Avaya Solution & Interoperability Test Lab

Application Notes for Telstra Enterprise SIP Trunking Service with Avaya Communication Server 1000 Release 7.6, Avaya Aura® Session Manager Release 6.3.15 and Avaya Session Border Controller for Enterprise Release 6.3.6 - Issue 1.0

Abstract

These Application Notes illustrate a sample configuration of Avaya Communication Server 1000 Release 7.6 and Avaya Aura® Session Manager Release 6.3.15 with SIP Trunks to Avaya Session Border Controller for Enterprise (Avaya SBCE) Release 6.3.6 when used to connect Telstra Enterprise SIP Trunking service available from Telstra (Australia).

Telstra Enterprise SIP Trunking service provides PSTN access via a SIP trunk between the enterprise and Telstra network as an alternative to legacy analog or digital trunks. This approach generally results in lower cost for the enterprise.

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

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

Table of Contents

1. Introduction

These Application Notes illustrate a sample configuration for Avaya Communication Server 1000 Release 7.6 (CS1000) and Avaya Aura® Session Manager Release 6.3.15 with SIP Trunks to Avaya Session Border Controller for Enterprise (Avaya SBCE) Release 6.3.6 when used to connect to the Telstra Enterprise SIP Trunking service available from Telstra (Australia).

Avaya Aura® Session Manager is a core SIP routing and integration engine that connects disparate SIP devices and applications within an enterprise. Avaya CS1000 is a telephony application server and is the point of connection between the enterprise endpoints and Avaya Aura® Session Manager. Avaya SBCE is the point of connection between Avaya Aura® Session Manager and Telstra Enterprise SIP Trunking service and is used to not only secure the SIP trunk, but also to make adjustments to VoIP traffic for interoperability.

The Enterprise SIP Trunking service available from Telstra is one of many SIP-based Voice over IP (VoIP) services offered to enterprises in Australia for a variety of voice communications needs. The Telstra Enterprise SIP Trunking service allows enterprises in Australia to place outbound local and long distance calls, receive inbound Direct Inward Dialing (DID) calls from the PSTN, and place calls between an enterprise's sites.

2. General Test Approach and Test Results

The general test approach was to make calls from/to Avaya CS1000 through Avaya Aura® Session Manager and Avaya SBCE using Telstra Enterprise SIP Trunking service. The configuration (shown in **Figure 1**) was used to exercise the features and functionality tests listed in **Section 2.1**.

DevