RLI  10           RLI  10
CCBA NO           CCBA NO           CCBA NO           CCBA NO
```

5.8. Calling Line Identification

This section documents basic configuration relevant to the Telenor configuration. Load **Overlay 15** at system terminal and enter the required values in bold. As shown below, **CLID** is set to **YES** and **ENTRY** is set to **0**. **HNTN** and **HLCL** match the required digits assigned by Telenor and **DIDN** is set to **NO**.

```
Load Overlay 15
TYPE NET_DATA
CUST 0
OPT
AC2
FNP
CLID YES
  SIZE
  INTL
  ENTRY 0
HNTN 004722
  ESA_HLCL
  ESA_INHN NO
  ESA_APDN NO
  HLCL 391531
  DIDN NO
  DIDN_LEN 0
  HLOC
  LSC
  CLASS_FMT DN
```

5.9. 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 Deskphone. Load **Overlay 20** at the system terminal and enter the following values. A unique four digit number is entered for the **KEY 00**. The value for **CFG_ZONE** is the value used in **Section 5.5** for IP and SIP telephones.

```
Load Overlay 20 IP Telephone configuration
DES  1140
TN   100 0 03 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 RCBD
     ICDA CDMD LLCN MCTD CLBD AUTR
     GPUD DPUD DNDA CFXA ARHD FITD CLTD ASCD
     CPFA CPTA ABDD CFHD FICD NAID BUZZ AGRD MOAD
     UDI RCC HBTA AHD IPND DDGA NAMA MIND PRSD NRWD NRCD NROD
     DRDD EXR0
     USMD USRD ULAD CCBD RTDD RBDD RBHD PGND OCBD FLXD FTTC DNDY DNO3 MCBN
     FDSD NOVD VOLA VOUD CDMR PRED RECA MCDD T87D SBMD KEM3 MSNV FRA  PKCH MUTA MWTD
---continued on next page----
```

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

DVLD CROD CROD
CPND_LANG ENG
RCO  0
HUNT 0
LHK  0
PLEV 02
PUID
DANI NO
AST  00
IAPG 1
AACS NO
ITNA NO
DGRP
MLWU_LANG 0
MLNG ENG
DNDR 0
KEY  00 MCR 6000 0     MARP
        CPND
          CPND_LANG ROMAN
            NAME IP1140
            XPLN 10
            DISPLAY_FMT FIRST,LAST
     01 MCR 6000 0
        CPND
          CPND_LANG ROMAN
            NAME IP1140
            XPLN 10
            DISPLAY_FMT FIRST,LAST
     02
     03 BSY
     04 DSP
     05
     06
     07
     08
     09
     10
     11
     12
     13
     14
     15
     16
     17 TRN
     18 AO6
     19 CFW 16
     20 RGA
     21 PRK
     22 RNP
     23
     24 PRS
     25 CHG
     26 CPN
```

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

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

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

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

MLNG ENG
DNDR 0
KEY  00 MCR 6066 0     MARP
        CPND
          CPND_LANG ROMAN
            NAME Digital Set
            XPLN 10
            DISPLAY_FMT FIRST,LAST
     01 MCR 6066 0
        CPND
          CPND_LANG ROMAN
            NAME Digital Set
            XPLN 10
            DISPLAY_FMT FIRST,LAST
     02 DSP
     03 MSB
     04
     05
     06
     07
     08
     09
     10
     11
     12
     13
     14
     15
     16
     17 TRN
     18 AO6
     19 CFW 16
     20 RGA
     21 PRK
     22 RNP
     23
     24 PRS
     25 CHG
     26 CPN
     27 CLT
     28 RLT
     29
     30
     31
```

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

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

ERL 00000
WRLS NO
DN   52002
AST  NO
IAPG 0
HUNT
TGAR 0
LDN  NO
NCOS 0
SGRP 0
RNPG 0
XLST
SCI  0
SCPW
SFLT NO
CAC_MFC 0
CLS  UNR DTN FBD XFD WTA THFD FND HTD ONS
     LPR XRD AGRD CWD SWD MWD RMMD SMWD LPD XHD SLKD CCSD LND TVD
     CFTD SFD MRD C6D CNID CLBD AUTU
     ICDD CDMD LLCN EHTD MCTD
     GPUD DPUD CFXD ARHD OVDD AGTD CLTD LDTD ASCD SDND
     MBXD CPFA CPTA UDI RCC HBTD IRGD  DDGA NAMA MIND
     NRWD NRCD NROD SPKD CRD PRSD MCRD
     EXR0 SHL SMSD ABDD CFHD DNDY DNO3
     CWND USMD USRD CCBD BNRD OCBD RTDD RBDD RBHD FAXA CNUD CNAD PGND FTTC
     FDSD NOVD CDMR PRED MCDD T87D SBMD PKCH MPTD
PLEV 02
PUID
AACS NO
MLWU_LANG 0
FTR  DCFW 4
```

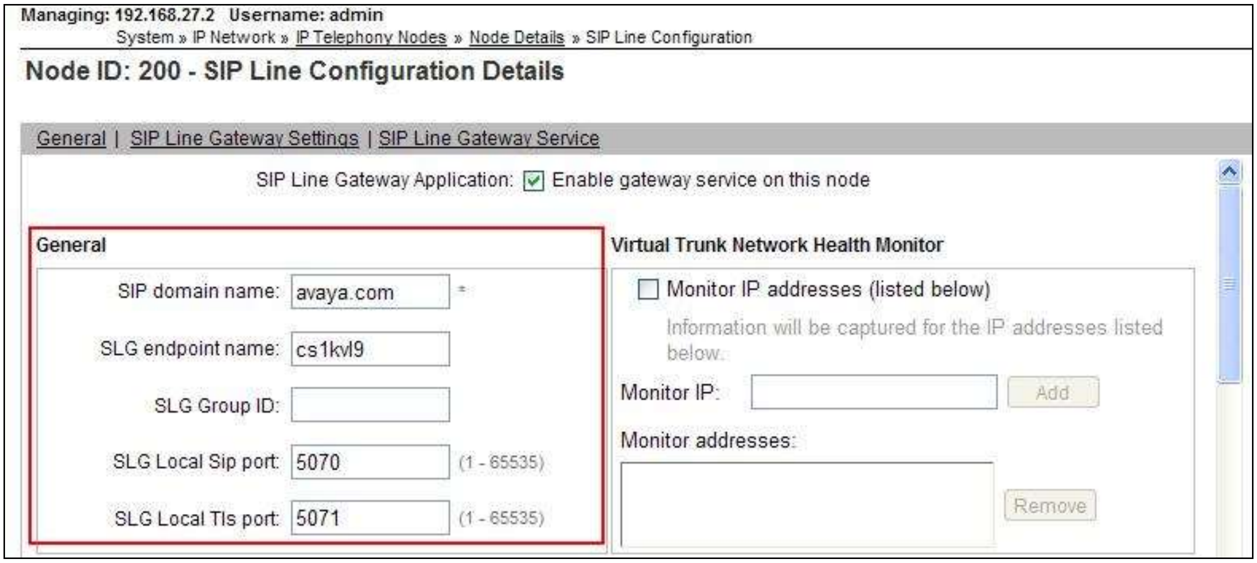
5.10.Configure the SIP Line Gateway Service

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 CS1000 system terminal and overlay 15 to activate SIP Line services (SLS_DATA), as in the following example where **SIPL_ON** is set to **YES**.

```
SLS_DATA
  SIPL_ON YES
  UAPR 11
  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 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 6.2**.
- **SLG endpoint name:** Enter the same endpoint name as the SIP Line Gateway in **Section 5.4** and this will be used for SIP gateway registration.
- **SLG Local Sip port:** Default value is **5070**.
- **SLG Local Tls port:** Default value is **5071**.



Managing: 192.168.27.2 Username: admin
System » IP Network » IP Telephony Nodes » Node Details » SIP Line Configuration

Node ID: 200 - 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: avaya.com *

SLG endpoint name: cs1kvl9

SLG Group ID:

SLG Local Sip port: 5070 (1 - 65535)

SLG Local Tls port: 5071 (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:

5.11.Configure SIP Line Telephones

When SIP Line service configuration is completed, use the CS1000 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 used in **Section 5.5** for IP and SIP telephones. A unique telephone number is entered for value **KEY 00**. The value for **KEY 01** is comprised of the **UAPR** (set in **Section 5.10**) value and the telephone number used in **KEY 00**.

```
Load Overlay 20 – SIP Telephone Configuration
DES  SIPD
TN   100 0 03 3  VIRTUAL
TYPE UEXT
CDEN 8D
CTYP XDLC
CUST 0
UXTY SIPL
MCCL YES
SIPN 1
SIP3 0
FMCL 0
TLSV 0
SIPU 8889
NDID 200
SUPR NO
SUBR DFLT MWI RGA CWI MSB
UXID
NUID
NHTN
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 RCBD
     ICDD CDMD LLCN MCTD CLBD AUTU
     GPUD DPUD DNDA CFXA ARHD FITD CLTD ASCD
     CPFA CPTA ABDD CFHD FICD NAID BUZZ AGRD MOAD

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

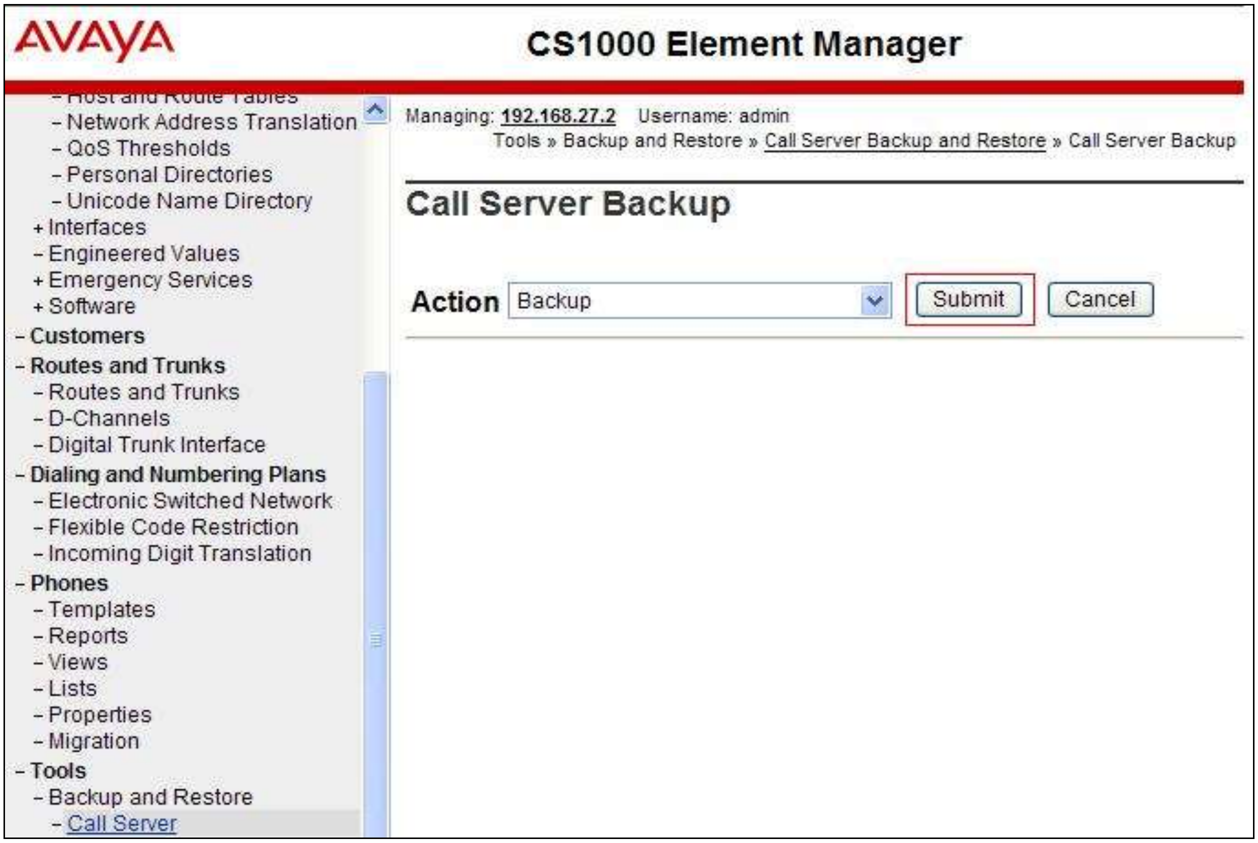
```
---continued from previous page---

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

AACS NO
ITNA NO
DGRP
MLWU_LANG 0
MLNG ENG
DNDR 0
KEY  00 MCR 6002 0     MARP
        CPND
          CPND_LANG ROMAN
            NAME Sigma 1140
            XPLN 11
            DISPLAY_FMT FIRST,LAST*
     01 HOT U 116002 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
```

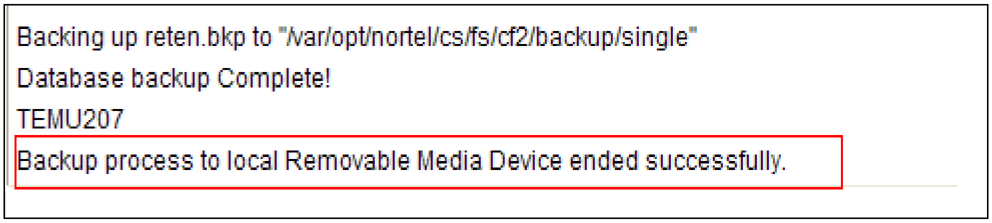
5.12. Save Configuration

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.



Action: Backup

The 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 1000 is complete.

6. Configuring Avaya Aura® Session Manager

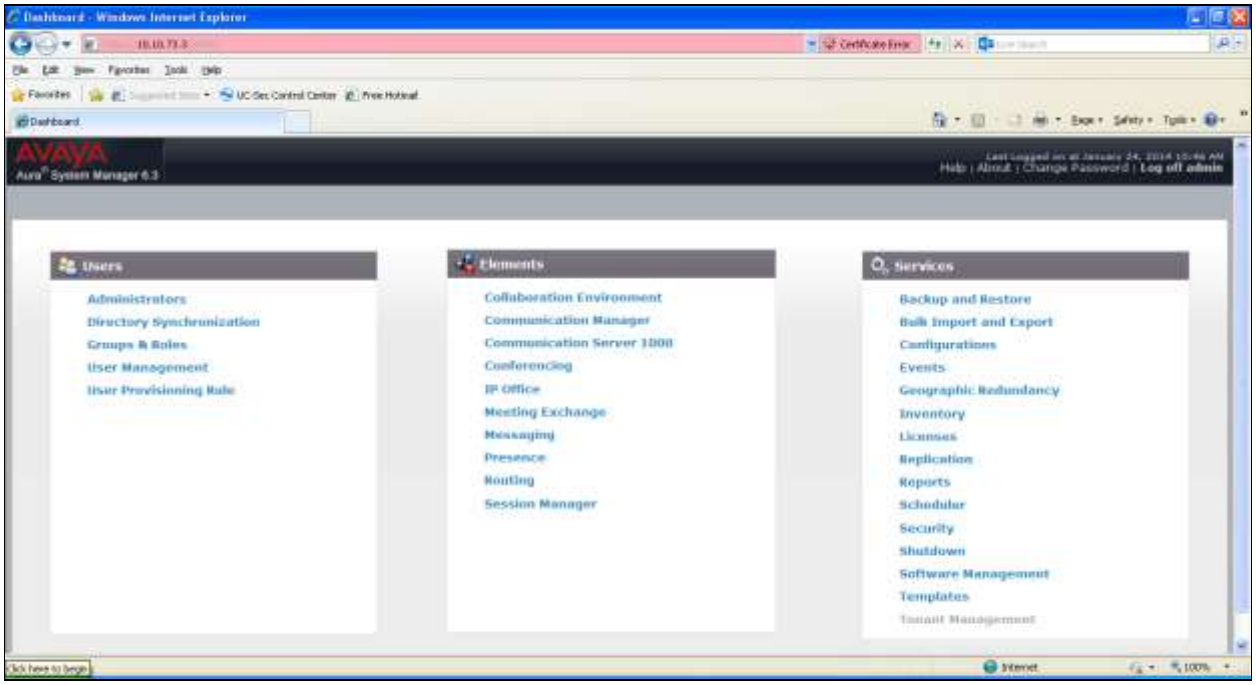
This section provides the procedures for configuring Session Manager. Session Manager is configured via System Manager. The procedures include the following areas:

- Log in to Avaya Aura® System Manager
- Administer SIP Domain
- Administer SIP Location
- Administer Adaptations
- Administer SIP Entities
- Administer Entity Links
- Administer Routing Policies
- Administer Dial Patterns

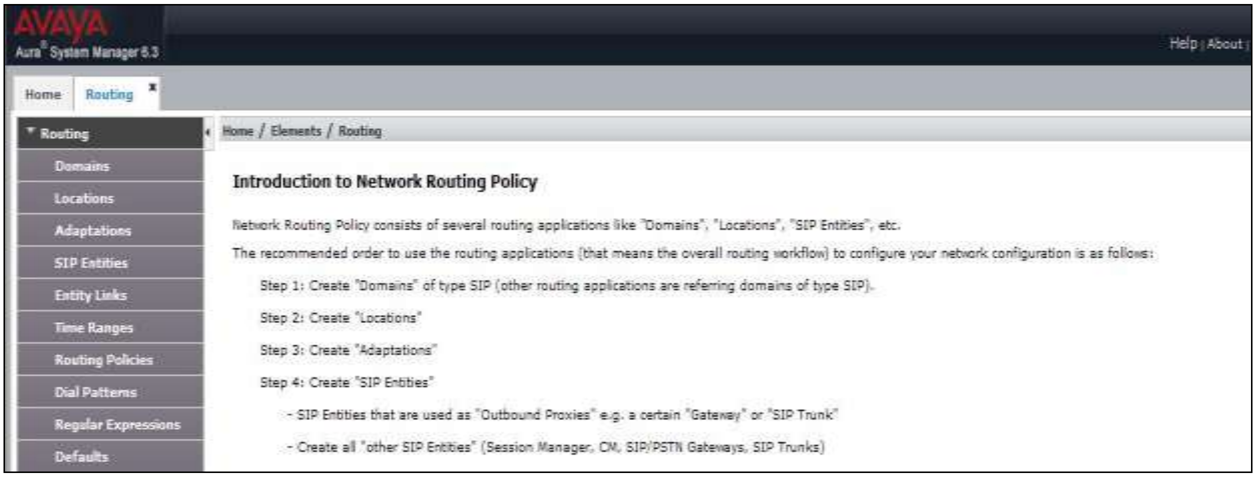
It may not be necessary to create all the items above when creating a connection to the service provider since some of these items would have already been defined as part of the initial Session Manager installation. This includes items such as certain SIP domains, locations, SIP entities, and Session Manager itself. However, each item should be reviewed to verify the configuration.

6.1. Log in to Avaya Aura® System Manager

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



Most of the configuration items are performed in the Routing Element. Click on **Routing** in the Elements column shown above to bring up the **Introduction to Network Routing Policy** screen.



Introduction to Network Routing Policy

Network Routing Policy consists of several routing applications like "Domains", "Locations", "SIP Entities", etc.

The recommended order to use the routing applications (that means the overall routing workflow) to configure your network configuration is as follows:

Step 1: Create "Domains" of type SIP (other routing applications are referring domains of type SIP).

Step 2: Create "Locations"

Step 3: Create "Adaptations"

Step 4: Create "SIP Entities"

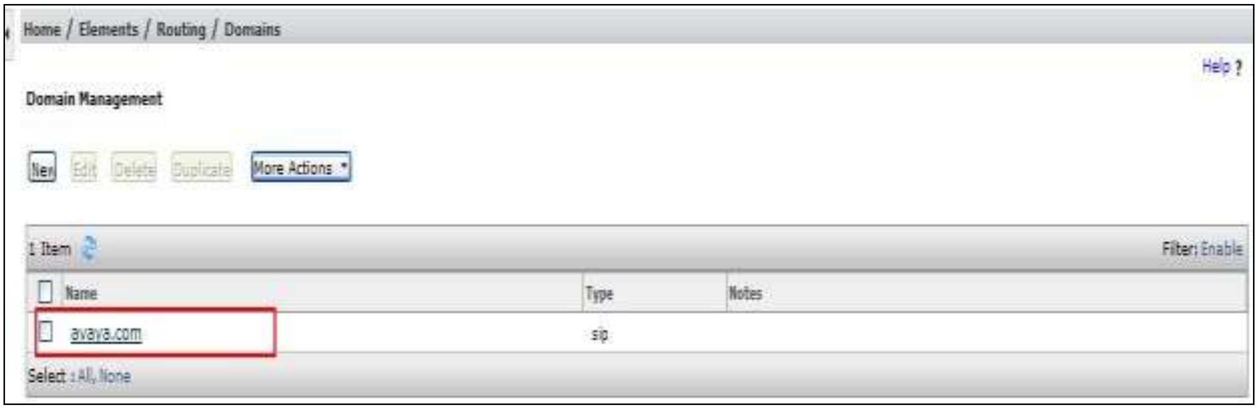
- SIP Entities that are used as "Outbound Proxies" e.g. a certain "Gateway" or "SIP Trunk"
- Create all "other SIP Entities" (Session Manager, CM, SIP/PSTN Gateways, SIP Trunks)

6.2. Administer SIP Domain

Create a SIP domain for each domain for which Session Manager will need to be aware in order to route calls. 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 a domain name. 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.



	Name	Type	Notes
□	avaya.com	sip	

6.3. Administer Locations

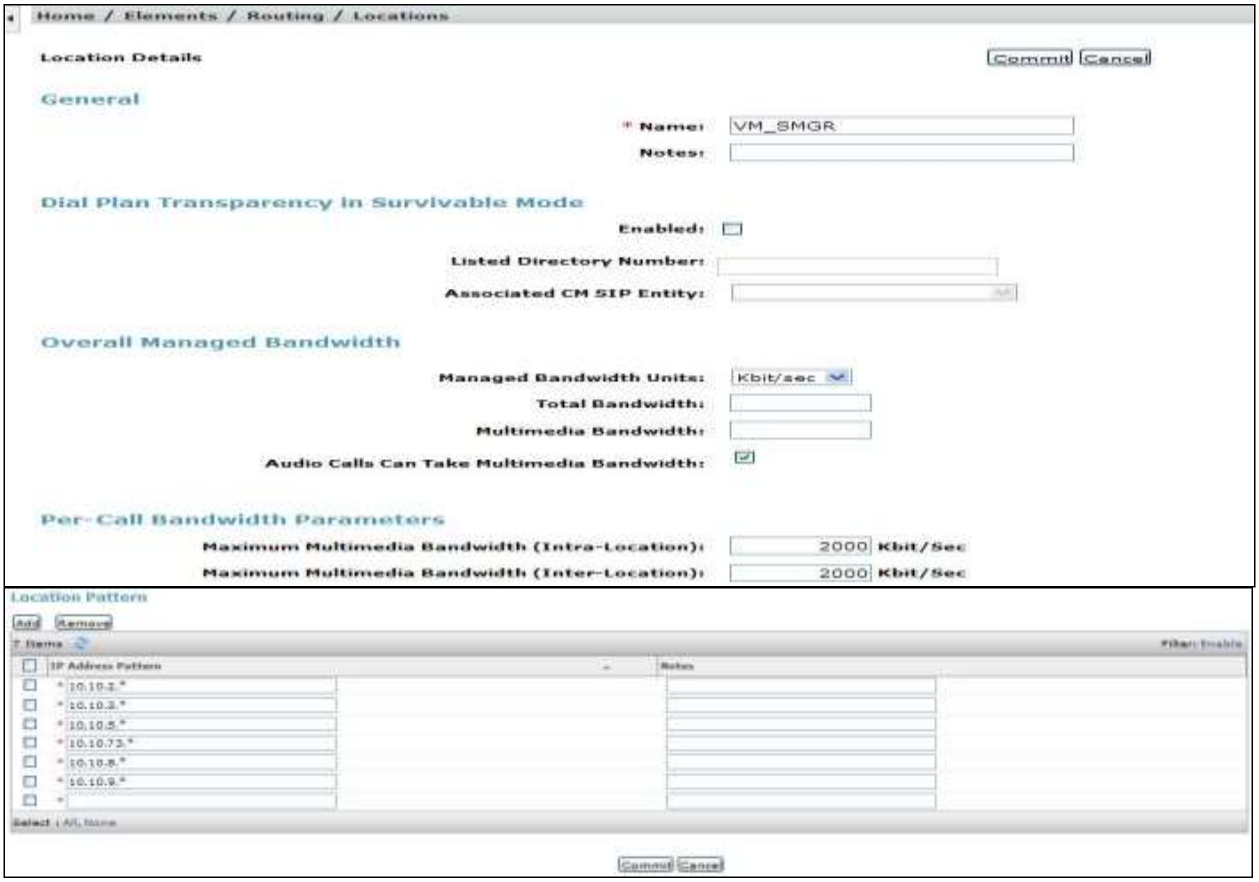
Locations can be used to identify logical and/or physical locations where SIP Entities reside for purposes of bandwidth management and call admission control. To add a location, navigate to **Routing →Locations** in the left-hand navigation pane and click the **New** button in the right pane (not shown). In the **General** section, enter the following values. Use default values for all remaining fields:

- **Name:** Enter a descriptive name for the location.
- **Notes:** Add a brief description (optional).

The Location Pattern is used to identify call routing based on IP address. Session Manager matches the IP address against the patterns defined in this section. If a call is from a SIP entity that does not match the IP address pattern then Session Manager uses the location administered for the SIP Entity. In the **Location Pattern** section, click **Add** and enter the following values.

- **IP Address Pattern** Enter the logical pattern used to identify the location.
- **Notes** Add a brief description [Optional].

Click **Commit** to save. The screenshot below shows the Location **VM_SMGR** defined for the compliance testing.



Location Details

General

* Name:	VM_SMGR
Notes:	

Dial Plan Transparency in Survivable Mode

Enabled:	□
Listed Directory Number:	
Associated CM SIP Entity:	

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):	2000 Kbit/Sec
Maximum Multimedia Bandwidth (Inter-Location):	2000 Kbit/Sec

Location Pattern

7 Items

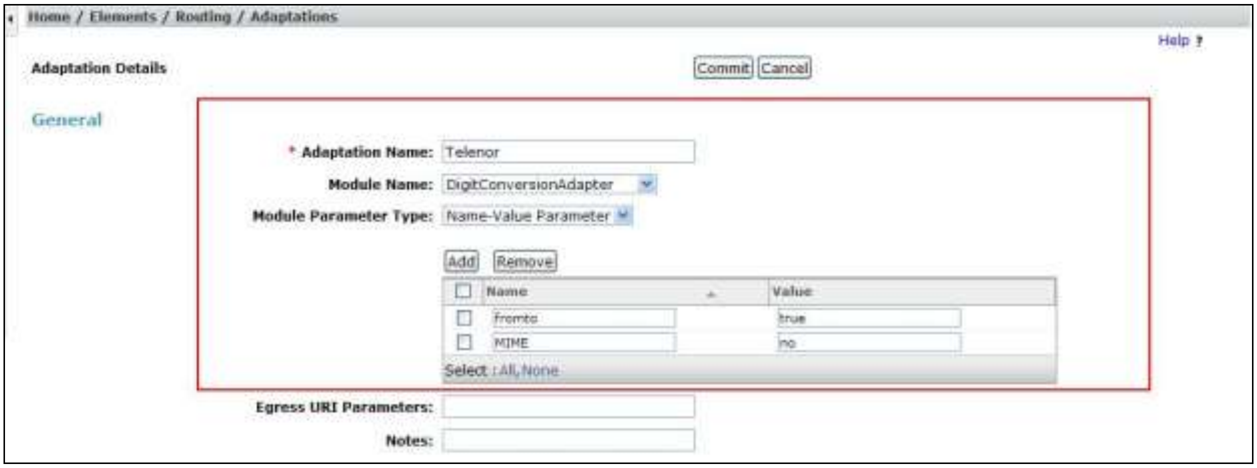
□	IP Address Pattern	Notes
□	* 10.10.1.*	
□	* 10.10.2.*	
□	* 10.10.5.*	
□	* 10.10.73.*	
□	* 10.10.8.*	
□	* 10.10.9.*	
□	*	

6.4. Administer Adaptations

Adaptations can be used to modify the called and calling party numbers to meet the requirements of the service. The called party number present in the SIP INVITE Request URI is modified by the Digit Conversion in the Adaptation. The example below was applied to the Avaya SBCE SIP entity and was used in test to convert numbers being passed between the Avaya SBCE and Session Manager.

To add an adaptation, under the **Routing** tab select **Adaptations** on the left hand menu and then click on the **New** button (not shown). Under **Adaption Details →General**:

- In the **Adaptation name** field enter an informative name.
- In the **Module name** field click on the down arrow and then select the <**click to add module**> entry from the drop down list and type **DigitConversionAdapter** in the resulting New Module Name field.
- **Module parameter** **MIME =no** strips MIME message bodies on egress from Session Manager.
  fromto=true modifies from and to headers of a message.



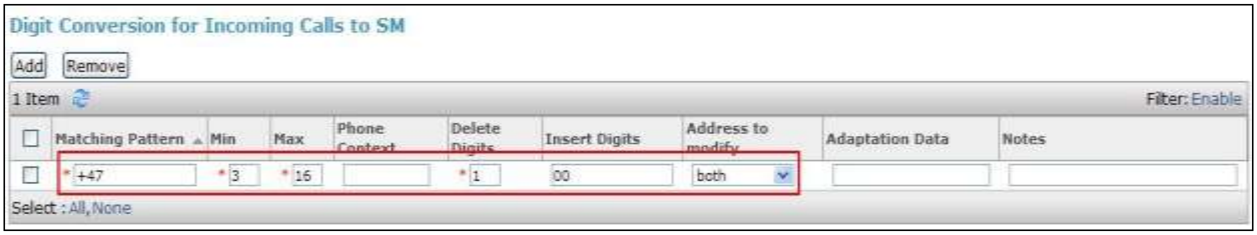
Adaptation Name: Telenor
Module Name: DigitConversionAdapter
Module Parameter Type: Name-Value Parameter

Name	Value
fromto	true
MIME	no

Egress URI Parameters:
Notes:

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

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

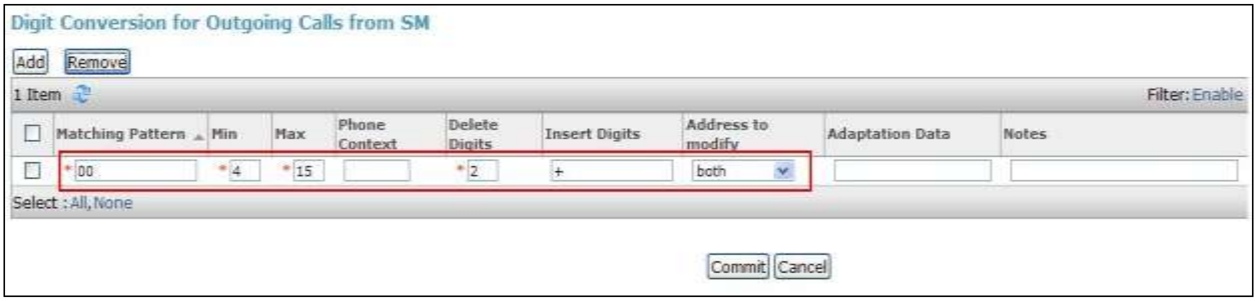

Digit Conversion for Incoming Calls to SM

□	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
□	* +47	* 3	* 16		* 1	00	both		

This will ensure any incoming numbers will have the + symbol removed and international dialing code 00 inserted before being presented to the CS1000.

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

- **Matching Pattern** Enter dialed prefix for calls to SIP endpoints registered to Session Manager.
- **Min** Enter minimum number of digits that must be dialed.
- **Max** Enter maximum number of digits that may be dialed.
- **Delete Digits** Enter number of digits that may be deleted.
- **Insert Digits** Enter digits to be added before the dialed number.
- **Address to modify** Select **both**.


Digit Conversion for Outgoing Calls from SM

□	Matching Pattern	Min	Max	Phone Context	Delete Digits	Insert Digits	Address to modify	Adaptation Data	Notes
□	* 00	* 4	* 15		* 2	+	both		

This will ensure any outbound numbers will have the dialing code 00 removed and international dialing symbol + inserted before being presented to the Avaya SBCE.

6.5. Administer SIP Entities

A SIP entity must be added for each SIP-based telephony system, supported by a SIP connection to Session Manager. To add a SIP entity, select **SIP Entities** on the left panel menu and then click on the **New** button (not shown). The following will need to be entered for each SIP entity. Under **General:**

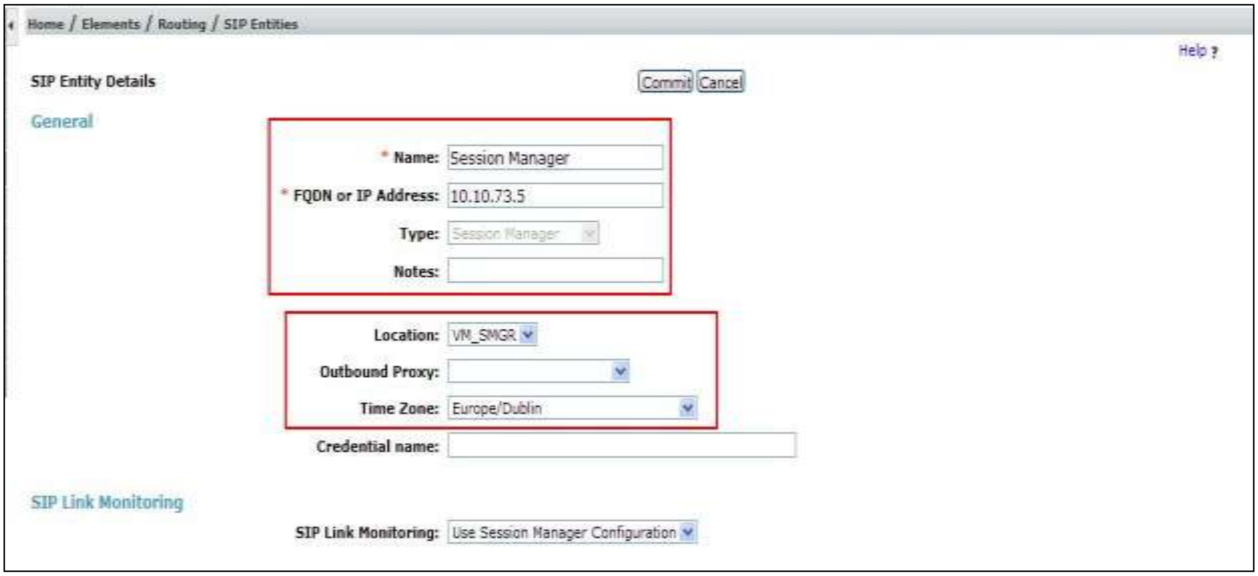
- In the **Name** field enter an informative name.
- In the **FQDN or IP Address** field enter the IP address of Session Manager or the signalling interface on the connecting system.
- In the **Type** field use **Session Manager** for a Session Manager SIP entity, **Other** for a CS1000 SIP entity and **SIP Trunk** for the Avaya SBCE SIP entity.
- In the **Adaptation** field (not available for the Session Manager SIP entity), select the appropriate Adaptation from the drop down menu.
- In the **Location** field select the appropriate location from the drop down menu.
- In the **Time Zone** field select the time zone for the SIP entity.

In this configuration there are three SIP entities:

- Session Manager SIP entity
- CS1000 SIP entity
- Avaya SBCE SIP entity

6.5.1. Avaya Aura® Session Manager SIP Entity

The following screens show the SIP entity for Session Manager. The **FQDN or IP Address** field is set to the IP address of the Session Manager SIP signaling interface. Set the location to that defined in **Section 6.3** and the **Time Zone** to the appropriate time zone.



SIP Entity Details

General

* Name: Session Manager

* FQDN or IP Address: 10.10.73.5

Type: Session Manager

Notes:

Location: VM_SMGR

Outbound Proxy:

Time Zone: Europe/Dublin

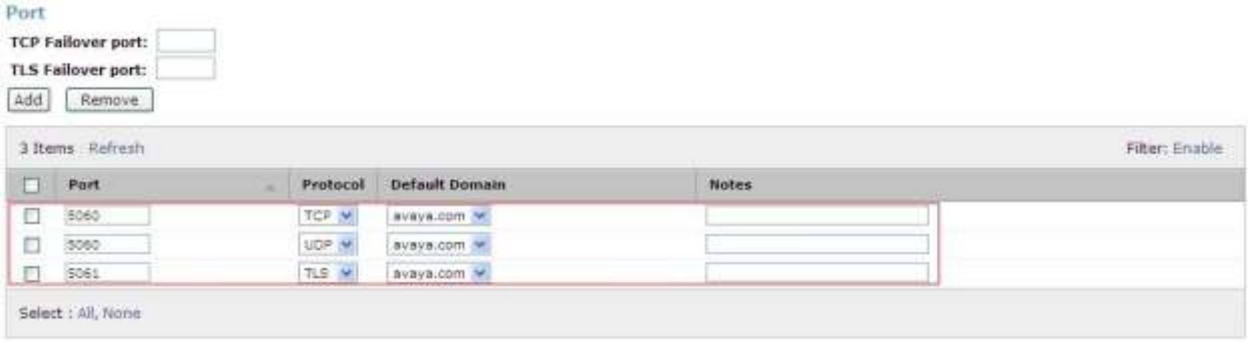
Credential name:

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

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

- In the **Port** field enter the port number on which the system listens for SIP requests.
- In the **Protocol** field select the transport protocol to be used for SIP requests.
- In the **Default Domain** field, from the drop down menu select **avaya.com** as the default domain.



Port

TCP Failover port:

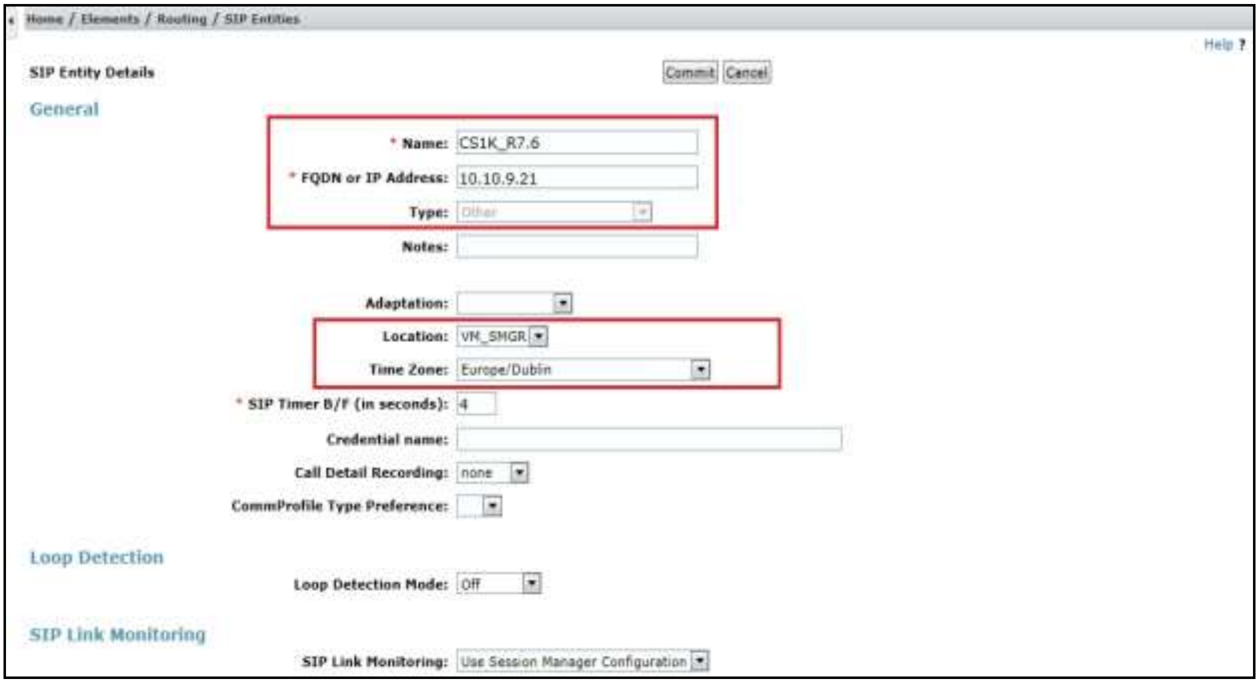
TLS Failover port:

3 Items

☐	Port	Protocol	Default Domain	Notes
☐	5060	TCP	avaya.com	
☐	5060	UDP	avaya.com	
☐	5061	TLS	avaya.com	

6.5.2. Avaya Communication Server 1000 SIP Entity

The following screen shows the SIP entity for CS1000. The **FQDN or IP Address** field is set to the Node IP address of the interface on CS1000 that will be providing SIP signalling as shown in **Section 5.4**. Set **Type** to **Other**, **Location** to that defined in **Section 6.3** and the **Time Zone** to the appropriate time zone.



SIP Entity Details

General

* Name: CS1K_R7.6

* FQDN or IP Address: 10.10.9.21

Type: Other

Notes:

Adaptation:

Location: VM_SMGR

Time Zone: Europe/Dublin

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

Credential name:

Call Detail Recording: none

CommProfile Type Preference:

Loop Detection

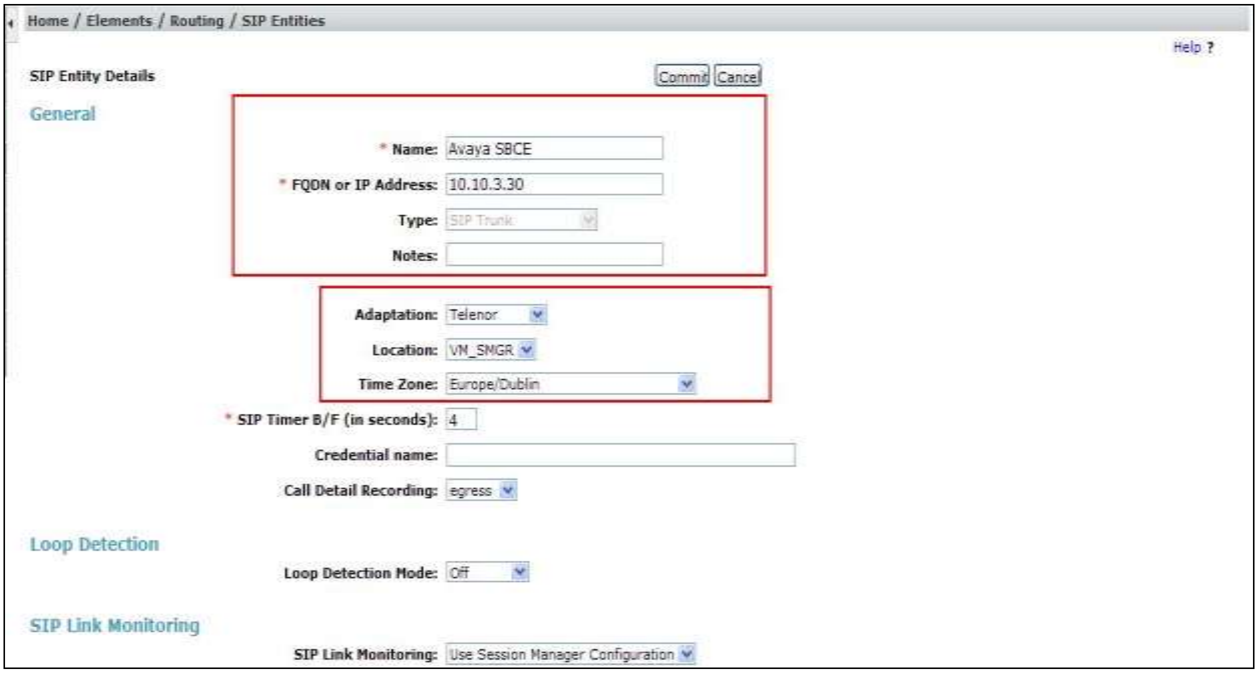
Loop Detection Mode: Off

SIP Link Monitoring

SIP Link Monitoring: Use Session Manager Configuration

6.5.3. Avaya Session Border Controller for Enterprise SIP Entity

The following screen shows the SIP entity for the Avaya SBCE used for routing calls. The **FQDN or IP Address** field is set to the IP address of the Avaya SBCE private network interface (see **Figure 1**). Set **Type** to **SIP Trunk**, **Location** to that defined in **Section 6.3**, set **Adaptation** to one created in **Section 6.4** and the **Time Zone** to the appropriate time zone.



SIP Entity Details

General

* Name: Avaya SBCE

* FQDN or IP Address: 10.10.3.30

Type: SIP Trunk

Notes:

Adaptation: Telenor

Location: VM_SMGR

Time Zone: Europe/Dublin

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

Credential name:

Call Detail Recording: egress

Loop Detection

Loop Detection Mode: Off

SIP Link Monitoring

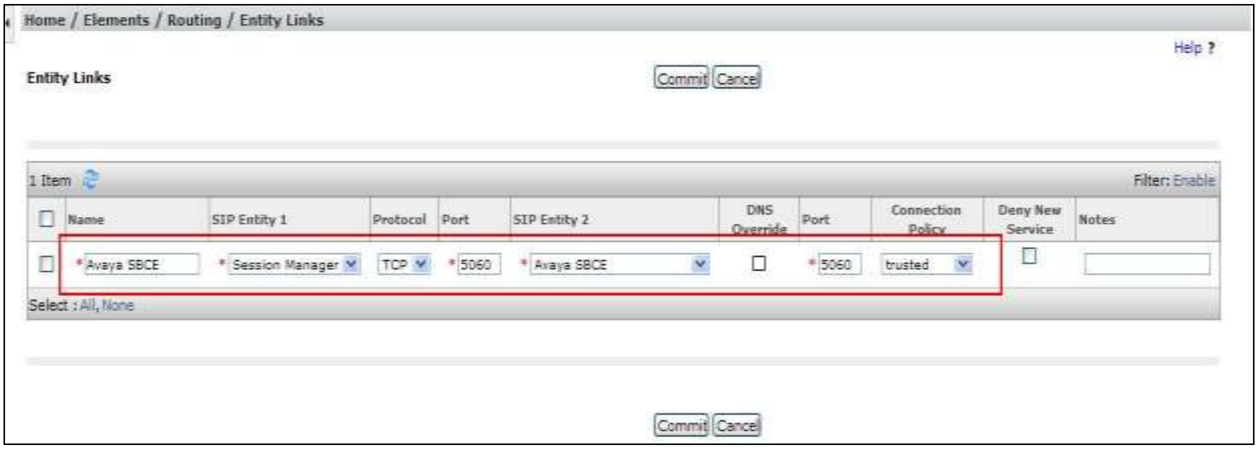
SIP Link Monitoring: Use Session Manager Configuration

6.6. Administer Entity Links

A SIP trunk between Session Manager and another system is described by an entity link. To add an entity link, select **Entity Links** on the left panel menu and click on the **New** button (not shown). Fill in the following fields in the new row that is displayed.

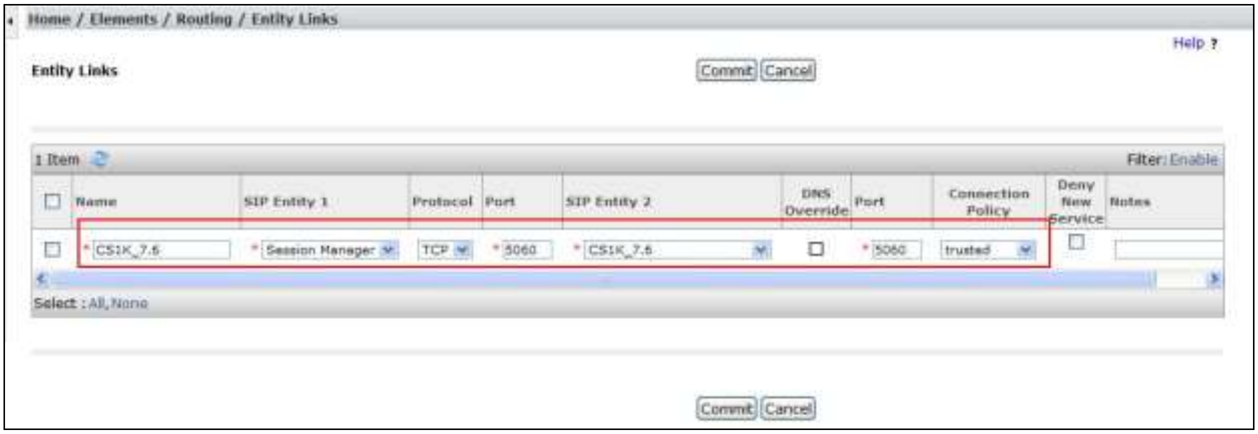
- In the **Name** field enter an informative name.
- In the **SIP Entity 1** field select **Session Manager**.
- In the **Protocol** field select the transport protocol to be used to send SIP requests.
- In the **Port** field enter the port number to which the other system sends its SIP requests.
- In the **SIP Entity 2** field select the other SIP entity for this link, created in **Section 6.5**.
- In the **Port** field enter the port number to which the other system expects to receive SIP requests.
- Select **Trusted** from the drop down menu to make the other system trusted.

Click **Commit** to save changes. The following screen shows the entity links used in this configuration.



Entity Links

☐	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
☐	* Avaya SBCE	* Session Manager	TCP	* 5060	* Avaya SBCE	☐	* 5060	trusted	☐	



Entity Links

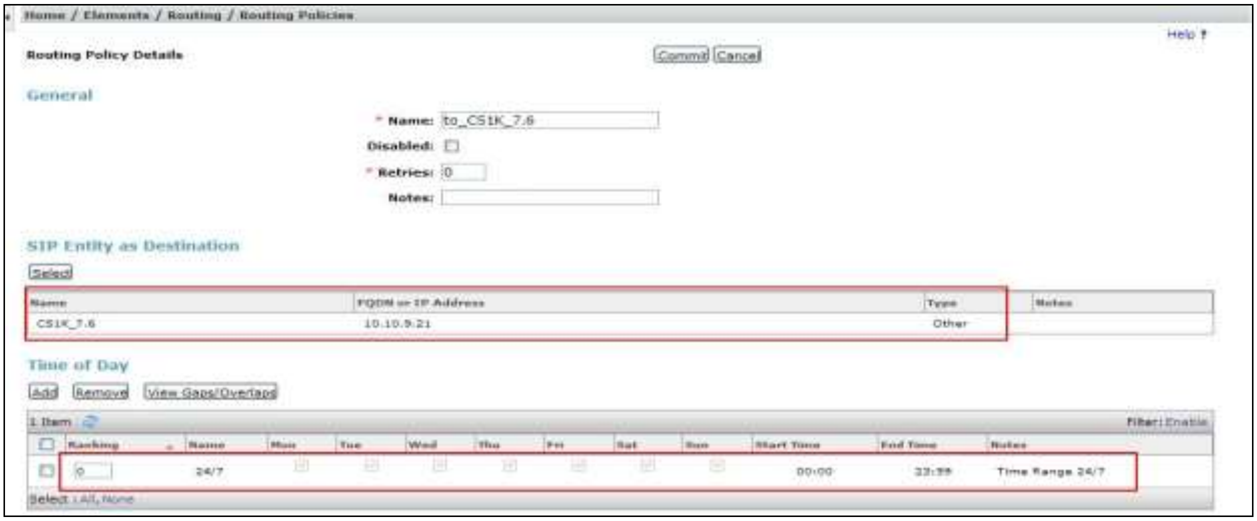
☐	Name	SIP Entity 1	Protocol	Port	SIP Entity 2	DNS Override	Port	Connection Policy	Deny New Service	Notes
☐	* CS1K_7.6	* Session Manager	TCP	* 5060	* CS1K_7.6	☐	* 5060	trusted	☐	

6.7. Administer Routing Policies

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

- Enter an informative name in the **Name** field.
- Under **SIP Entity as Destination**, click **Select**, and then select the appropriate SIP entity to which this routing policy applies.
- Under **Time of Day**, click **Add**, and then select the time range.

The following screen shows the routing policy for Communication Server 1000:



Home / Elements / Routing / Routing Policies

Routing Policy Details

General

* Name: to_CS1K_7.6
Disabled: □
* Retries: 0
Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
CS1K_7.6	10.10.9.21	Other	

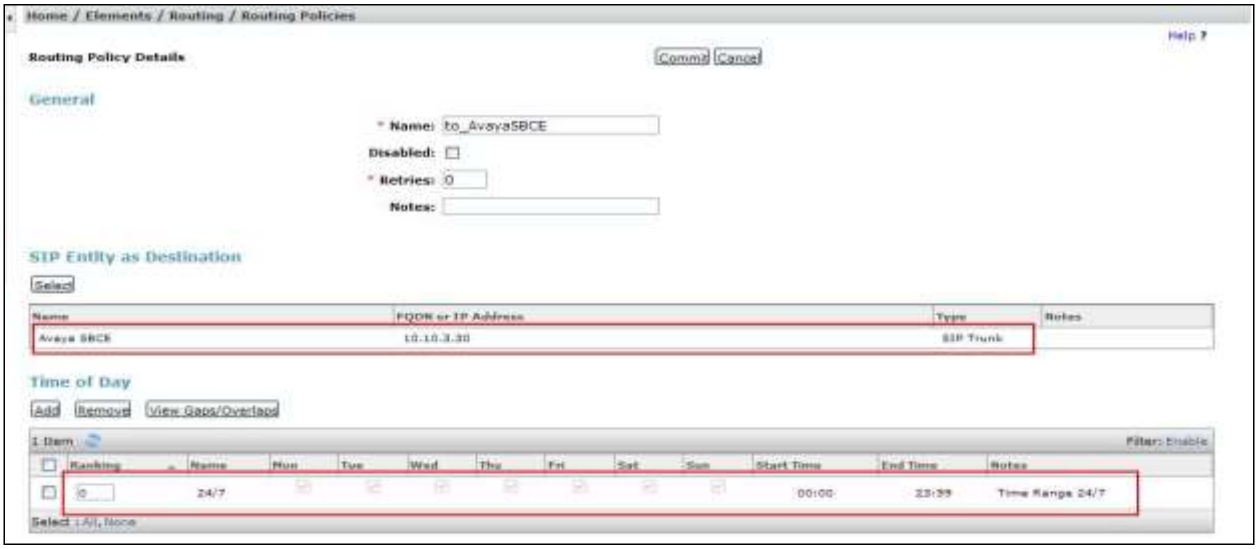
Time of Day

1 Item　　Filter: Enable

□	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
□	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

Select : All, None

The following screen shows the routing policy for the Avaya SBCE:



Home / Elements / Routing / Routing Policies

Routing Policy Details

General

* Name: to_AvayaSBCE
Disabled: □
* Retries: 0
Notes:

SIP Entity as Destination

Name	FQDN or IP Address	Type	Notes
Avaya SBCE	10.10.3.30	SIP Trunk	

Time of Day

1 Item　　Filter: Enable

□	Ranking	Name	Mon	Tue	Wed	Thu	Fri	Sat	Sun	Start Time	End Time	Notes
□	0	24/7	☑	☑	☑	☑	☑	☑	☑	00:00	23:59	Time Range 24/7

Select : All, None

6.8. Administer Dial Patterns

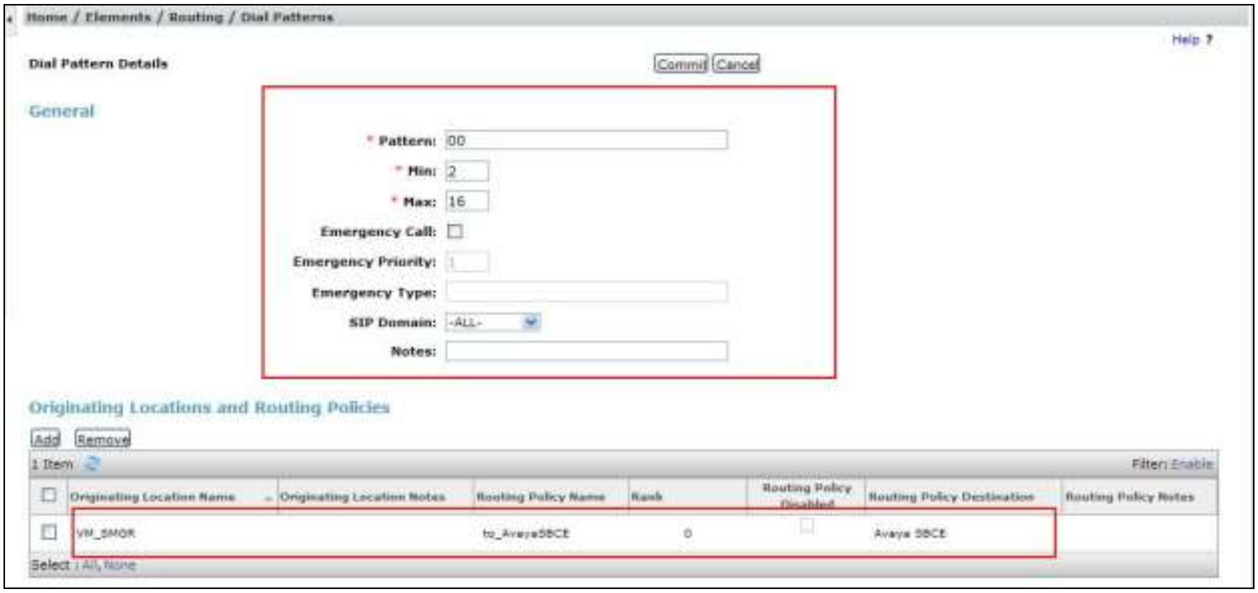
A dial pattern must be defined to direct calls to the appropriate telephony system. To configure a dial pattern select **Dial Patterns** on the left panel menu and then click on the **New** button (not shown).

Under **General**:

- In the **Pattern** field enter a dialed number or prefix to be matched.
- In the **Min** field enter the minimum length of the dialed number.
- In the **Max** field enter the maximum length of the dialed number.
- In the **SIP Domain** field select **–ALL-**.

Under **Originating Locations and Routing Policies**, click **Add**. In the resulting screen (not shown) under **Originating Location** select **Locations** created in **Section 6.3** and under **Routing Policies** select one of the routing policies defined in **Section 6.7**. Click **Select** button to save (not shown).

The following screen shows an example dial pattern configured for the Avaya SBCE which will route the calls out to the PSTN via the Telenor SIP Trunk service.



Dial Pattern Details

General

* Pattern: 00

* Min: 2

* Max: 16

Emergency Call: □

Emergency Priority: 1

Emergency Type:

SIP Domain: -ALL-

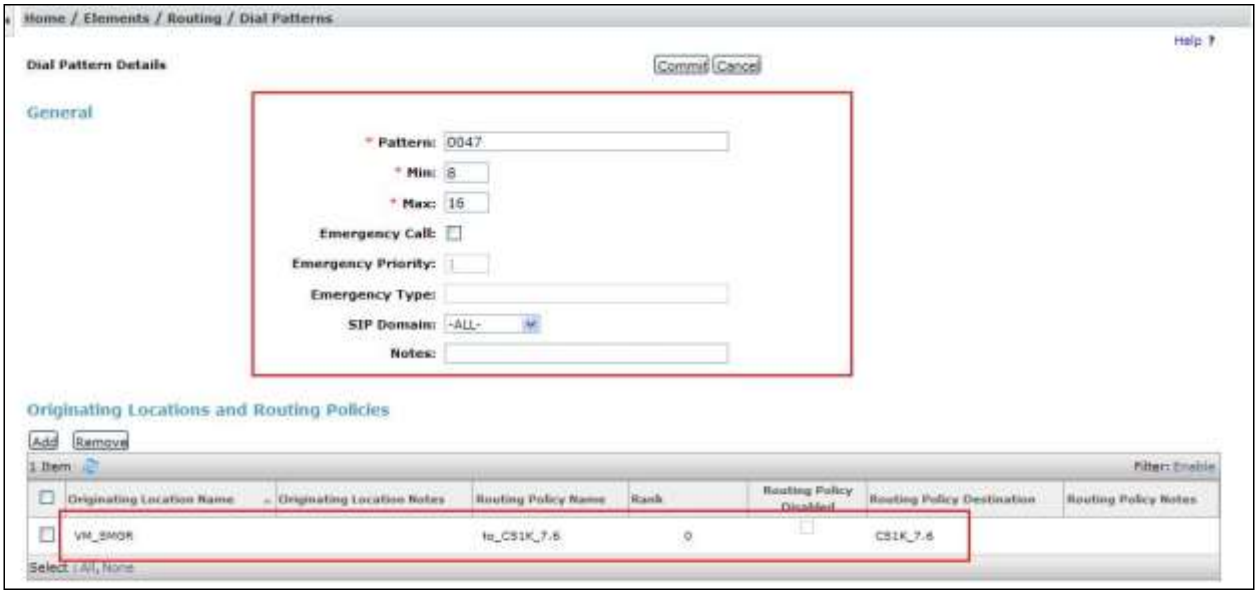
Notes:

Originating Locations and Routing Policies

1 Item

□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	VM_SMGR		to_AvayaSBCE	0	□	Avaya SBCE	

The following screen shows an example dial pattern configured for the CS1000. This dial pattern will route the calls to CS1000 endpoints.



Dial Pattern Details

General

* Pattern:	0047
* Min:	8
* Max:	16
Emergency Call:	□
Emergency Priority:	1
Emergency Type:	
SIP Domain:	-ALL-
Notes:	

Originating Locations and Routing Policies

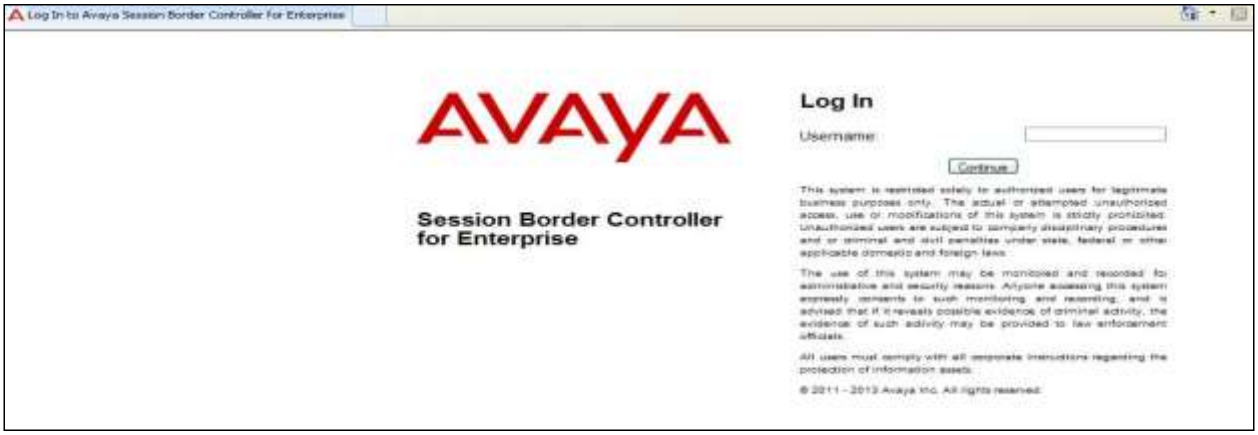
□	Originating Location Name	Originating Location Notes	Routing Policy Name	Rank	Routing Policy Disabled	Routing Policy Destination	Routing Policy Notes
□	VM_SMGR		to_CS1K_7.6	0	□	CS1K_7.6	

7. Configure Avaya Session Border Controller for Enterprise

This section describes the configuration of the Avaya SBCE. The Avaya SBCE provides security and manipulation of signalling to provide an interface to the Service Provider's SIP Trunk that is standard where possible and adapted to the Service Provider's SIP implementation where necessary.

7.1. Access Avaya Session Border Controller for Enterprise

Access the Avaya SBCE using a web browser by entering the URL **https://<ip-address>**, where **<ip-address>** is the management IP address configured at installation and enter the **Username** and **Password**.


Log In to Avaya Session Border Controller for Enterprise
AVAYA
Session Border Controller for Enterprise
Log In
Continue

Username:

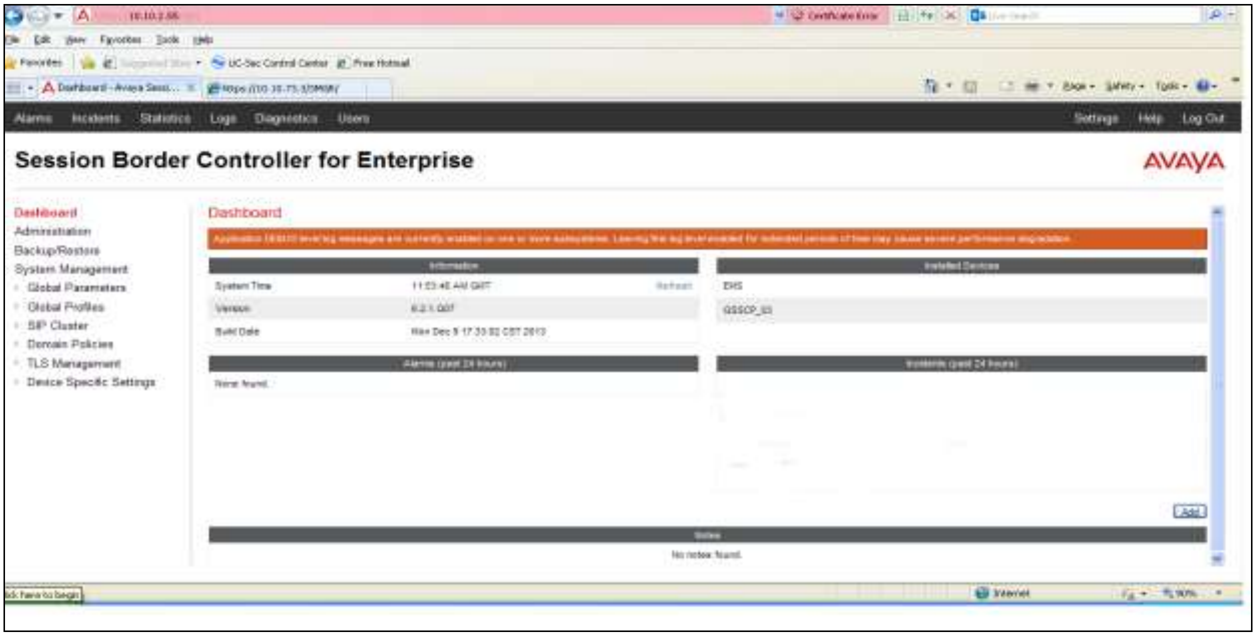
This system is restricted solely to authorized users for legitimate business purposes only. The actual or attempted unauthorized access, use or modifications of this system is strictly prohibited. Unauthorized users are subject to company disciplinary procedures and or criminal and civil penalties under state, federal or other applicable domestic and foreign laws.

The use of this system may be monitored and recorded for administrative and security reasons. Anyone accessing this system expressly consents to such monitoring and recording, and is advised that if it reveals possible evidence of criminal activity, the evidence of such activity may be provided to law enforcement officials.

All users must comply with all corporate instructions regarding the protection of information assets.

© 2011 - 2013 Avaya Inc. All rights reserved.

The main page of the Avaya SBCE will appear.



Dashboard

Information	
System Time	11:53:46 AM GMT
Version	6.2.1.Q07
Build Date	Mon Dec 9 17:33:02 CST 2013

Installed Devices
EMS
GSSCP_33

Alarms (past 24 hours)

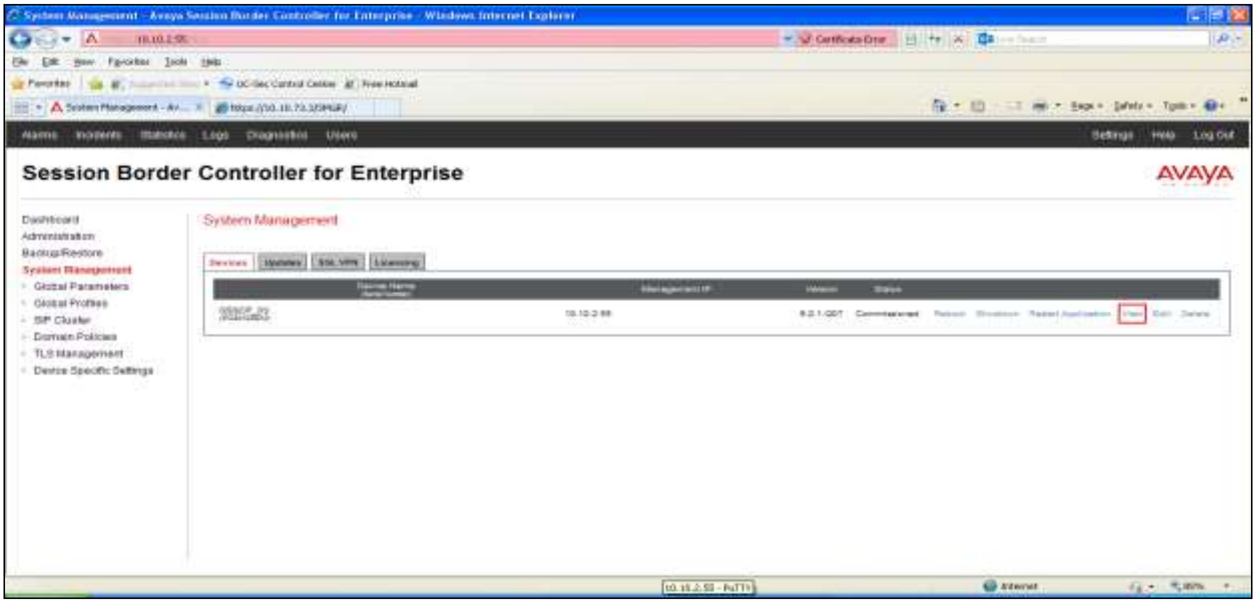
None found.

Incidents (past 24 hours)

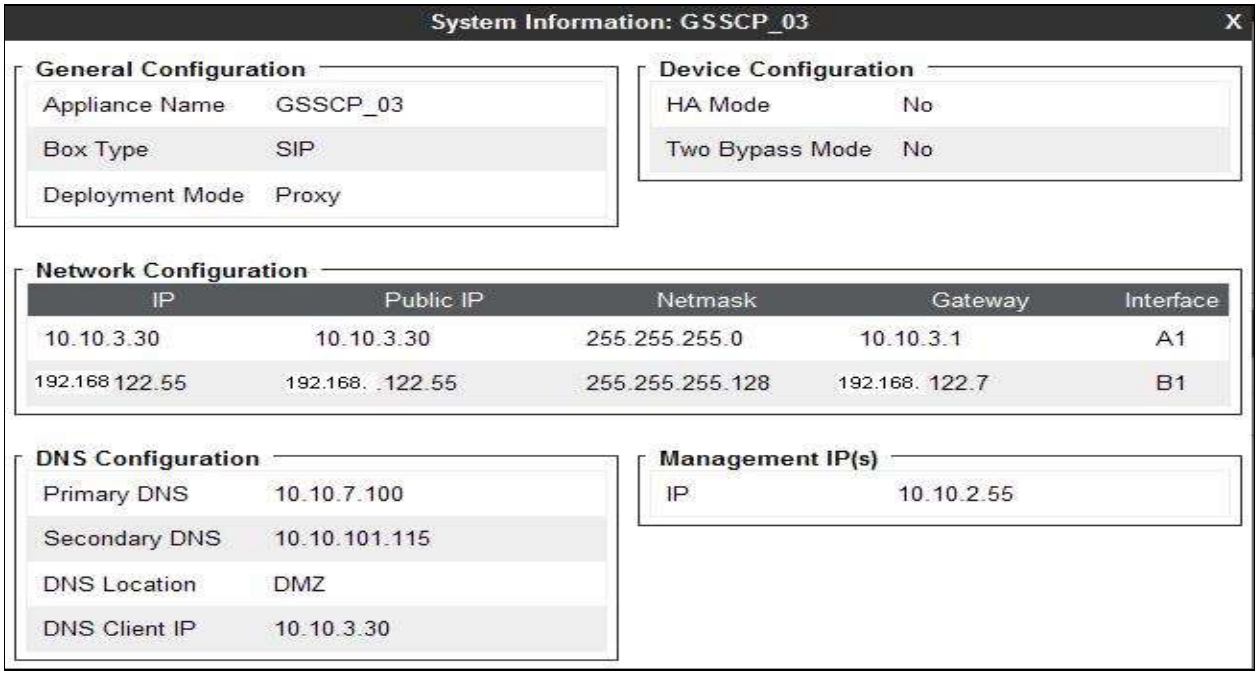
Notes

No notes found.

To view system information that was configured during installation, navigate to **System Management**. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named **GSSCP_03** is shown. To view the configuration of this device, click **View** (the third option from the right).



The **System Information** screen shows the **General Configuration**, **Device Configuration**, **Network Configuration**, **DNS Configuration** and **Management IP** information.



System Information: GSSCP_03

General Configuration

Appliance Name	GSSCP_03
Box Type	SIP
Deployment Mode	Proxy

Device Configuration

HA Mode	No
Two Bypass Mode	No

Network Configuration

IP	Public IP	Netmask	Gateway	Interface
10.10.3.30	10.10.3.30	255.255.255.0	10.10.3.1	A1
192.168 122.55	192.168. .122.55	255.255.255.128	192.168. 122.7	B1

DNS Configuration

Primary DNS	10.10.7.100
Secondary DNS	10.10.101.115
DNS Location	DMZ
DNS Client IP	10.10.3.30

Management IP(s)

IP	10.10.2.55

7.2. Global Profiles

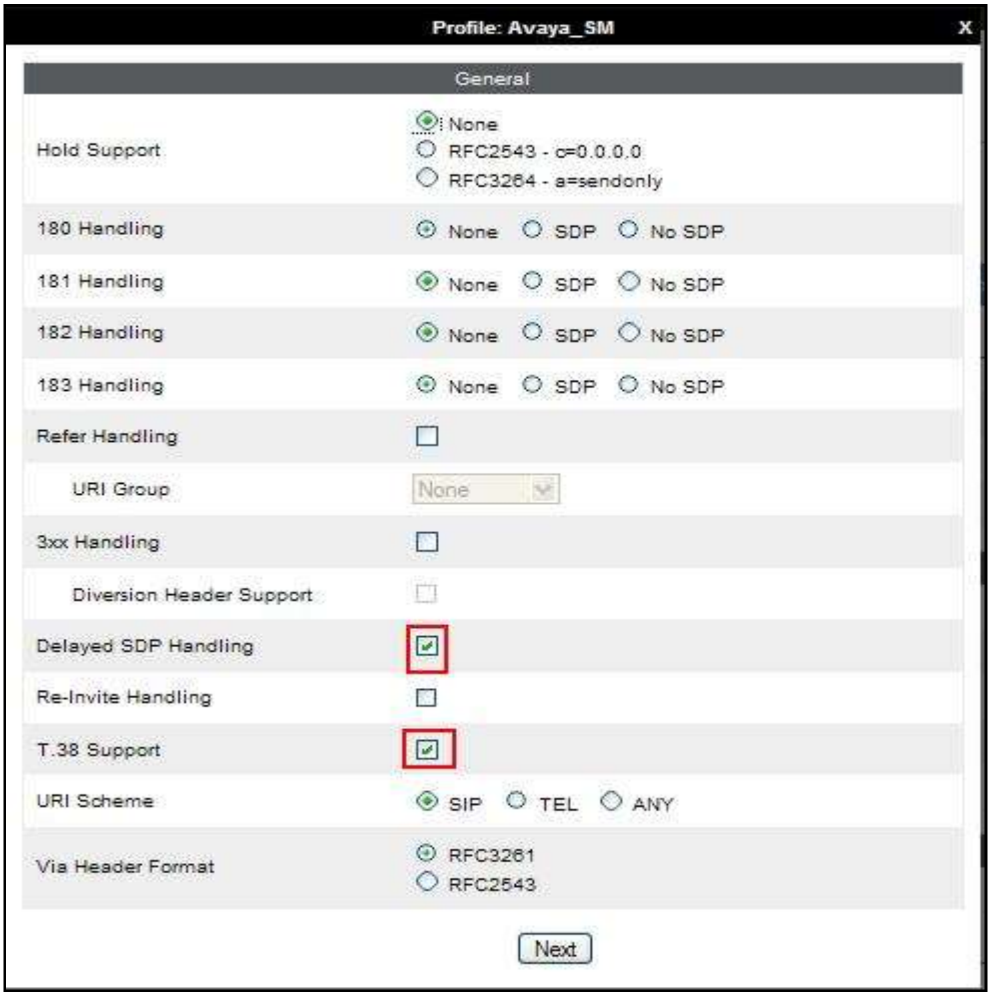
Global Profiles allows for configuration of parameters across all Avaya SBCE appliances.

7.2.1. Server Interworking - Avaya

Server Interworking allows the configuration and management of various SIP call server-specific capabilities such as call hold and T.38. From the left-hand menu select **Global Profiles →** **Server Interworking** and click on **Add Profile.**

- Enter profile name such as **Avaya_SM** and click **Next** (not shown).
- Check **Delayed SDP Handling**.
- Check **T.38 Support**.
- All other options on the **General** Tab can be left at default.

Click on **Next** on the following screens.

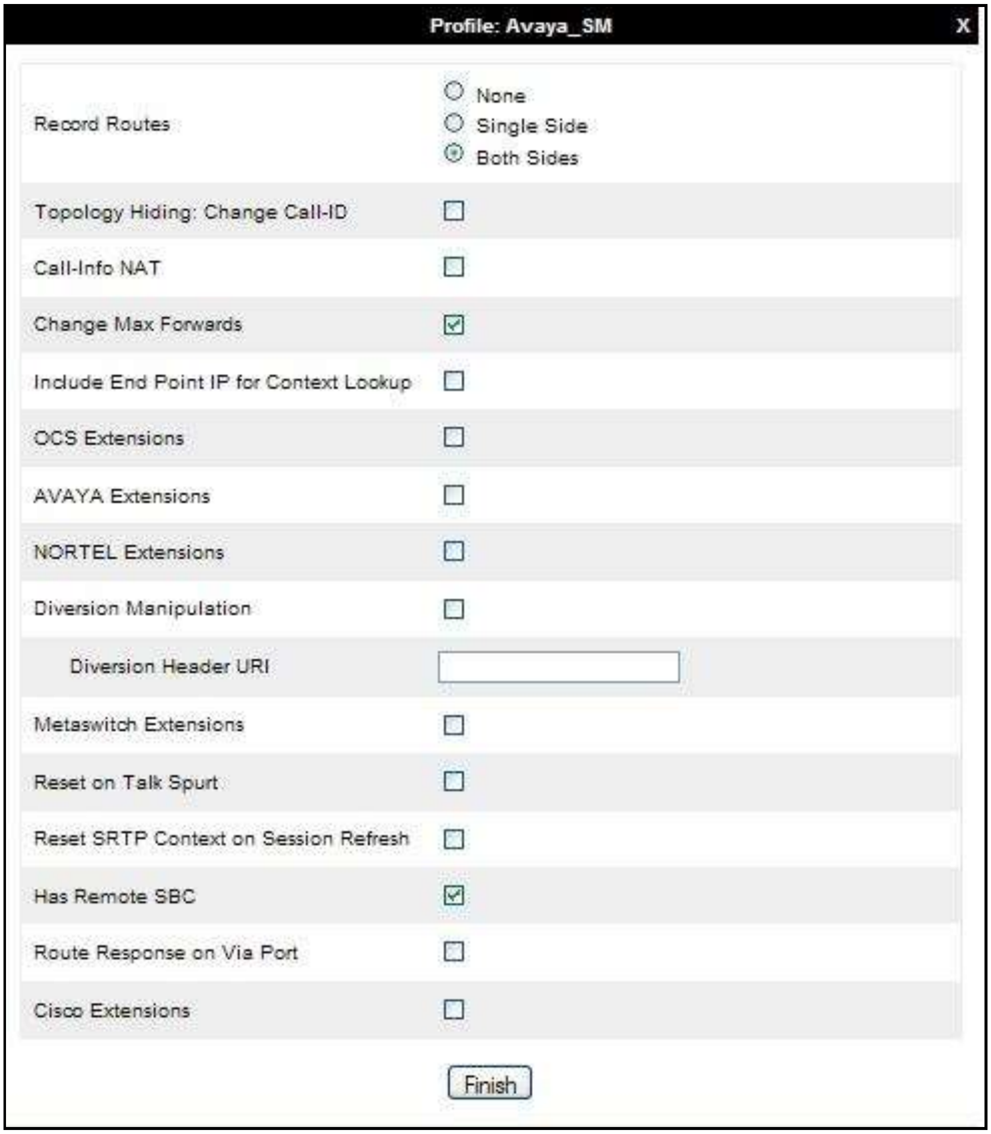


Profile: Avaya_SM

General

Hold Support	● None ○ RFC2543 - c=0.0.0.0 ○ RFC3264 - a=sendonly
180 Handling	● None ○ SDP ○ No SDP
181 Handling	● None ○ SDP ○ No SDP
182 Handling	● None ○ SDP ○ No SDP
183 Handling	● None ○ SDP ○ No SDP
Refer Handling	□
URI Group	None
3xx Handling	□
Diversion Header Support	□
Delayed SDP Handling	☑
Re-Invite Handling	□
T.38 Support	☑
URI Scheme	● SIP ○ TEL ○ ANY
Via Header Format	● RFC3261 ○ RFC2543

Default values can be used for the **Advanced Settings** window (not shown). Click **Finish**.



Profile: Avaya_SM

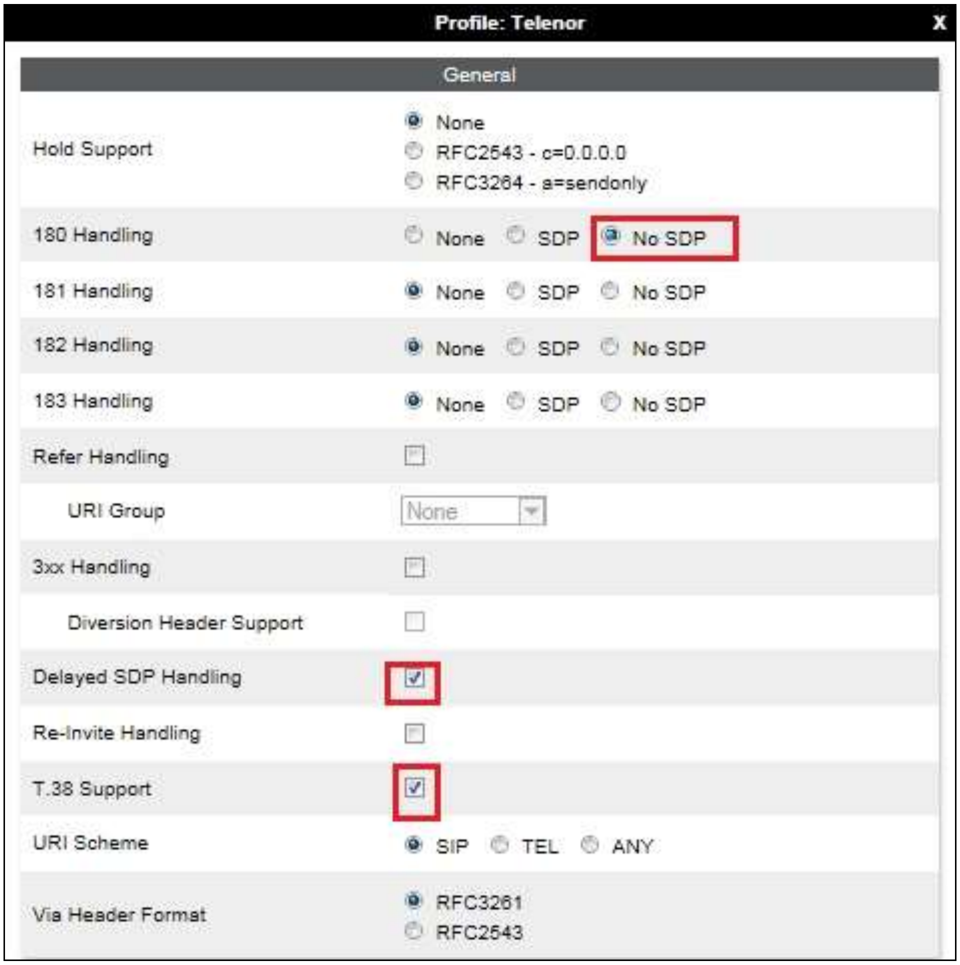
Record Routes	○ None ○ Single Side ● Both Sides
Topology Hiding: Change Call-ID	□
Call-Info NAT	□
Change Max Forwards	☑
Include End Point IP for Context Lookup	□
OCS Extensions	□
AVAYA Extensions	□
NORTEL Extensions	□
Diversion Manipulation	□
Diversion Header URI	
Metaswitch Extensions	□
Reset on Talk Spurt	□
Reset SRTP Context on Session Refresh	□
Has Remote SBC	☑
Route Response on Via Port	□
Cisco Extensions	□

7.2.2. Server Interworking – Telenor

From the left-hand menu select **Global Profiles** → **Server Interworking** and click on **Add Profile** (not shown).

- Enter profile name such as **Telenor** and click **Next** (not shown).
- Check **180 Handling** = **No SDP**.
- Check **Delayed SDP Handling**.
- Check **T.38 Support**.
- All other options on the **General** Tab can be left at default.

Click on **Next** on the following screens.

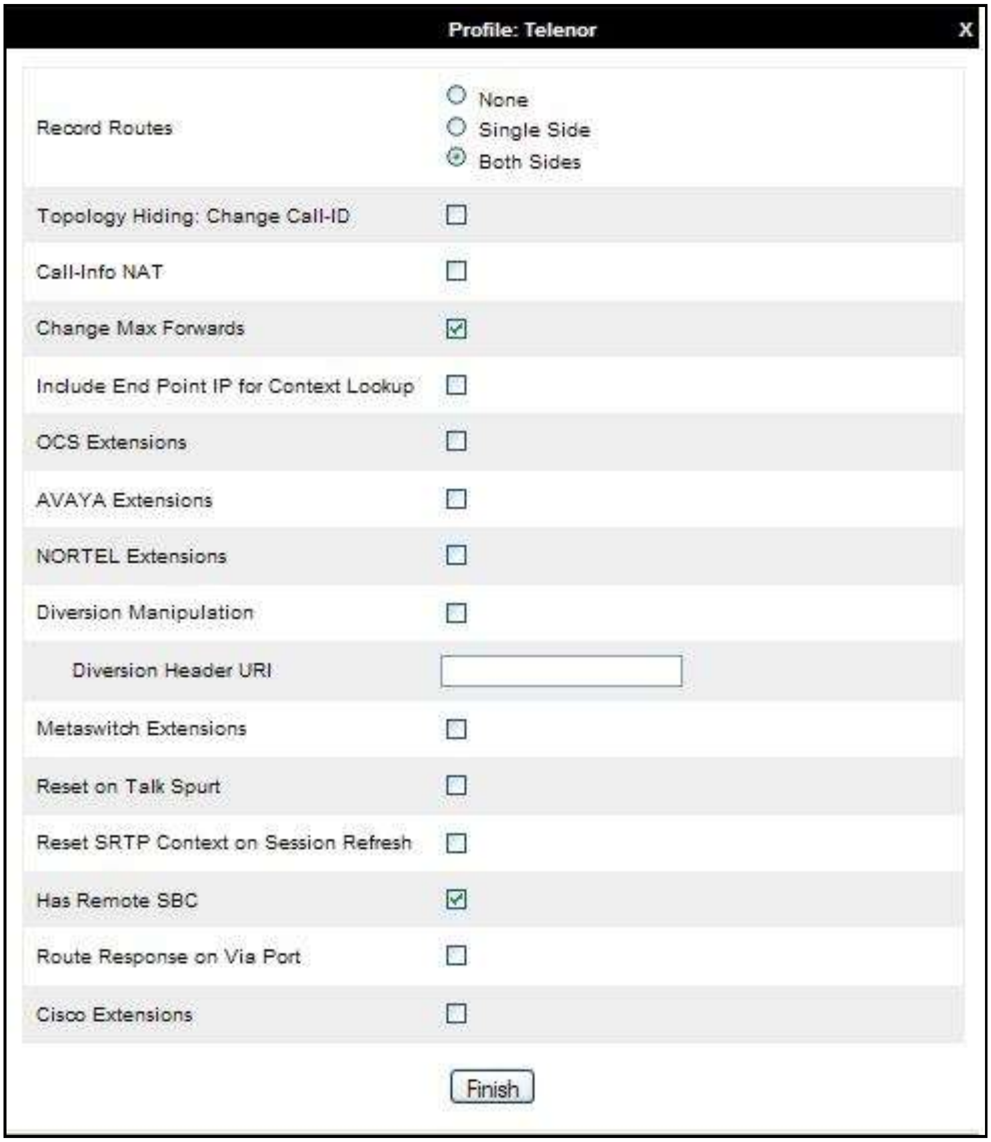


Profile: Telenor

General

Hold Support	● None ○ RFC2543 - c=0.0.0.0 ○ RFC3264 - a=sendonly
180 Handling	○ None ○ SDP ● No SDP
181 Handling	● None ○ SDP ○ No SDP
182 Handling	● None ○ SDP ○ No SDP
183 Handling	● None ○ SDP ○ No SDP
Refer Handling	□
URI Group	None
3xx Handling	□
Diversion Header Support	□
Delayed SDP Handling	☑
Re-Invite Handling	□
T.38 Support	☑
URI Scheme	● SIP ○ TEL ○ ANY
Via Header Format	● RFC3261 ○ RFC2543

Default values can be used for the **Advanced Settings** window (not shown). Click **Finish**.



Profile: Telenor

Record Routes	○ None ○ Single Side ● Both Sides
Topology Hiding: Change Call-ID	□
Call-Info NAT	□
Change Max Forwards	☑
Include End Point IP for Context Lookup	□
OCS Extensions	□
AVAYA Extensions	□
NORTEL Extensions	□
Diversion Manipulation	□
Diversion Header URI	
Metaswitch Extensions	□
Reset on Talk Spurt	□
Reset SRTP Context on Session Refresh	□
Has Remote SBC	☑
Route Response on Via Port	□
Cisco Extensions	□

7.2.3. Routing

Routing profiles define a specific set of packet routing criteria that are used in conjunction with other types of domain policies to identify a particular call flow and thereby ascertain which security features will be applied to those packets. Parameters defined by Routing Profiles include packet transport settings, name server addresses and resolution methods, next hop routing information, and packet transport types.

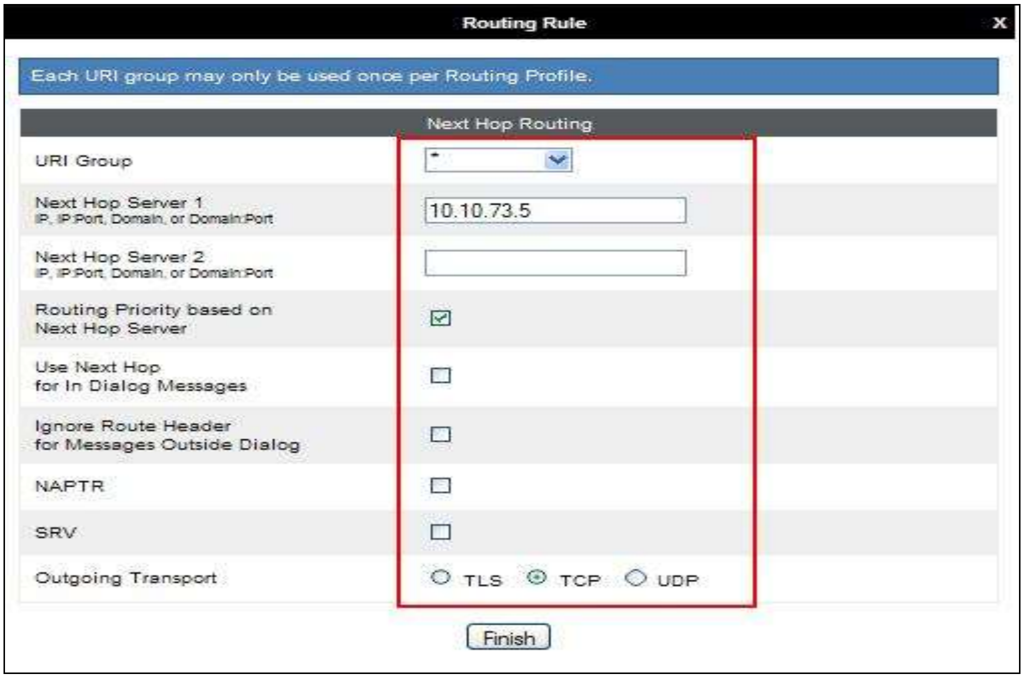
Routing information is required for routing to Session Manager on the internal side and the Telenor address on the external side. The IP addresses and ports defined here will be used as the destination addresses for signalling. If no port is specified in the **Next Hop IP Address**, default 5060 is used.

Create a Routing Profile for both Session Manager and Telenor SIP trunk. To add a routing profile, navigate to **Global Profiles → Routing** and select **Add Profile**. Enter a **Profile Name** and click **Next** to continue.
In the new window that appears, enter the following values. Use default values for all remaining fields:

- **URI Group:** Select "*****" from the drop down box.
- **Next Hop Server 1:** Enter the Domain Name or IP address of the Primary Next Hop server, e.g. Session Manager.
- **Next Hop Server 2:** (Optional) Enter the Domain Name or IP address of the secondary Next Hop server.
- **Routing Priority based on Next Hop Server**: Checked.
- **Use Next Hop for In Dialog Messages**: Select only if there is no secondary Next Hopserver.
- **Outgoing Transport:** Choose the protocol used for transporting outgoing signaling packets.

Click **Finish**.

The following screen shows the Routing Profile to Session Manager.

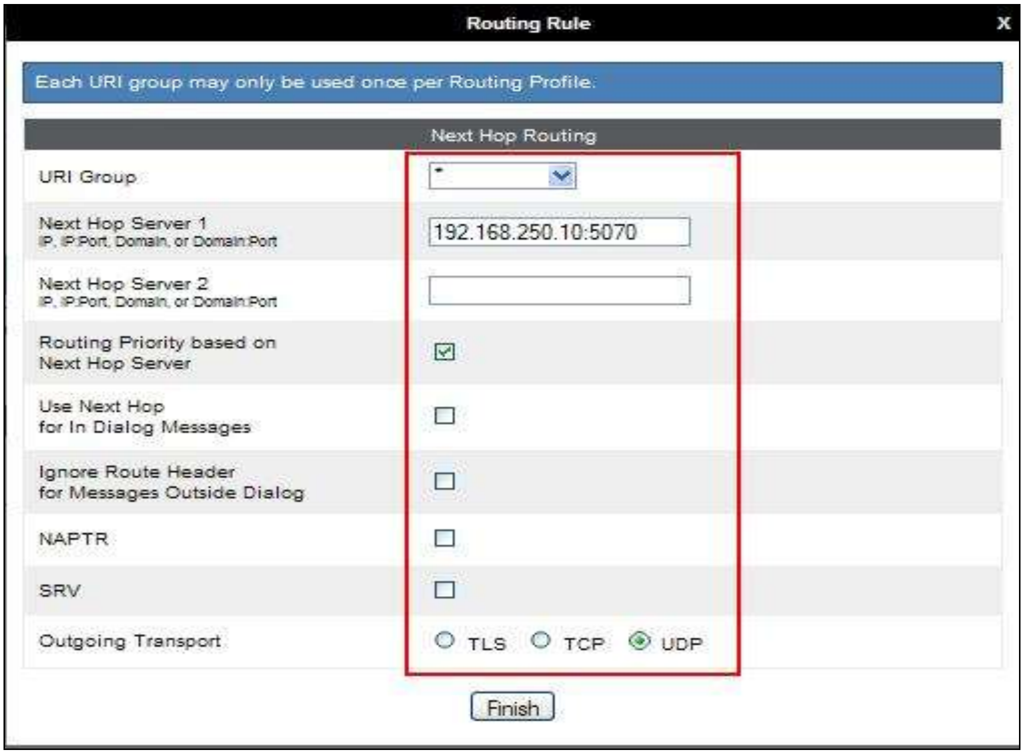


Routing Rule

Each URI group may only be used once per Routing Profile.

Next Hop Routing	
URI Group	*
Next Hop Server 1 IP, IP:Port, Domain, or Domain:Port	10.10.73.5
Next Hop Server 2 IP, IP:Port, Domain, or Domain:Port	
Routing Priority based on Next Hop Server	☑
Use Next Hop for In Dialog Messages	□
Ignore Route Header for Messages Outside Dialog	□
NAPTR	□
SRV	□
Outgoing Transport	○ TLS ● TCP ○ UDP

The following screen shows the Routing Profile to Telenor. Note: IP Port **5070** was used in the Telenor configuration for this compliance test.



Routing Rule

Each URI group may only be used once per Routing Profile.

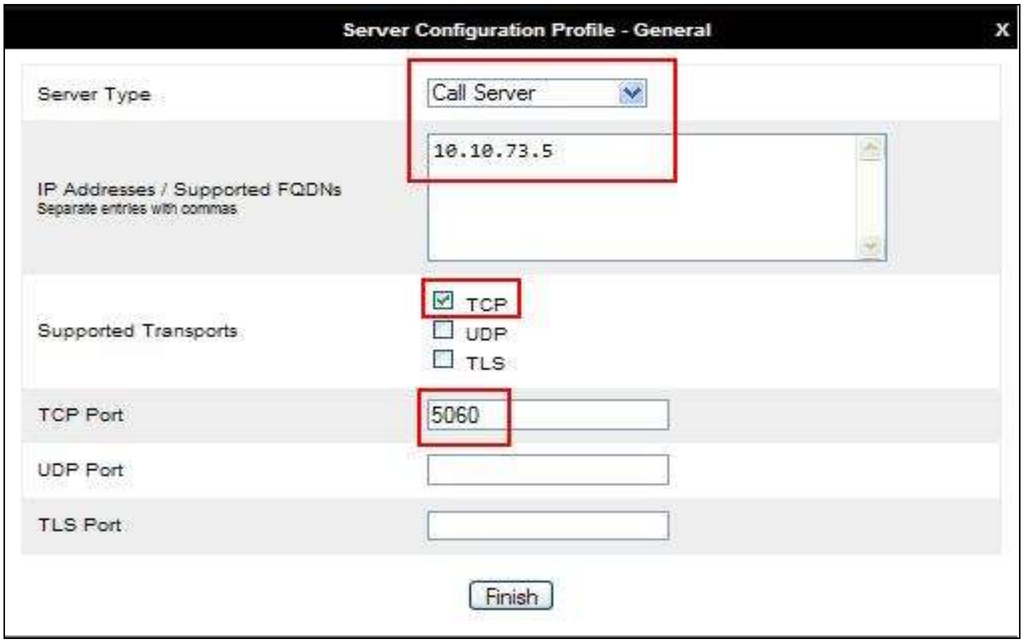
Next Hop Routing	
URI Group	*
Next Hop Server 1 IP, IP:Port, Domain, or Domain:Port	192.168.250.10:5070
Next Hop Server 2 IP, IP:Port, Domain, or Domain:Port	
Routing Priority based on Next Hop Server	☑
Use Next Hop for In Dialog Messages	□
Ignore Route Header for Messages Outside Dialog	□
NAPTR	□
SRV	□
Outgoing Transport	○ TLS ○ TCP ● UDP

7.2.4. Server Configuration – Avaya Aura® Session Manager

Servers are defined for each server connected to the Avaya SBCE. In this case, Telenor is connected as the Trunk Server and Session Manager is connected as the Call Server.

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs allow the configuration and management of various SIP call server-specific parameters such as TCP and UDP port assignments, IP Server type, heartbeat signaling parameters and some advanced options. From the left-hand menu select **Global Profiles → Server Configuration** and click on **Add Profile** and enter a descriptive name (not shown). On the **Add Server Configuration Profile** tab, set the following:

- Select **Server Type** to be **Call Server**.
- Enter **IP Addresses / Supported FQDNs** to **10.10.73.5** (Session Manager IP Address).
- For **Supported Transports**, check **TCP**.
- Set **TCP Port** to **5060**.
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs.


Server Configuration Profile - General

Server Type: Call Server

IP Addresses / Supported FQDNs
Separate entries with commas: 10.10.73.5

Supported Transports: ☑ TCP ☐ UDP ☐ TLS

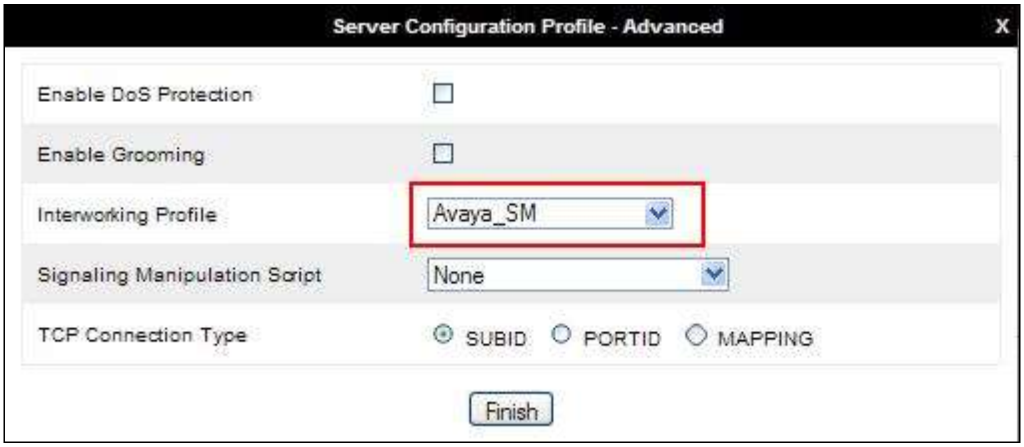
TCP Port: 5060

UDP Port:

TLS Port:

On the **Advanced** tab:

- Select **Avaya_SM** for **Interworking Profile**.
- Click **Finish**.



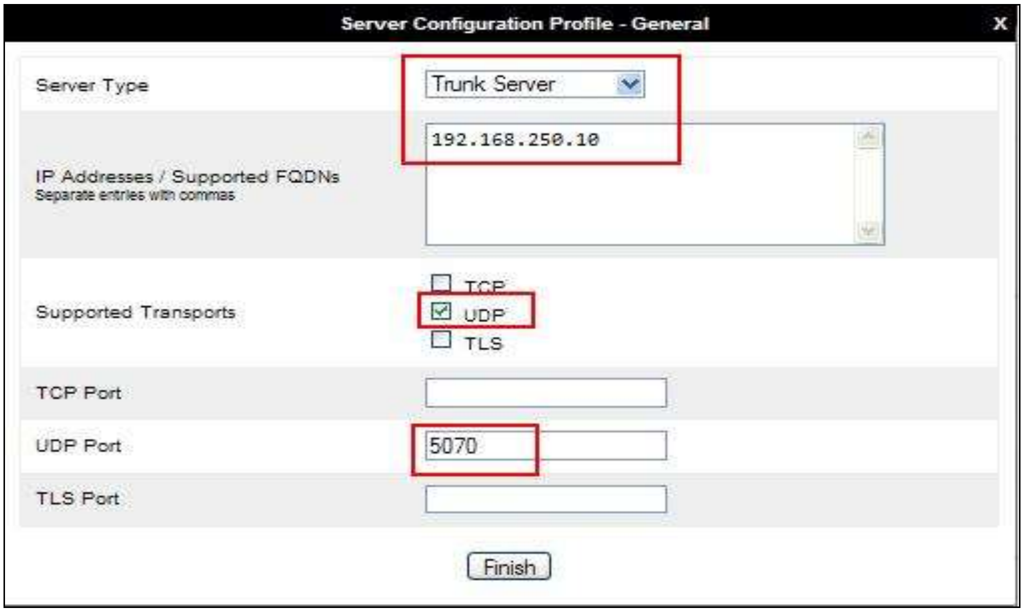
Server Configuration Profile - Advanced

Enable DoS Protection	□
Enable Grooming	□
Interworking Profile	Avaya_SM
Signaling Manipulation Script	None
TCP Connection Type	● SUBID ○ PORTID ○ MAPPING

7.2.5. Server Configuration – Telenor

To define the Telenor Trunk Server, navigate to select **Global Profiles → Server Configuration** and click on **Add Profile** and enter a descriptive name (not shown). On the **Add Server Configuration Profile** tab, click on **Edit** and set the following:

- Select **Server Type** as **Trunk Server**.
- Set **IP Address** to **192.168.250.10** (Telenor SIP Trunk).
- **Supported Transports**: Check **UDP**.
- Set **UDP Port** to **5070**.
- Click on **Next** (not shown) to use default entries on the **Authentication** and **Heartbeat** tabs.

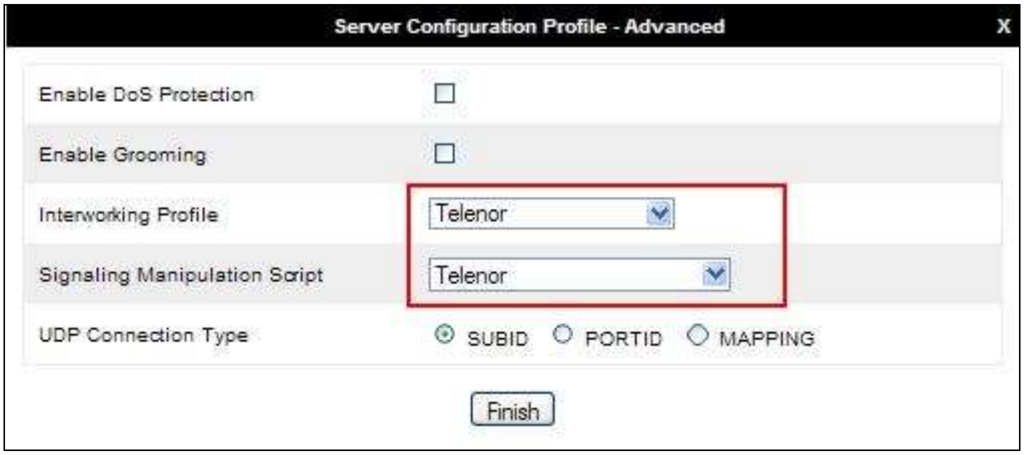


Server Configuration Profile - General

Server Type	Trunk Server
IP Addresses / Supported FQDNs Separate entries with commas	192.168.250.10
Supported Transports	□ TCP ☑ UDP □ TLS
TCP Port	
UDP Port	5070
TLS Port	

On the **Advanced** tab:

- Select **Telenor** for **Interworking Profile**.
- Select **Telenor** for **Signaling Manipulation Script** (**Section 7.2.7**).
- Click **Finish**.



Server Configuration Profile - Advanced

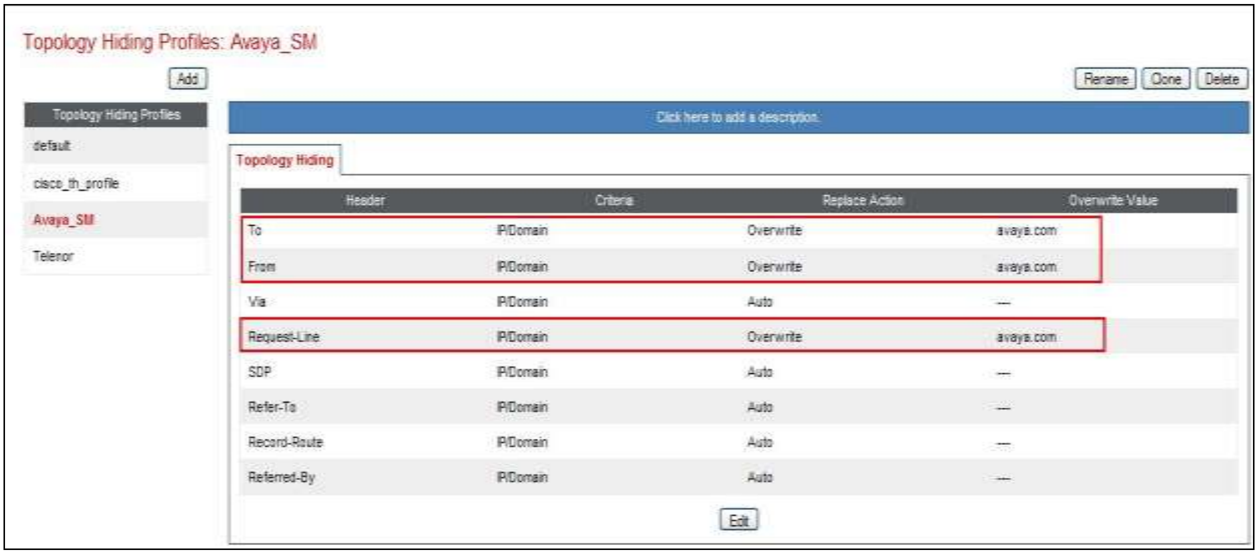
Enable DoS Protection	□
Enable Grooming	□
Interworking Profile	Telenor
Signaling Manipulation Script	Telenor
UDP Connection Type	● SUBID ○ PORTID ○ MAPPING

7.2.6. Topology Hiding

Topology hiding is used to hide local information such as private IP addresses and local domain names. The local information can be overwritten with a domain name or IP addresses. The default **Replace Action** is **Auto**, this replaces local information with IP addresses, generally the next hop. Topology hiding has the advantage of presenting single Via and Record-Route headers externally where multiple headers may be received from the enterprise, particularly from Session Manager. In some cases where Topology Hiding can't be applied, in particular the Contact header, IP addresses are translated to the Avaya SBCE external addresses using NAT.

To define Topology Hiding for the Session Manager, navigate to **Global Profiles → Topology Hiding** in the menu on the left-hand side (not shown). Click on **Add Profile** and enter details in the **Topology Hiding Profile** pop-up menu (not shown).

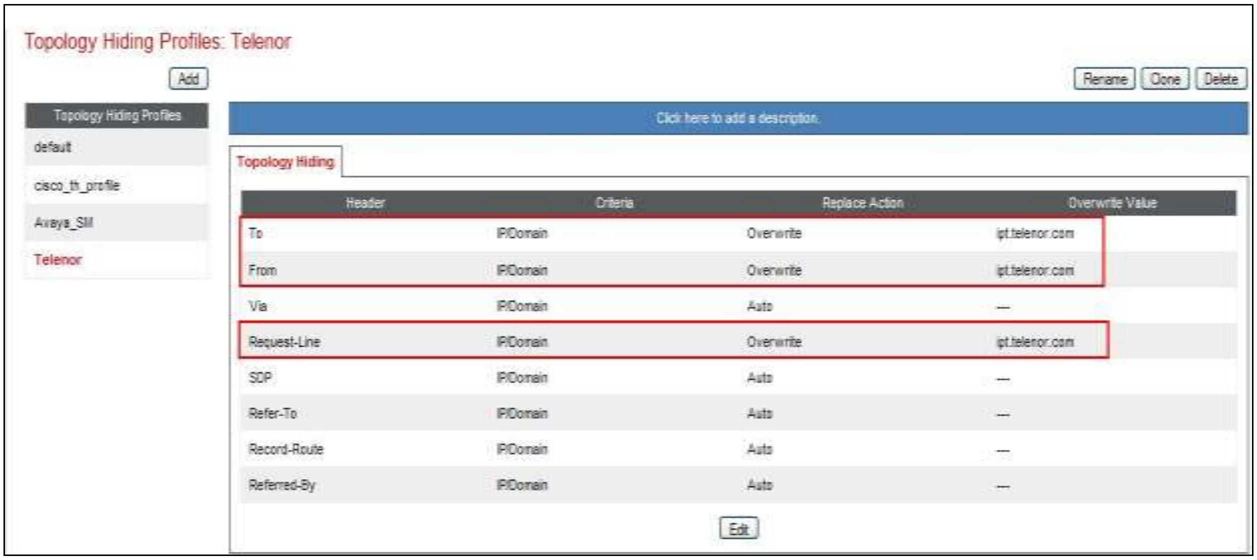
- Enter a descriptive Profile Name such as **Avaya_SM**.
- Under the **Header** field for **To**, **From** and **Request Line**, select **IP/Domain** under **Criteria** and **Overwrite** under **Replace Action**. For **Overwrite Value**, insert **avaya.com**.
- Click **Finish** (not shown).



Header	Criteria	Replace Action	Overwrite Value
To	IP/Domain	Overwrite	avaya.com
From	IP/Domain	Overwrite	avaya.com
Via	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	avaya.com
SDP	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---

To define Topology Hiding for Telenor, navigate to **Global Profiles → Topology Hiding** in the menu on the left hand side (not shown). Click on **Add Profile** and enter details in the **Topology Hiding Profile** pop-up menu (not shown).

- Enter a descriptive Profile Name such as **Telenor**.
- Under the **Header** field for **To**, **From** and **Request Line**, select **IP/Domain** under **Criteria** and **Overwrite** under **Replace Action**. For **Overwrite Value**, insert **ipt.telenor.com**.
- Click **Finish** (not shown).



Topology Hiding Profiles: Telenor

Header	Criteria	Replace Action	Overwrite Value
To	IP/Domain	Overwrite	ipt.telenor.com
From	IP/Domain	Overwrite	ipt.telenor.com
Via	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	ipt.telenor.com
SDP	IP/Domain	Auto	---
Refer-To	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
Referred-By	IP/Domain	Auto	---

7.2.7. Signaling Manipulation

The Signaling Manipulation feature allows the ability to add, change and delete any of the headers in a SIP message. This feature will add the ability to configure such manipulation in a highly flexible manner using a proprietary scripting language called SigMa. The SigMa scripting language is designed to express any of the SIP header manipulation operations to be done by the Avaya SBCE.

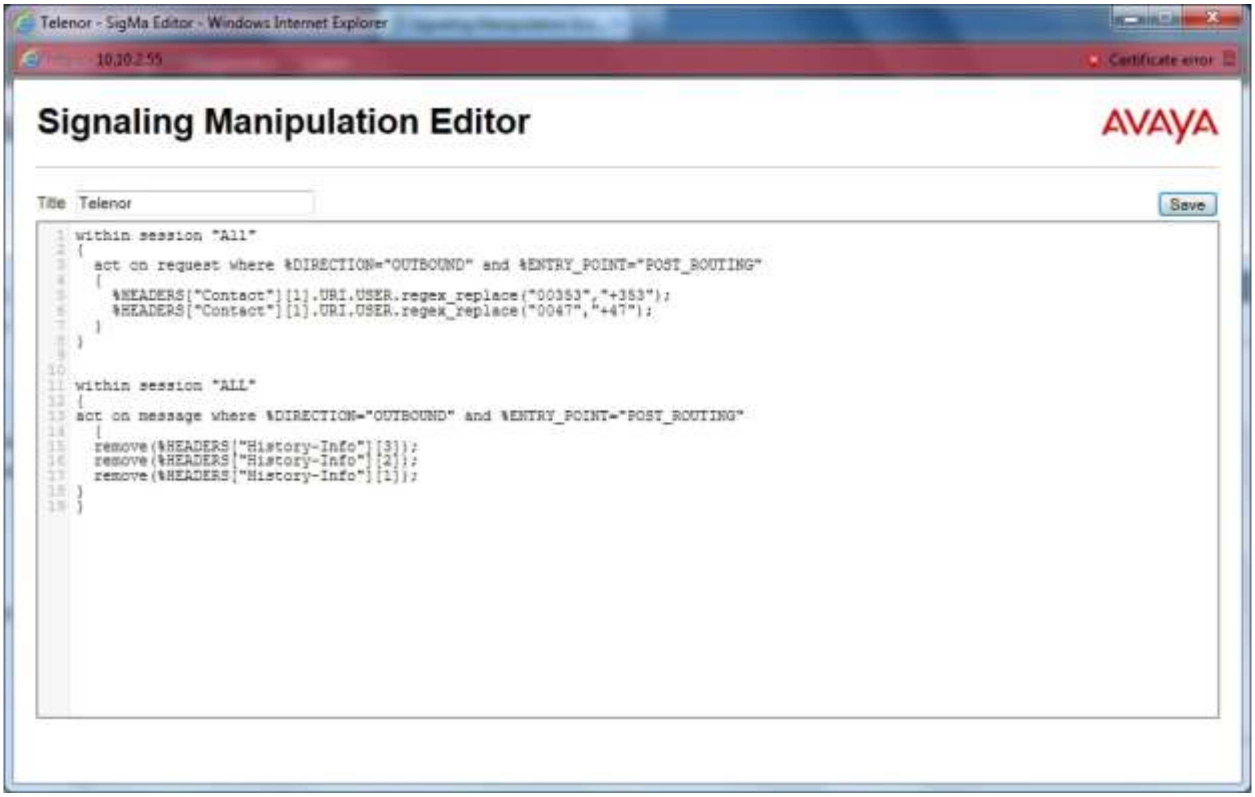
On outbound international calls from the CS1000, it was observed that the numbering format in the Contact Header contained "00" instead of "+". Telenor require all international numbering format to be E.164. Telenor also required the removal of History-Info Headers from all messaging. A SigMa script was required on the Avaya SBCE to convert the "00" to "+" in the Contact Header and remove unwanted History-Info Headers from all messaging.

To define the signalling manipulation, navigate to **Global Profiles → Signaling Manipulation** in the main menu on the left hand side (not shown). Click on **Add Script** and enter a title in the script editor (not shown). The script text is displayed below.

```
within session "All"
{
  act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    %HEADERS["Contact"][1].URI.USER.regex_replace("00353","+353");
    %HEADERS["Contact"][1].URI.USER.regex_replace("0047","+47");
  }
}


within session "ALL"
{
act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
  remove(%HEADERS["History-Info"][3]);
  remove(%HEADERS["History-Info"][2]);
  remove(%HEADERS["History-Info"][1]);
}
}
```

Once entered and saved, the script appears as shown in the following screenshot:


Telenor - SigMa Editor - Windows Internet Explorer
10.10.2.55
Certificate error
Signaling Manipulation Editor
AVAYA
Save

Title Telenor

```
within session "All"
{
  act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
    %HEADERS["Contact"][1].URI.USER.regex_replace("00353","+353");
    %HEADERS["Contact"][1].URI.USER.regex_replace("0047","+47");
  }
}


within session "ALL"
{
act on message where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
  {
  remove(%HEADERS["History-Info"][3]);
  remove(%HEADERS["History-Info"][2]);
  remove(%HEADERS["History-Info"][1]);
}
}
```

7.3. Domain Policies

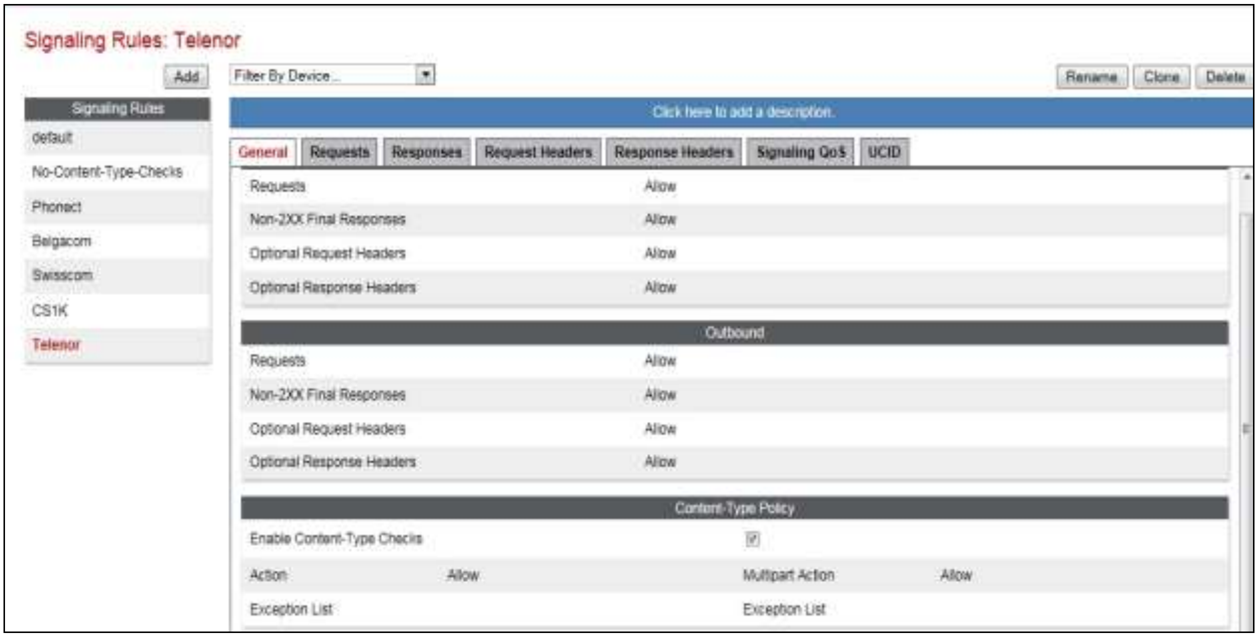
Domain Policies allow the configuration of sets of rules designed to control and normalize the behavior of call flows, based upon various criteria of communication sessions originating from or terminating in the enterprise. Domain Policies include rules for Application, Media, Signaling, Security, etc.

In the reference configuration, only a new Signaling Rule was defined. All other rules under Domain Policies, linked together on End Point Policy Groups later in this section, used one of the default sets already pre-defined in the configuration. Please note that changes should not be made to any of the defaults. If changes are needed, it is recommended to create a new rule by cloning one the defaults and then make the necessary changes to the new rule.

7.3.1. Signalling Rules

Signalling rules are a mechanism on the Avaya SBCE to manipulate the signalling beyond simple header manipulation. Signaling Rules allow action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. In the case of Telenor, the SIP messages are manipulated to avoid the overhead of re-assembling fragmented UDP packets, reduce packet size and removed unnecessary Headers. This is achieved by removing Avaya proprietary and unnecessary headers to reduce the SIP messages packet size to below the Maximum Transmission Unit (MTU) so that fragmentation does not occur.
To define the signalling rule, navigate to **Domain Policies →Signaling Rules** in the main menu on the left hand side. Click on **Add** and enter details in the Signalling Rule pop-up box.

- In the **Rule Name** field enter a descriptive name such as **Telenor** for the signalling rule to remove Avaya proprietary and unnecessary headers and click **Next** and **Next** again, then **Finish** (not shown).



Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

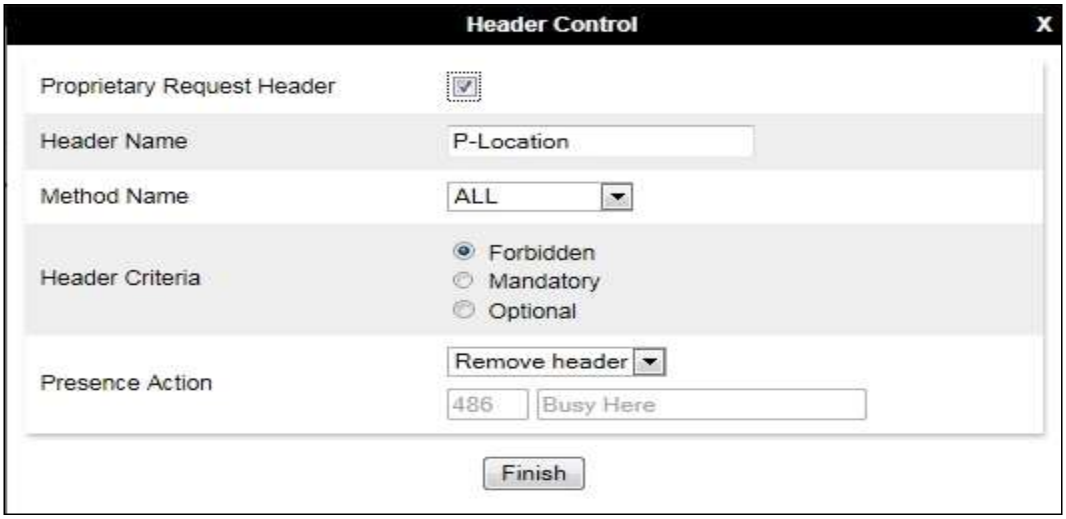
Outbound	
Requests	Allow
Non-2XX Final Responses	Allow
Optional Request Headers	Allow
Optional Response Headers	Allow

Content-Type Policy			
Enable Content-Type Checks		☑	
Action	Allow	Multipart Action	Allow
Exception List		Exception List	

Select the **Request Headers** tab (not shown) and define the rules to remove Avaya proprietary headers as follows:

- Click on **Add In Header Control** (not shown).
- Check the **Proprietary Request Header** box.
- Enter the name of the header to be removed in the **Header Name** field.
- Select **ALL** in the **Method Name** field.
- Check **Forbidden** in the **Header Criteria** options.
- In the **Presence Action** drop down menu, select **Remove header**.
- Click **Finish**.

The following example shows configuration for removal of **P-Location** headers from request messages.



Proprietary Request Header ☑

Header Name P-Location

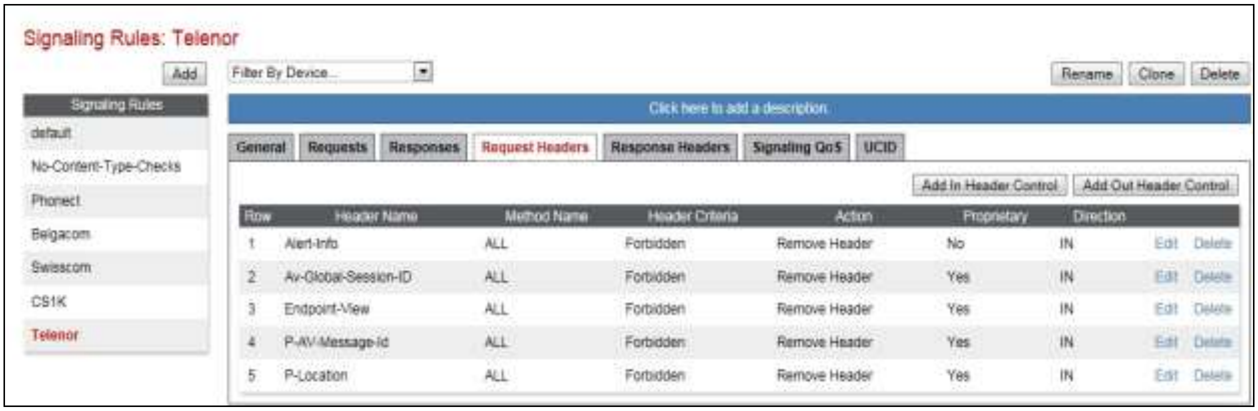
Method Name ALL

Header Criteria ● Forbidden ○ Mandatory ○ Optional

Presence Action Remove header 486 Busy Here

Note: The above is an example of the proprietary headers. During test, the same was done for Alert-Info, Av-Global-Session-ID, Endpoint-View, P-AV-Message-Id, P-Charging-Vector and P-Location headers.

When finished, all the Request Headers defined will be shown under the **Request Headers** tab as shown in the screenshot.



Signaling Rules: Telenor

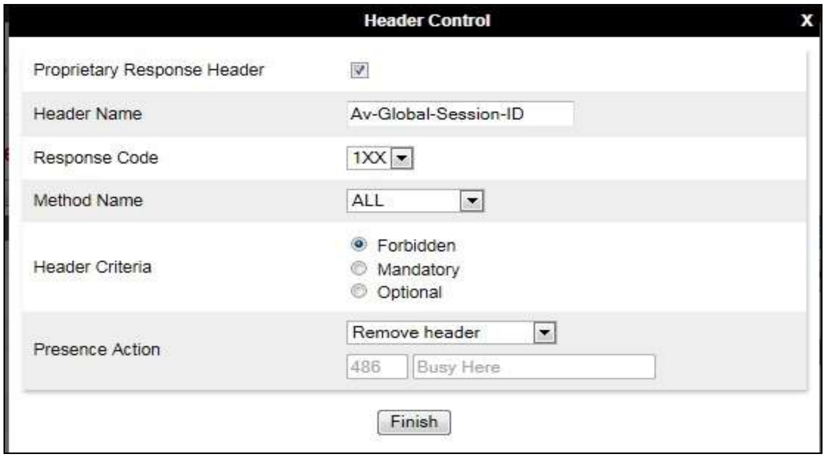
Row	Header Name	Method Name	Header Criteria	Action	Proprietary	Direction		
1	Alert-Info	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
2	Av-Global-Session-ID	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
3	Endpoint-View	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
4	P-AV-Message-Id	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
5	P-Location	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete

The same is required for Response headers. Select the **Response Headers** tab (not shown) and define the rules to remove Avaya proprietary headers as follows:

- Click on **Add In Header Control** (not shown).
- Check the **Proprietary Response Header** box.
- Enter the name of the header to be removed in the **Header Name** field.
- Select **1XX** in the **Response Code** drop down menu, this will remove the header from 183 Session Progress and 180 Ringing messages.
- Select **ALL** in the **Method Name** field.
- Check **Forbidden** in the **Header Criteria** options.
- In the **Presence Action** drop down menu, select **Remove header**
- Click **Finish**.

Repeat above process and select **2XX** in the **Response Code** so that the header is removed from 200 OK messages.

The following example shows configuration for removal of **Av-Global-Session-ID** headers from **1XX** responses.

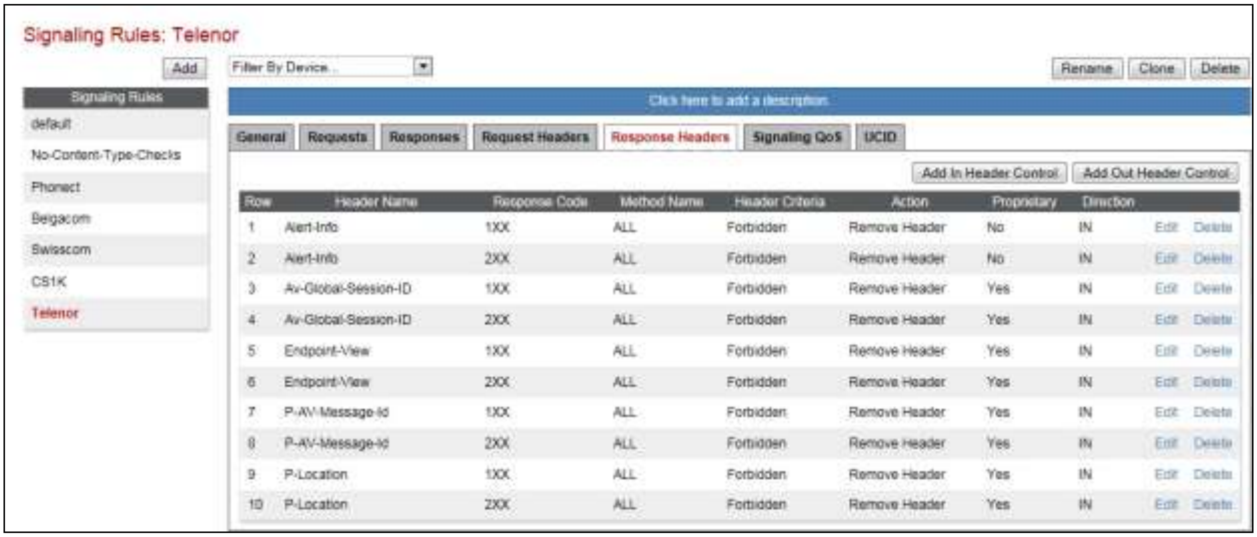


Header Control

Proprietary Response Header	☑
Header Name	Av-Global-Session-ID
Response Code	1XX
Method Name	ALL
Header Criteria	● Forbidden ○ Mandatory ○ Optional
Presence Action	Remove header 486 Busy Here

Note: The previous screenshot shows an example of an unnecessary header. During test, the same was done for Alert-Info, Av-Global-Session-ID, Endpoint-View, P-AV-Message-Id and P-Location headers.

When finished, all the Response Headers defined will be shown under the **Response Headers** tab as shown in the screenshot.

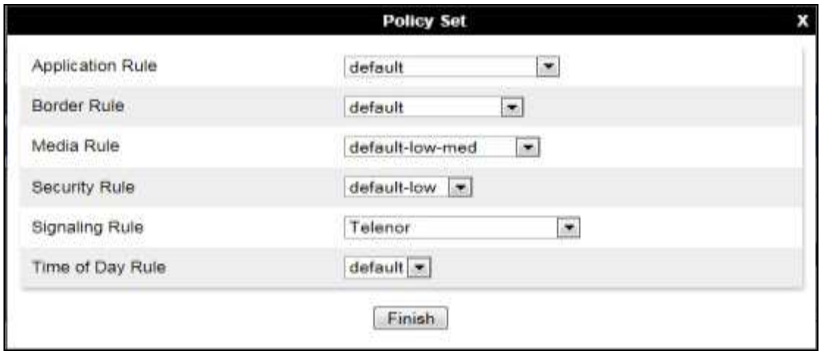


Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction	
1	Alert-Info	1XX	ALL	Forbidden	Remove Header	No	IN	Edit Delete
2	Alert-Info	2XX	ALL	Forbidden	Remove Header	No	IN	Edit Delete
3	Av-Global-Session-ID	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit Delete
4	Av-Global-Session-ID	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit Delete
5	Endpoint-View	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit Delete
6	Endpoint-View	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit Delete
7	P-AV-Message-Id	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit Delete
8	P-AV-Message-Id	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit Delete
9	P-Location	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit Delete
10	P-Location	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit Delete

End point policy groups are required to implement the signalling rules. To define one for the Session Manager, navigate to **Domain Policies → End Point Policy Groups** in the main menu on the left hand side. Click on **Add** and enter details in the Policy Group pop-up box (not shown).

- In the **Group Name** field enter a descriptive name for Telenor network, in this case **Telenor**, and click **Next** (not shown).
- Leave the **Application Rule**, **Border Rule**, **Media Rule**, **Security Rule** and **Time of Day Rule** fields at their default values.
- In the **Signaling Rule** drop down menu, select the recently added signalling rule for **Telenor**.

Click **Finish**.



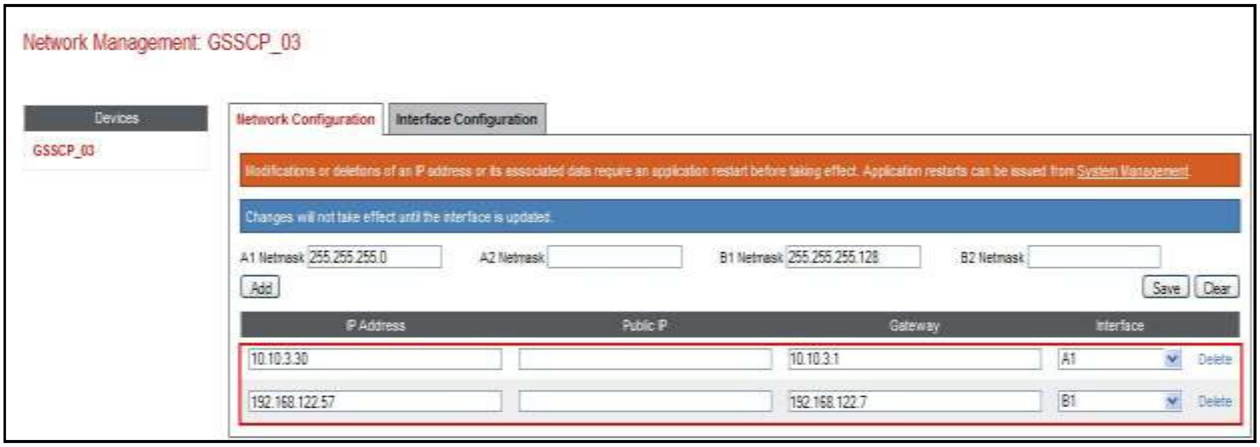
Application Rule	default
Border Rule	default
Media Rule	default-low-med
Security Rule	default-low
Signaling Rule	Telenor
Time of Day Rule	default

7.4. Define Network Information

Network information is required on the Avaya SBCE to allocate IP addresses and masks to the interfaces. Note that only the **A1** and **B1** interfaces are used, typically the **A1** interface is used for the internal side and **B1** is used for external. Each side of the Avaya SBCE can have only one interface assigned.

To define the network information, navigate to **Device Specific Settings → Network Management** in the menu on the left-hand side and click on **Add** (not shown). Enter details in the blank box that appears at the end of the list

- Click on **Add**.
- Define **A1 Netmask**, **IP Address** and **Gateway** and assign to **Interface A1**.
- Click **Save** to save the information.
- Click on **Add**.
- Define **B1 Netmask**, **IP Address** and **Gateway** and assign to **Interface B1**.
- Click **Save** to save the information.
- Click on **System Management** in the main menu (not shown).
- Select **Restart Application** indicated by an icon in the status bar (not shown).



Network Management: GSSCP_03

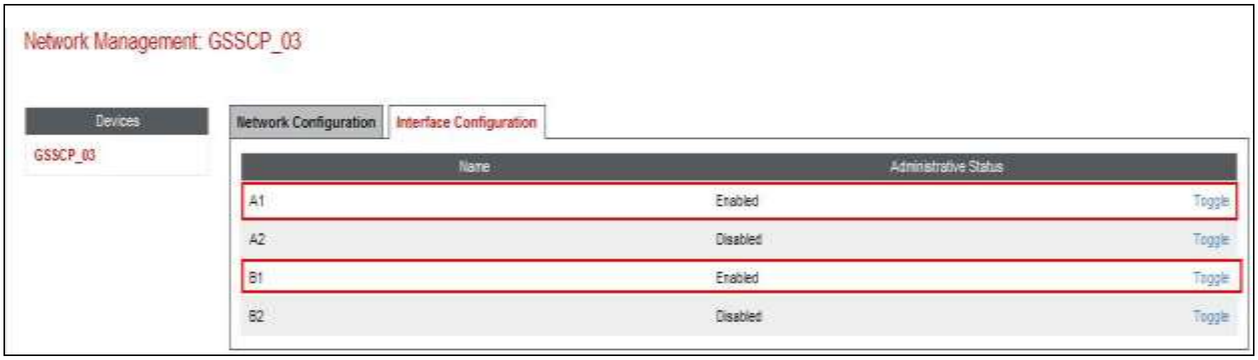
Modifications or deletions of an IP address or its associated data require an application restart before taking effect. Application restarts can be issued from System Management.

Changes will not take effect until the interface is updated.

A1 Netmask 255.255.255.0   A2 Netmask   B1 Netmask 255.255.255.128   B2 Netmask

IP Address	Public IP	Gateway	Interface	
10.10.3.30		10.10.3.1	A1	Delete
192.168.122.57		192.168.122.7	B1	Delete

Select the **Interface Configuration** tab and click on **Toggle State** to enable the interfaces.



Network Management: GSSCP_03

Name	Administrative Status	
A1	Enabled	Toggle
A2	Disabled	Toggle
B1	Enabled	Toggle
B2	Disabled	Toggle

7.5. Define Interfaces

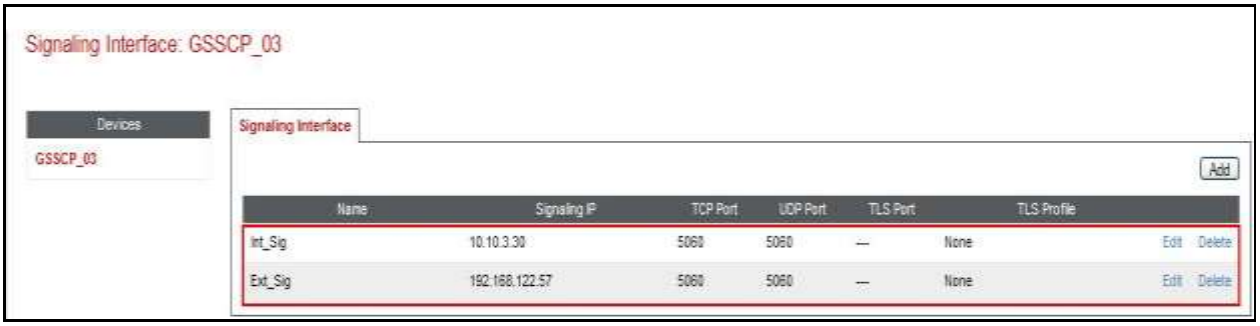
When the IP addresses and masks are assigned to the interfaces, these are then configured as signalling and media interfaces.

7.5.1. Signalling Interfaces

The Signalling Interface screen allows the IP Address and ports to be set for transporting signaling messages over the SIP trunk. The Avaya SBCE listens for SIP requests on the defined ports. Create a Signaling Interface for both the inside and outside IP interfaces. To create a new Signaling Interface, navigate to **Device Specific Settings → Signaling Interface** (not shown) and click **Add**.

- **Name**: **Int_Sig**.
- **Signaling IP**: **10.10.3.30** (Internal address for calls toward Session Manager).
- **TCP Port**: **5060**.
- **UDP Port**: **5060**.
- Click **Finish** (not shown).
- Select **Add**.
- **Name**: **Ext_Sig**.
- **Signaling IP: 192.168.122.57** (External address for calls toward Telenor).
- **UDP Port**: **5060**.
- Click **Finish** (not shown).

The following screen shows the signaling interfaces created in the sample configuration for the inside and outside IP interfaces.



Signaling Interface: GSSCP_03

Name	Signaling IP	TCP Port	UDP Port	TLS Port	TLS Profile	
Int_Sig	10.10.3.30	5060	5060	—	None	Edit Delete
Ext_Sig	192.168.122.57	5060	5060	—	None	Edit Delete

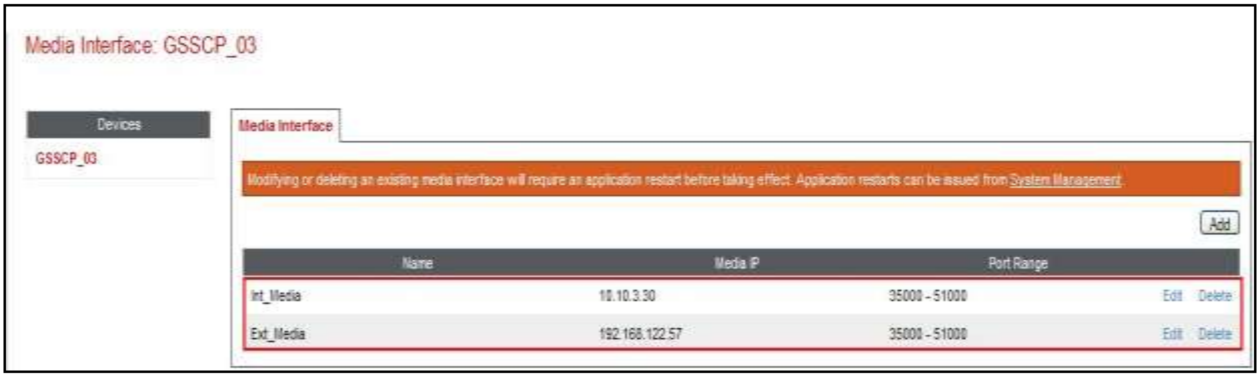
7.5.2. Media Interfaces

The Media Interface screen allows the IP address and ports to be set for transporting Media over the SIP trunk. The Avaya SBCE listens for SIP media on the defined ports.

To create a new Media Interface, navigate to **Device Specific Settings → Media Interface** (not shown).

- Select **Add**.
- **Name**: **Int_Media**.
- **Media IP**: **10.10.3.30** (Internal address for calls toward Session Manager).
- **Port Range**: **35000-51000**.
- Click **Finish** (not shown).
- Select **Add**.
- **Name**: **Ext_Media**.
- **Media IP**: **192.168.122.57** (External address for calls toward Telenor).
- **Port Range**: **35000-5100**.
- Click **Finish** (not shown).

The following screen shows the Media Interfaces created in the sample configuration for the inside and outside IP interfaces.



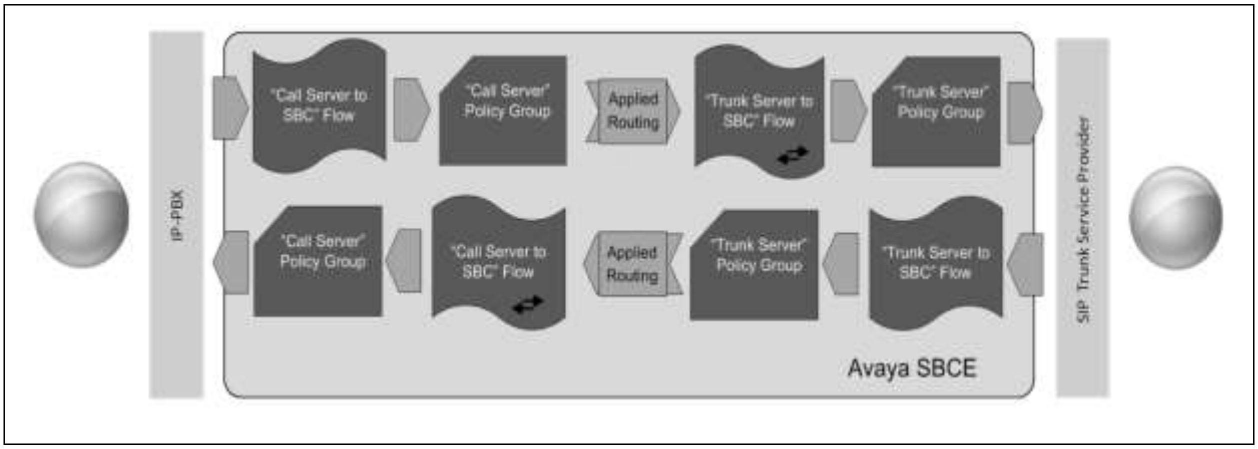
Media Interface: GSSCP_03

Modifying or deleting an existing media interface will require an application restart before taking effect. Application restarts can be issued from System Management.

Name	Media IP	Port Range		
Int_Media	10.10.3.30	35000 - 51000	Edit	Delete
Ext_Media	192.168.122.57	35000 - 51000	Edit	Delete

7.6. Server Flows

When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing is applied and the destination endpoint is determined, the policies for this destination endpoint are applied. The context is maintained, so as to be applied to future packets in the same flow. The following screen illustrates the flow through the Avaya SBCE to secure a SIP Trunk call.

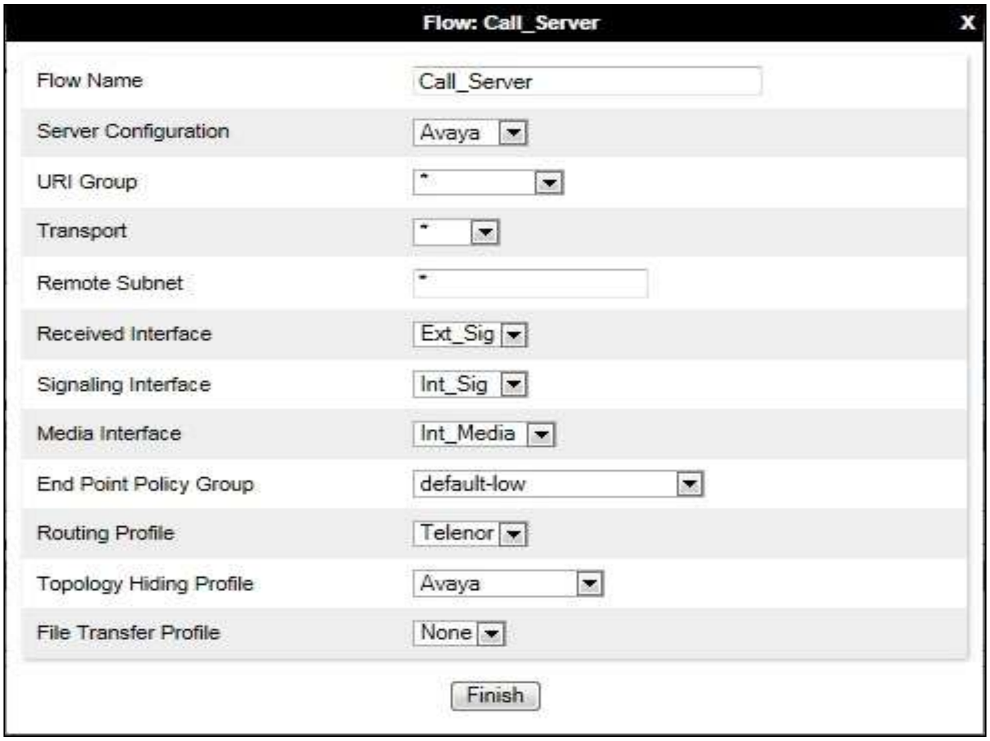

IP-PBX
"Call Server to SBC" Flow
"Call Server" Policy Group
Applied Routing
"Trunk Server to SBC" Flow
"Trunk Server" Policy Group
"Call Server" Policy Group
"Call Server to SBC" Flow
Applied Routing
"Trunk Server" Policy Group
"Trunk Server to SBC" Flow
Avaya SBCE
SIP Trunk Service Provider

To create a Server Flow, navigate to **Device Specific Settings → End Point Flows**. Select the **Server Flows** tab and click **Add Flow** (not shown).

- **Flow Name:** Enter a descriptive name.
- **Server Configuration:** Select a Server Configuration created in **Section 7.2.4** and **7.2.5** and assign to the Flow.
- **Received Interface:** Select the Signaling Interface the Server Configuration is allowed to receive SIP messages from.
- **Signaling Interface:** Select the Signaling Interface used to communicate with the Server Configuration.
- **Media Interface:** Select the Media Interface used to communicate with the Server Configuration.
- **End Point Policy Group:** Select the policy assigned to the Server Configuration.
- **Routing Profile:** Select the profile the Server Configuration will use to route SIP messages to.
- **Topology Hiding Profile:** Select the profile to apply toward the Server Configuration.

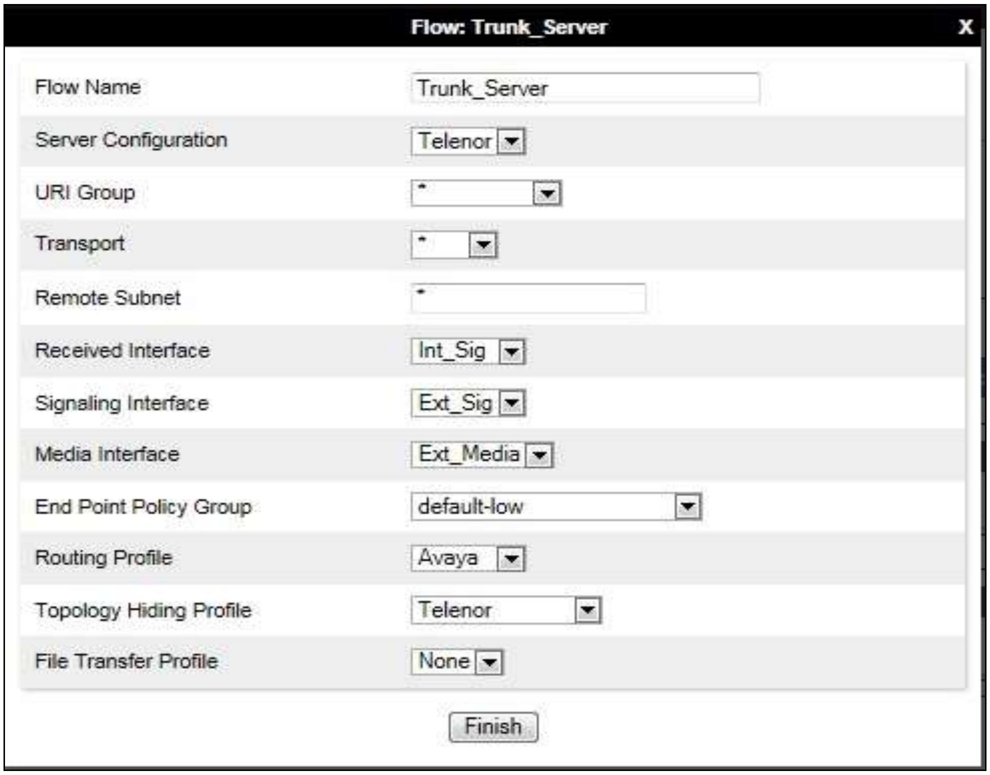
Click **Finish** to save and exit.

The following screen shows the Server Flow for Session Manager.



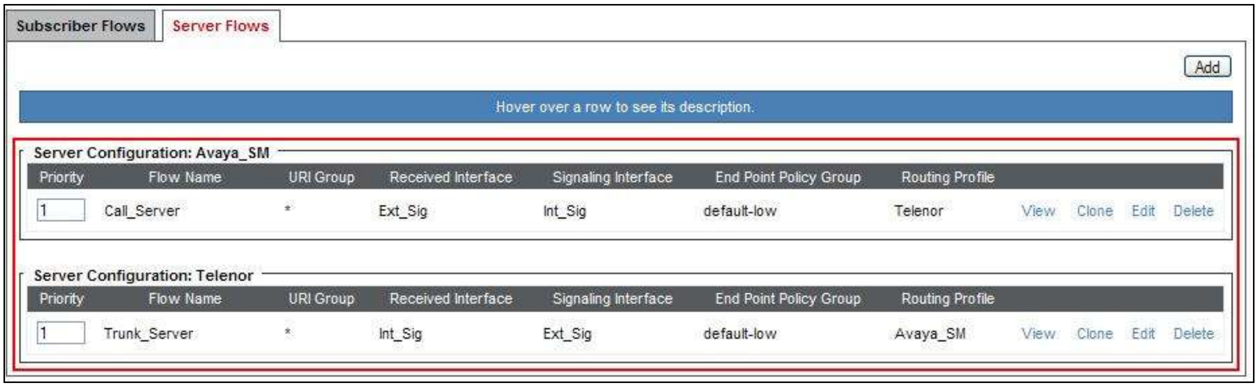
Flow Name	Call_Server
Server Configuration	Avaya
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Ext_Sig
Signaling Interface	Int_Sig
Media Interface	Int_Media
End Point Policy Group	default-low
Routing Profile	Telenor
Topology Hiding Profile	Avaya
File Transfer Profile	None

The following screen shows the Server Flow for Telenor.



Flow Name	Trunk_Server
Server Configuration	Telenor
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	Int_Sig
Signaling Interface	Ext_Sig
Media Interface	Ext_Media
End Point Policy Group	default-low
Routing Profile	Avaya
Topology Hiding Profile	Telenor
File Transfer Profile	None

This configuration ties all the previously entered information together so that calls can be routed from Session Manager to Telenor SIP Trunk service and vice versa. The following screenshot shows all configured flows.



Server Configuration: Avaya_SM

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	Call_Server	*	Ext_Sig	Int_Sig	default-low	Telenor	View	Clone	Edit	Delete

Server Configuration: Telenor

Priority	Flow Name	URI Group	Received Interface	Signaling Interface	End Point Policy Group	Routing Profile				
1	Trunk_Server	*	Int_Sig	Ext_Sig	default-low	Avaya_SM	View	Clone	Edit	Delete

8. Telenor Configuration

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

9. Verification Steps

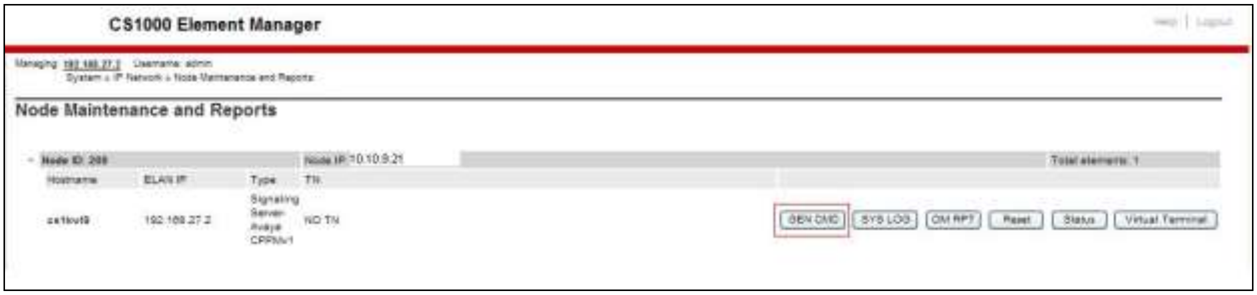
This section provides verification steps that may be performed in the field to verify that the solution is configured properly.

9.1. Avaya Communication Server 1000 Verification

This section illustrates sample verifications that may be performed using the Avaya CS1000 Element Manager GUI.

9.1.1. IP Network Maintenance and Reports Commands

From Element Manager, navigate to **System → IP Network → Node Maintenance and Reports** as shown below. In the resultant screen on the right, click the **GEN CMD** button.



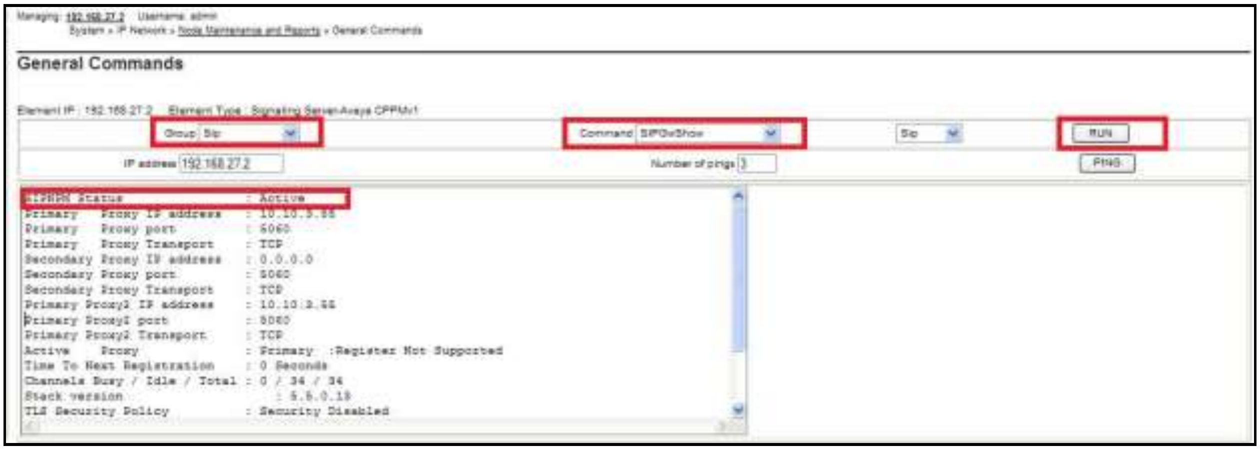
Managing: 192.168.27.2 Username: admin
System » IP Network » Node Maintenance and Reports

Node Maintenance and Reports

- Node ID: 200		Node IP: 10.10.9.21		Total elements: 1
Hostname	ELAN IP	Type	TN	
cs1kvt9	192.168.27.2	Signaling Server Avaya CPPMv1	NO TN	

The **General Commands** page is displayed. A variety of commands are available by selecting an appropriate **Group** and **Command** from the drop-down menus, and selecting **RUN**.

To check the status of the SIP Gateway to Session Manager in the sample configuration, select **Sip** from the **Group** menu and **SIPGwShow** from the **Command** menu. Click **RUN**. The example output below shows that Session Manager has **SIPNPM Status** "**Active**".



Managing: 192.168.27.2 Username: admin
System » IP Network » Node Maintenance and Reports » General Commands

General Commands

Element IP : 192.168.27.2 Element Type : Signaling Server-Avaya CPPMv1

Group: Sip

Command: SIPGwShow

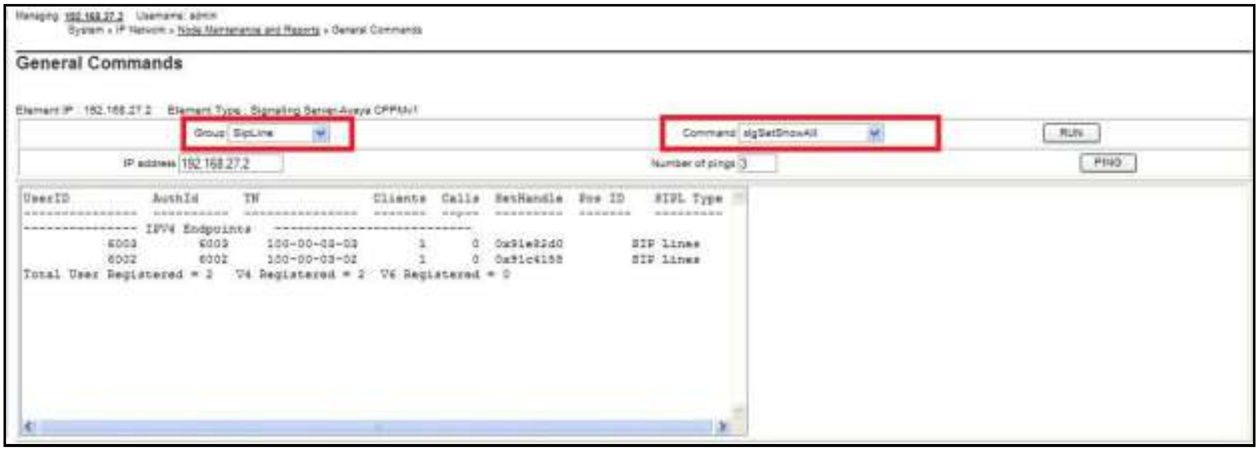
Sip

IP address: 192.168.27.2

Number of pings: 3

```
SIPNPM Status                 : Active
Primary   Proxy IP address    : 10.10.3.55
Primary   Proxy port          : 5060
Primary   Proxy Transport     : TCP
Secondary Proxy IP address    : 0.0.0.0
Secondary Proxy port          : 5060
Secondary Proxy Transport     : TCP
Primary Proxy2 IP address     : 10.10.3.55
Primary Proxy2 port           : 5060
Primary Proxy2 Transport      : TCP
Active    Proxy               : Primary  :Register Not Supported
Time To Next Registration     : 0 Seconds
Channels Busy / Idle / Total : 0 / 34 / 34
Stack version                     : 5.5.0.18
TLS Security Policy           : Security Disabled
```

The following screen shows a means to view registered SIP telephones. The screen shows the output of the **Command sigSetShowAll** in **Group SipLine**.



Managing: 192.168.27.2 Username: admin
System » IP Network » Node Maintenance and Reports » General Commands

General Commands

Element IP : 192.168.27.2 Element Type : Signaling Server-Avaya CPPMv1

Group: SipLine

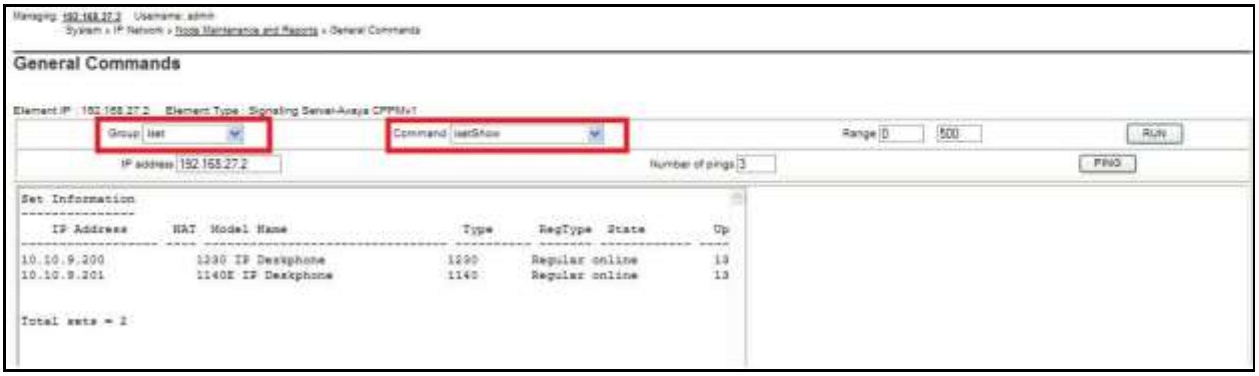
Command: sigSetShowAll

IP address: 192.168.27.2

Number of pings: 3

```
UserID           AuthId      TN                 Clients  Calls  SetHandle  Pos ID   SIPL Type
---------------- ----------  -----------------  -------  -----  ---------  -------  ---------
---------------- IPV4 Endpoints  ----------------------------
            6003        6003      100-00-03-03        1      0  0x91e82d0          SIP Lines
            6002        6002      100-00-03-02        1      0  0x91c4158          SIP Lines
Total User Registered = 2   V4 Registered = 2  V6 Registered = 0
```

The following screen shows a means to view IP UNIStim telephones. The screen shows the output of the **Command isetShow** in **Group Iset**.



Managing: 192.168.27.2 Username: admin
System » IP Network » Node Maintenance and Reports » General Commands

General Commands

Element IP : 192.168.27.2 Element Type : Signaling Server-Avaya CPPMv1

Group: Iset

Command: isetShow

Range: 0 500

IP address: 192.168.27.2

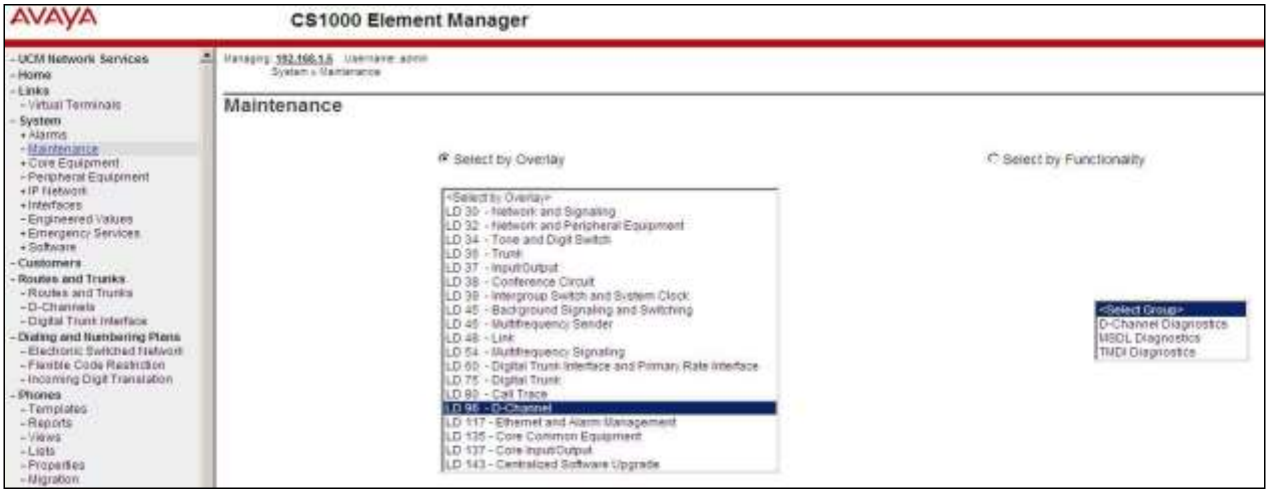
Number of pings: 3

```
Set Information
---------------
    IP Address      NAT  Model Name                       Type       RegType  State        Up
--------------- ---- ------------------------------- ---------- ------- ----------- ----
10.10.9.200          1230 IP Deskphone                    1230       Regular online       13
10.10.9.201          1140E IP Deskphone                   1140       Regular online       13


Total sets = 2
```

9.2. Verify Avaya Communication Server 1000 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 by Functionality** table as shown below.



CS1000 Element Manager

Managing: 192.168.1.5 Username: admin
System » Maintenance

Maintenance

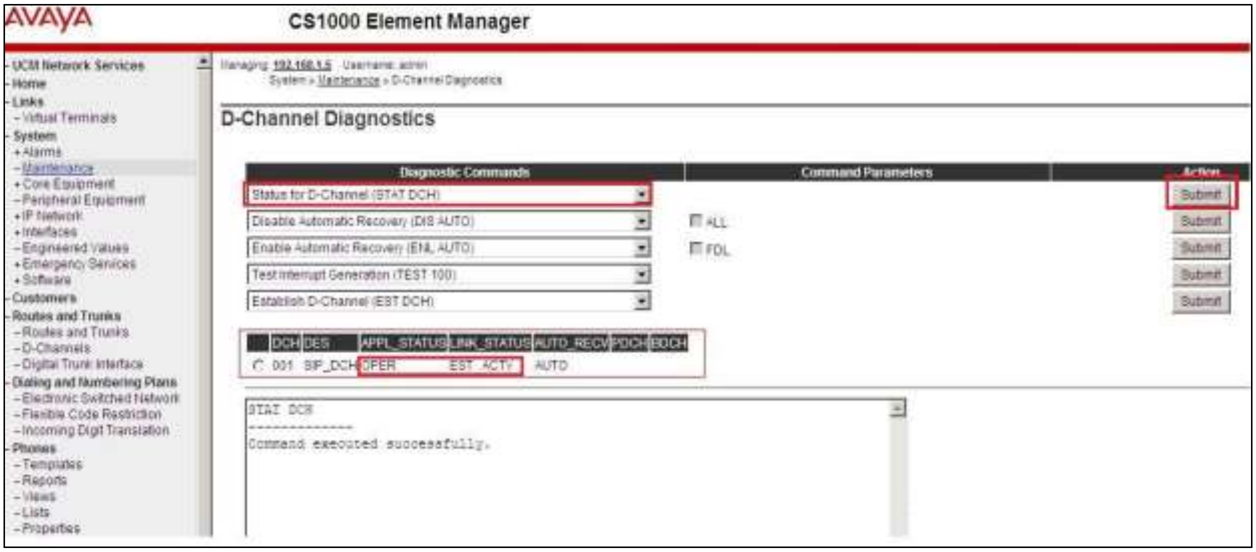
● Select by Overlay: LD 96 - D-Channel

○ Select by Functionality

AVAYA
- UCM Network Services
- Home
- Links
- Virtual Terminals
- System
+ Alarms
- Maintenance
+ Core Equipment
- Peripheral Equipment
+ IP Network
+ Interfaces
- Engineered Values
+ Emergency Services
+ Software
- Customers
- Routes and Trunks
- Routes and Trunks
- D-Channels
- Digital Trunk Interface
- Dialing and Numbering Plans
- Electronic Switched Network
- Flexible Code Restriction
- Incoming Digit Translation
- Phones
- Templates
- Reports
- Views
- Lists
- Properties
- Migration
<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
<Select Group>
D-Channel Diagnostics
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**.



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

D-Channel Diagnostics

Diagnostic Commands	Command Parameters
Status for D-Channel (STAT DCH)	
Disable Automatic Recovery (DIS AUTO)	□ ALL
Enable Automatic Recovery (ENL AUTO)	□ FDL
Test Interrupt Generation (TEST 100)	
Establish D-Channel (EST DCH)	

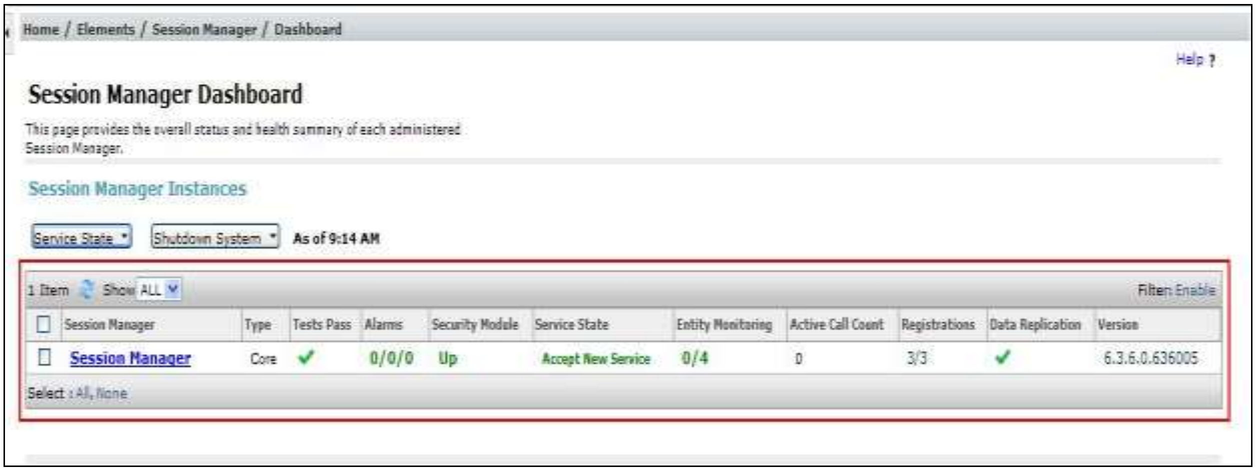
	DCH	DES	APPL_STATUS	LINK_STATUS	AUTO_RECV	PDCH	BDCH
○	001	SIP_DCH	OPER	EST ACTV	AUTO		

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

9.3. Verify Avaya Aura® Session Manager Operational Status

9.3.1. Verify Avaya Aura® Session Manager is Operational

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



Home / Elements / Session Manager / Dashboard

Session Manager Dashboard

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

Session Manager Instances

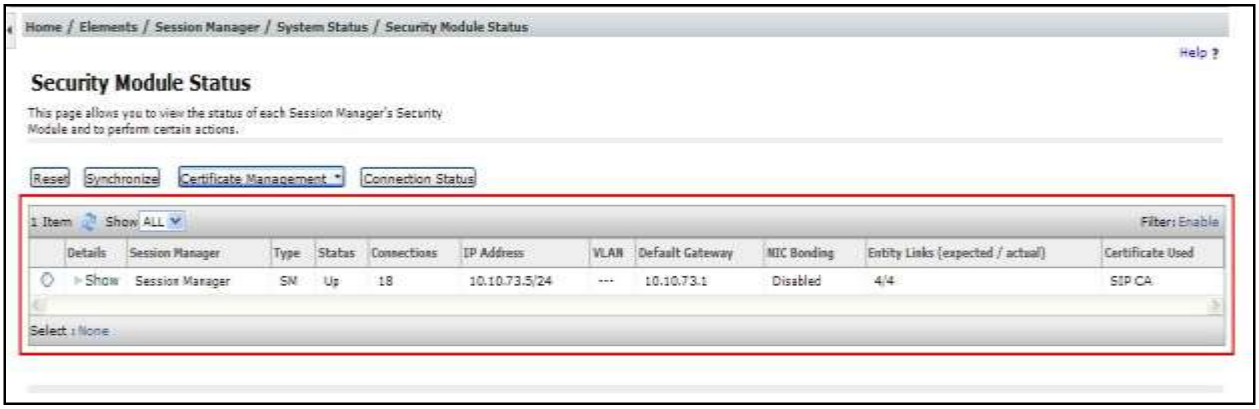
As of 9:14 AM

1 Item Show ALL Filter: Enable

□	Session Manager	Type	Tests Pass	Alarms	Security Module	Service State	Entity Monitoring	Active Call Count	Registrations	Data Replication	Version
□	Session Manager	Core	✓	0/0/0	Up	Accept New Service	0/4	0	3/3	✓	6.3.6.0.636005

Select : All, None

Navigate to **Elements → Session Manager → System Status → Security Module Status** 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.



Home / Elements / Session Manager / System Status / Security Module Status

Security Module Status

This page allows you to view the status of each Session Manager's Security Module and to perform certain actions.

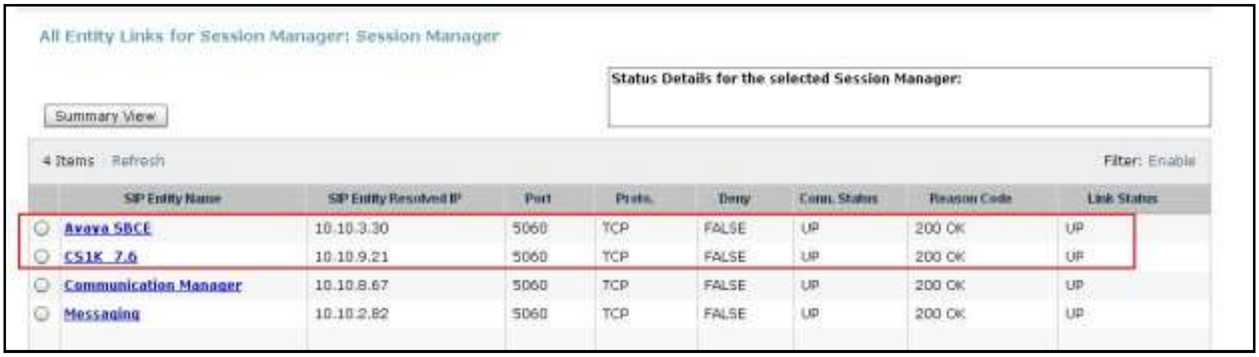
1 Item Show ALL Filter: Enable

	Details	Session Manager	Type	Status	Connections	IP Address	VLAN	Default Gateway	NIC Bonding	Entity Links (expected / actual)	Certificate Used
○	▸Show	Session Manager	SM	Up	18	10.10.73.5/24	---	10.10.73.1	Disabled	4/4	SIP CA

Select : None

9.3.2. Verify SIP Entity Link Status

Navigate to **Elements → Session Manager → System Status → SIP Entity Monitoring** (not shown) to view more detailed status information for one of the SIP Entity Links. Select the SIP Entity for CS1000 from the **All Monitored SIP Entities** table (not shown) to open the **SIP Entity, Entity Link Connection Status** page.

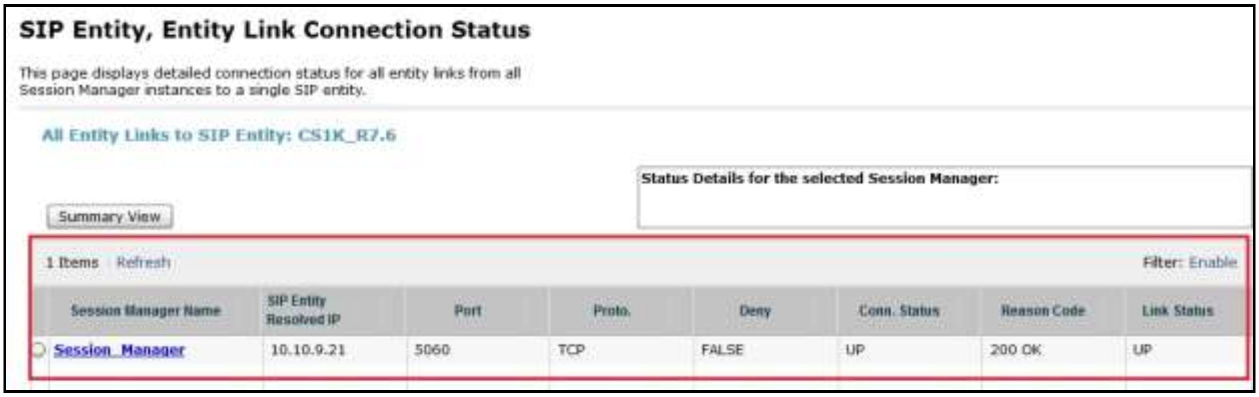


All Entity Links for Session Manager: Session Manager

Status Details for the selected Session Manager:

	SIP Entity Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
○	Avaya SBCE	10.10.3.30	5060	TCP	FALSE	UP	200 OK	UP
○	CS1K_7.6	10.10.9.21	5060	TCP	FALSE	UP	200 OK	UP
○	Communication Manager	10.10.8.67	5060	TCP	FALSE	UP	200 OK	UP
○	Messaging	10.10.2.82	5060	TCP	FALSE	UP	200 OK	UP

In the **All Entity Links to SIP Entity: CS1K** 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_R7.6

Status Details for the selected Session Manager:

	Session Manager Name	SIP Entity Resolved IP	Port	Proto.	Deny	Conn. Status	Reason Code	Link Status
○	Session_Manager	10.10.9.21	5060	TCP	FALSE	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 Entities:** table.

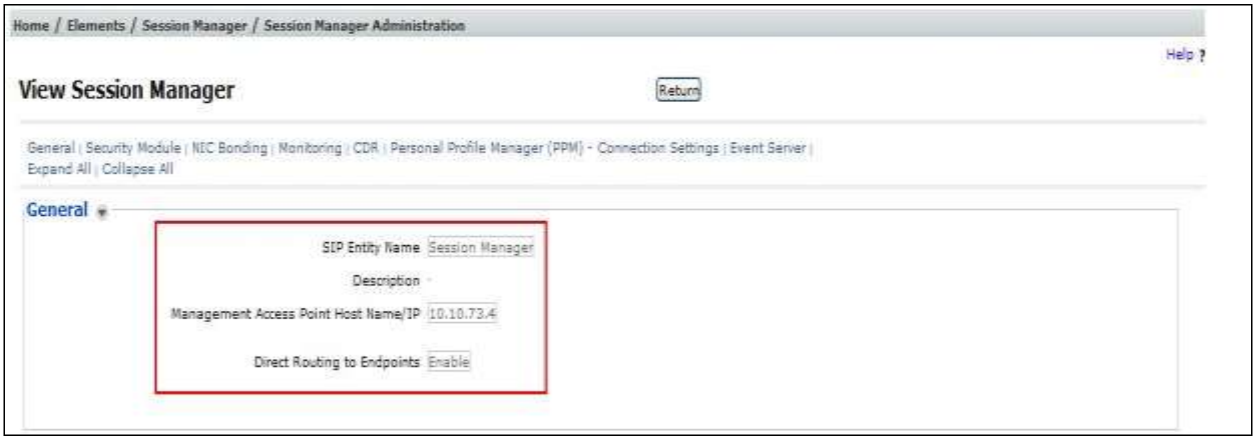
9.3.3. Verify Avaya Aura® Session Manager Instance

The creation of a Session Manager Instance provides the linkage between System Manager and Session Manager. This was most likely done as part of the initial Session Manager installation. To add a Session Manager, navigate to **Elements → Session Manager → Session Manager Administration** in the left-hand navigation pane and click on the **new** button in the right pane (not shown). If the Session Manager instance already exists, click **View** (not shown) to view the configuration. Enter/verify the data as described below and shown in the following screen:

In the **General** section, enter the following values:

• **SIP Entity Name:**	Select the SIP Entity created for Session Manager.
• **Description**:	Add a brief description (optional).
• **Management Access Point Host Name/IP:**	Enter the IP address of the Session Manager management interface.

The following screen shows the Session Manager values used for the compliance test.

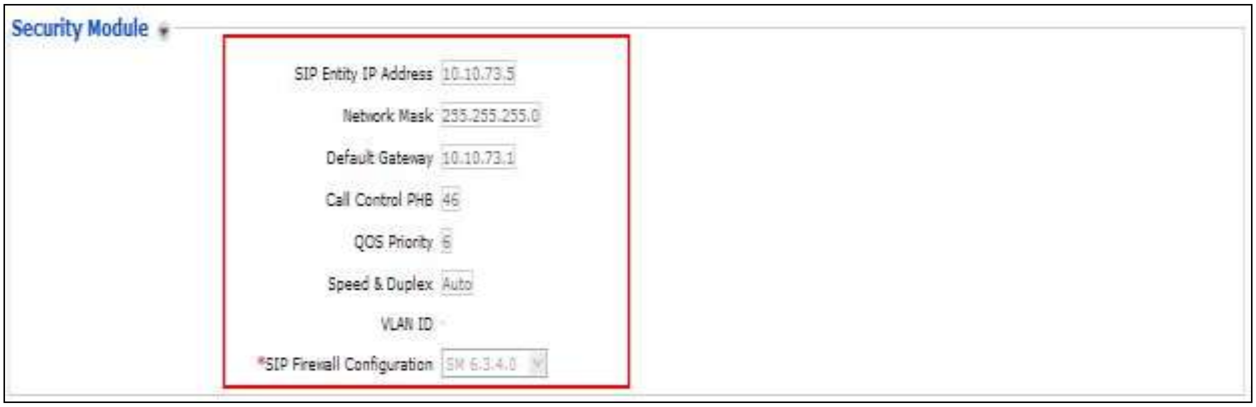

Home / Elements / Session Manager / Session Manager Administration
Help ?
View Session Manager
Return
General | Security Module | NIC Bonding | Monitoring | CDR | Personal Profile Manager (PPM) - Connection Settings | Event Server |
Expand All | Collapse All
General

SIP Entity Name: Session Manager
Description:
Management Access Point Host Name/IP: 10.10.73.4
Direct Routing to Endpoints: Enable

In the **Security Module** section, enter the following values:

- **SIP Entity IP Address:** Should be filled in automatically based on the SIP Entity Name. Otherwise, enter IP address of Session Manager signaling interface.
- **Network Mask:** Enter the network mask corresponding to the IP address of Session Manager.
- **Default Gateway**: Enter the IP address of the default gateway for Session Manager.

Use default values for the remaining fields. Click **Save** (not shown) to add this Session Manager. The following screen shows the remaining Session Manager values used for the compliance test.



Security Module

SIP Entity IP Address	10.10.73.5
Network Mask	255.255.255.0
Default Gateway	10.10.73.1
Call Control PHB	46
QOS Priority	6
Speed & Duplex	Auto
VLAN ID	
*SIP Firewall Configuration	SM 6.3.4.0

10. Conclusion

These Application Notes describe the configuration necessary to connect Avaya Aura® Communication Server R7.6, Avaya Aura® Session Manager R6.3 and Avaya Session Border Controller for Enterprise R6.2 to Telenor SIP Trunk service. Telenor's SIP Trunk service is a SIP-based Voice over IP solution providing businesses a flexible, cost-saving alternative to traditional hardwired telephony trunks. The service was successfully tested with a number of observations listed in **Section 2.2**.

11. References

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

[1] *Implementing Avaya Aura® Session Manager*, Release 6.3

[2] *Installing Service Packs for Avaya Aura® Session Manager*, Release 6.3

[3] *Upgrading Avaya Aura® Session Manager*, Release 6.3

[4] *Maintaining and Troubleshooting Avaya Aura® Session Manager Release 6.3*

[5] *Installing and Configuring Avaya Aura® System Platform Release 6.3*

[6] *Implementing Avaya Aura® System Manager Release 6.3*

[7] *Upgrading Avaya Aura® System Manager to 6.3*

[8] *Avaya Communication Server 1000 Installation and Commissioning*, Document Number NN43041-310.

[9] *Feature Listing Reference Avaya Communication Server 1000*, Document Number NN43001-111, 05.01.

[10] *Linux Platform Base and Applications Installation and Commissioning Avaya Communication Server 1000*, Document Number NN43001-315

[11] *Unified Communications Management Common Servers Fundamentals Avaya Communication Server 1000*, Document Number NN43001-116

[12] *Software Input Output Reference – Maintenance Avaya Communication Server 1000*, Document Number NN43001-711

[13] *Signaling Server IP Line Applications Fundamentals Avaya Communication Server 1000*, Document Number NN43001-125

[14] *SIP Software for Avaya 1100 Series IP Deskphones-Administration*, Document Number NN43170-600

[15] *Installing Avaya Session Border Controller for Enterprise*, Release 6.2

[16] *Upgrading Avaya Session Border Controller for Enterprise* Release 6.2

[17] *Administering Avaya Session Border Controller for Enterprise* Release 6.2

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

Appendix A – Communication Server 1000 Software

Communication Server 1000 call server patches and plug ins

```
TID: 46379

VERSION 4121

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

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

RELEASE 7
ISSUE 65 P  +
IDLE_SET_DISPLAY NORTEL
DepList 1: core Issue: 01(created: 2013-05-28 04:19:50 (est))

MDP>LAST SUCCESSFUL MDP REFRESH :2013-09-12 14:50:17(Local Time)
MDP>USING DEPLIST ZIP FILE DOWNLOADED :2013-05-28 04:30:29(est)
SYSTEM HAS NO USER SELECTED PEPS IN-SERVICE


LOADWARE VERSION: PSWV 100+

INSTALLED LOADWARE PEPS : 1
PAT#  CR #          PATCH REF #     NAME            DATE        FILENAME
00    wi01057886    ISS1:1OF1       DSP2AB07        13/09/2013  DSP2AB07.LW


ENABLED PLUGINS : 2

PLUGIN    STATUS      PRS/CR_NUM    MPLR_NUM      DESCRIPTION
-------------------------------------------------------------
201       ENABLED     Q00424053     MPLR08139     PI:Cant XFER OUTG TRK TO OUTG TRK
501       ENABLED     Q02138637     MPLR30070     Enables blind transfer to a SIP endpoint even
if SIP UPDATE is not supported by the far end
```

Communication Server 1000 call server deplists

```
VERSION 4121
RELEASE 7
ISSUE 65 P +
DepList 1: core Issue: 01 (created: 2013-05-28 04:19:50 (est))

IN-SERVICE PEPS
PAT# CR #           PATCH REF #     NAME      DATE        FILENAME       SPECINS
000  wi01058359     ISS1:1OF1       p32331_1  24/04/2014  p32331_1.cpl   NO
001  wi01064599     iss1:1of1       p32580_1  24/04/2014  p32580_1.cpl   NO
002  wi01056067     ISS1:1OF1       p32457_1  24/04/2014  p32457_1.cpl   NO
003  wi01063263     ISS1:1OF1       p32573_1  24/04/2014  p32573_1.cpl   NO
004  wi01065842     ISS1:1OF1       p32478_1  24/04/2014  p32478_1.cpl   NO
005  wi01062607     ISS1:1OF1       p32503_1  24/04/2014  p32503_1.cpl   NO
006  wi01070756     ISS1:1OF1       p32444_1  24/04/2014  p32444_1.cpl   NO
007  wi01039280     ISS1:1OF1       p32423_1  24/04/2014  p32423_1.cpl   NO
008  wi01087543     ISS1:1OF1       p32662_1  24/04/2014  p32662_1.cpl   NO
009  wi00933195     ISS1:1OF1       p32491_1  24/04/2014  p32491_1.cpl   NO
010  wi01071379     ISS1:1OF1       p32522_1  24/04/2014  p32522_1.cpl   NO
011  wi01068669     ISS1:1OF1       p32333_1  24/04/2014  p32333_1.cpl   NO
012  wi01066991     ISS1:1OF1       p32449_1  24/04/2014  p32449_1.cpl   NO
013  wi01070474     iss1:1of1       p32407_1  24/04/2014  p32407_1.cpl   NO
014  WI0110261      ISS1:1OF1       p32758_1  24/04/2014  p32758_1.cpl   NO
015  wi01094305     ISS1:1OF1       p32640_1  24/04/2014  p32640_1.cpl   NO
```

```
016  wi01047890      ISS1:1OF1       p32697_1  24/04/2014  p32697_1.cpl   NO
017  wi01055300      ISS1:1OF1       p32543_1  24/04/2014  p32543_1.cpl   NO
018  wi01082456      ISS1:1OF1       p32596_1  24/04/2014  p32596_1.cpl   NO
019  wi01058621      ISS1:1OF1       p32339_1  24/04/2014  p32339_1.cpl   NO
020  wi01061484      ISS1:1OF1       p32576_1  24/04/2014  p32576_1.cpl   NO
021  wi01078723      ISS1:1OF1       p32532_1  24/04/2014  p32532_1.cpl   NO
022  wi01048457      ISS1:1OF1       p32581_1  24/04/2014  p32581_1.cpl   NO
023  wi01075355      ISS1:1OF1       p32594_1  24/04/2014  p32594_1.cpl   NO
024  wi01053597      ISS1:1OF1       p32304_1  24/04/2014  p32304_1.cpl   NO
025  wi01045058      ISS1:1OF1       p32214_1  24/04/2014  p32214_1.cpl   NO
026  wi01075359      ISS1:1OF1       p32671_1  24/04/2014  p32671_1.cpl   NO
027  wi01025156      ISS1:1OF1       p32136_1  24/04/2014  p32136_1.cpl   NO
028  wi01061481      ISS1:1OF1       p32382_1  24/04/2014  p32382_1.cpl   NO
029  wi01035976      ISS1:1OF1       p32173_1  24/04/2014  p32173_1.cpl   NO
030  wi01088775      ISS1:1OF1       p32659_1  24/04/2014  p32659_1.cpl   NO
031  wi01070465      iss1:1of1       p32562_1  24/04/2014  p32562_1.cpl   NO
032  wi01088585      ISS1:1OF1       p32656_1  24/04/2014  p32656_1.cpl   NO
033  wi01063864      ISS1:1OF1       p32410_1  24/04/2014  p32410_1.cpl   YES
034  wi01034961      ISS1:1OF1       p32144_1  24/04/2014  p32144_1.cpl   NO
035  wi01055480      ISS1:1OF1       p32712_1  24/04/2014  p32712_1.cpl   NO
036  wi01034307      ISS1:1OF1       p32615_1  24/04/2014  p32615_1.cpl   NO
037  wi01065118      ISS1:1OF1       p32397_1  24/04/2014  p32397_1.cpl   NO
038  wi01075360      iss1:1of1       p32602_1  24/04/2014  p32602_1.cpl   NO
039  wi00884716      ISS1:1OF1       p32517_1  24/04/2014  p32517_1.cpl   NO
040  wi01068851      ISS1:1OF1       p32439_1  24/04/2014  p32439_1.cpl   NO
041  wi01053314      ISS1:1OF1       p32555_1  24/04/2014  p32555_1.cpl   NO
042  wi01059388      iss1:1of1       p32628_1  24/04/2014  p32628_1.cpl   NO
043  wi01087528      ISS1:1OF1       p32700_1  24/04/2014  p32700_1.cpl   NO
044  wi01072027      ISS1:1OF1       p32689_1  24/04/2014  p32689_1.cpl   NO
045  wi01052428      ISS1:1OF1       p32606_1  24/04/2014  p32606_1.cpl   NO
046  wi01053920      ISS1:1OF1       p32303_1  24/04/2014  p32303_1.cpl   NO
047  wi01070468      iss1:1of1       p32418_1  24/04/2014  p32418_1.cpl   NO
048  wi01067822      ISS1:1OF1       p32466_1  24/04/2014  p32466_1.cpl   YES
049  wi01060826      ISS1:1OF1       p32379_1  24/04/2014  p32379_1.cpl   NO
050  wi01075352      ISS1:1OF1       p32603_1  24/04/2014  p32603_1.cpl   NO
051  wi01043367      ISS1:1OF1       p32232_1  24/04/2014  p32232_1.cpl   NO
052  wi01083584      ISS1:1OF1       p32619_1  24/04/2014  p32619_1.cpl   NO
053  wi01060241      ISS1:1OF1       p32381_1  24/04/2014  p32381_1.cpl   NO
054  wi01053195      ISS1:1OF1       p32297_1  24/04/2014  p32297_1.cpl   NO
055  wi00897254      ISS1:1OF1       p31127_1  24/04/2014  p31127_1.cpl   NO
056  wi01061483      ISS1:1OF1       p32359_1  24/04/2014  p32359_1.cpl   NO
057  wi01085855      ISS1:1OF1       p32658_1  24/04/2014  p32658_1.cpl   NO
058  wi01075353      ISS1:1OF1       p32613_1  24/04/2014  p32613_1.cpl   NO
059  wi01070471      ISS1:1OF1       p32415_1  24/04/2014  p32415_1.cpl   NO
060  wi01074003      ISS1:1OF1       p32421_1  24/04/2014  p32421_1.cpl   NO
061  wi01060382      iss1:1of1       p32623_1  24/04/2014  p32623_1.cpl   YES
062  wi01068042      ISS1:1OF1       p32669_1  24/04/2014  p32669_1.cpl   NO
063  wi01072023      ISS1:1OF1       p32130_1  24/04/2014  p32130_1.cpl   YES
064  wi01065922      ISS1:1OF1       p32516_1  24/04/2014  p32516_1.cpl   NO
065  wi01057403      ISS1:1OF1       p32591_1  24/04/2014  p32591_1.cpl   NO
066  wi01069441      ISS1:1OF1       p32097_1  24/04/2014  p32097_1.cpl   NO
067  wi01070473      ISS1:1OF1       p32413_1  24/04/2014  p32413_1.cpl   NO
068  wi01056633      ISS1:1OF1       p32322_1  24/04/2014  p32322_1.cpl   NO
069  wi01052968      ISS1:1OF1       p32540_1  24/04/2014  p32540_1.cpl   NO
070  wi01072032      ISS1:1OF1       p32448_1  24/04/2014  p32448_1.cpl   NO
071  wi01073100      ISS1:1OF1       p32599_1  24/04/2014  p32599_1.cpl   NO
072  wi01035980      ISS1:1OF1       p32558_1  24/04/2014  p32558_1.cpl   NO
073  wi01041453      ISS1:1OF1       p32587_1  24/04/2014  p32587_1.cpl   NO
074  wi01032756      ISS1:1OF1       p32673_1  24/04/2014  p32673_1.cpl   NO
075  wi01092300      ISS1:1OF1       p32692_1  24/04/2014  p32692_1.cpl   NO
076  wi00996734      ISS1:1OF1       p32550_1  24/04/2014  p32550_1.cpl   NO
077  wi01022599      ISS1:1OF1       p32080_1  24/04/2014  p32080_1.cpl   NO
078  wi01060341      ISS1:1OF1       p32578_1  24/04/2014  p32578_1.cpl   NO
079  wi01091447      ISS1:1OF1       p32675_1  24/04/2014  p32675_1.cpl   NO
080  wi01070580      ISS1:1OF1       p32380_1  24/04/2014  p32380_1.cpl   NO
081  wi01089519      ISS1:1OF1       p32665_1  24/04/2014  p32665_1.cpl   NO
082  WI01077073      ISS1:1OF1       p32534_1  24/04/2014  p32534_1.cpl   NO
083  wi01080753      ISS1:1OF1       p32518_1  24/04/2014  p32518_1.cpl   NO
084  wi01065125      ISS1:1OF1       p32416_1  24/04/2014  p32416_1.cpl   NO
```

Communication Server 1000 signaling server service updates

```
Product Release: 7.65.16.00

In System service updates: 34
PATCH#  IN_SERVICE   DATE       SPECINS   REMOVABLE   NAME
0       Yes          02/04/14   YES       YES         cs1000-dmWeb-7.65.16.22-1.i386.000
2       Yes          02/04/14   YES       yes         tzdata-2013c-2.el5.i386.001
3       Yes          31/03/14   NO        YES         cs1000-linuxbase-7.65.16.22-02.i386.000
6       Yes          27/09/13   NO        yes         cs1000-cs1000WebService_6-0-7.65.16.21-
00.i386.000
7       Yes          31/03/14   NO        YES         cs1000-Jboss-Quantum-7.65.16.22-3.i386.000
8       Yes          27/09/13   NO        YES         cs1000-pd-7.65.16.21-00.i386.000
9       Yes          27/09/13   NO        YES         cs1000-shared-carrdtct-7.65.16.21-
01.i386.000
10      Yes          27/09/13   NO        YES         cs1000-shared-tpselect-7.65.16.21-
01.i386.000
12      Yes          27/09/13   NO        yes         cs1000-dbcom-7.65.16.21-00.i386.000
13      Yes          31/03/14   YES       YES         cs1000-patchWeb-7.65.16.22-1.i386.000
14      Yes          27/09/13   NO        YES         cs1000-shared-xmsg-7.65.16.21-00.i386.000
15      Yes          02/04/14   YES       YES         cs1000-cs-7.65.P.100-02.i386.000
16      Yes          02/04/14   YES       YES         cs1000-tps-7.65.16.21-11.i386.000
17      Yes          27/09/13   NO        YES         cs1000-mscAnnc-7.65.16.21-02.i386.001
18      Yes          27/09/13   NO        YES         cs1000-mscAttn-7.65.16.21-04.i386.001
19      Yes          27/09/13   NO        YES         cs1000-mscConf-7.65.16.21-02.i386.001
20      Yes          27/09/13   NO        YES         cs1000-mscMusc-7.65.16.21-02.i386.001
21      Yes          27/09/13   NO        YES         cs1000-mscTone-7.65.16.21-03.i386.001
22      Yes          02/04/14   NO        YES         cs1000-sps-7.65.16.21-8.i386.000
23      Yes          02/04/14   NO        YES         cs1000-shared-omm-7.65.16.21-2.i386.000
24      Yes          02/04/14   YES       YES         cs1000-baseWeb-7.65.16.22-1.i386.000
26      Yes          02/04/14   YES       YES         cs1000-csmWeb-7.65.16.22-1.i386.000
28      Yes          02/10/13   NO        YES         cs1000-gk-7.65.16.21-01.i386.000
29      Yes          02/04/14   YES       YES         cs1000-csoneksvrmgr-7.65.16.22-1.i386.000
30      Yes          02/10/13   NO        YES         cs1000-snmp-7.65.16.21-00.i686.000
38      Yes          02/04/14   YES       YES         cs1000-emWebLocal_6-0-7.65.16.22-1.i386.000
39      Yes          02/04/14   YES       YES         cs1000-ftrpkg-7.65.16.22-1.i386.000
40      Yes          02/04/14   YES       YES         cs1000-ipsec-7.65.16.22-1.i386.000
41      Yes          02/04/14   YES       YES         cs1000-vtrk-7.65.16.23-58.i386.000
42      Yes          02/04/14   NO        YES         cs1000-cppmUtil-7.65.16.22-1.i686.000
43      Yes          02/04/14   YES       YES         cs1000-oam-logging-7.65.16.22-3.i386.000
44      Yes          02/04/14   YES       YES         cs1000-bcc-7.65.16.22-6.i386.000
45      Yes          02/04/14   YES       YES         cs1000-nrsm-7.65.16.22-2.i386.000
46      Yes          02/04/14   YES       YES         cs1000-emWeb_6-0-7.65.16.22-5.i386.000
```

Communication Server 1000 system software

```
Product Release: 7.65.16.00
Base Applications
   base                        7.65.16     [patched]
   NTAFS                       7.65.16
   sm                          7.65.16
   cs1000-Auth                 7.65.16
   Jboss-Quantum               n/a         [patched]
   cnd                         7.65.16
   lhmonitor                   7.65.16
   baseAppUtils                7.65.16
   dfoTools                    7.65.16
   cppmUtil                    n/a         [patched]
   oam-logging                 n/a         [patched]
   dmWeb                       n/a         [patched]
   baseWeb                     n/a         [patched]
   ipsec                       n/a         [patched]
   Snmp-Daemon-TrapLib         n/a         [patched]
   ISECSH                      7.65.16
   patchWeb                    n/a         [patched]
   EmCentralLogic               7.65.16
Application configuration: CS+SS+NRS+EM
Packages:
CS+SS+NRS+EM
Configuration version:     7.65.16-00
   cs                           7.65.16     [patched]
   dbcom                        7.65.16.21  [patched]
   cslogin                      7.65.16
   sigServerShare               7.65.16     [patched]
   csv                          7.65.16
   tps                          7.65.16.21  [patched]
   vtrk                         7.65.16.22  [patched]
   pd                           7.65.16.21  [patched]
   sps                          7.65.16.21  [patched]
   ncs                          7.65.16
   gk                           7.65.16.21  [patched]
   nrsm                         7.65.16     [patched]
   nrsmWebService               7.65.16
   managedElementWebService     7.65.16
   EmConfig                     7.65.16
   emWeb_6-0                    7.65.16     [patched]
   emWebLocal_6-0               7.65.16     [patched]
   csmWeb                       7.65.16     [patched]
   bcc                          7.65.16     [patched]
   ftrpkg                       7.65.16     [patched]
   cs1000WebService_6-0         7.65.16     [patched]
   mscAnnc                      7.65.16.21  [patched]
   mscAttn                      7.65.16.21  [patched]
   mscConf                      7.65.16.21  [patched]
   mscMusc                      7.65.16.21  [patched]
   mscTone                      7.65.16.21  [patched
```

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.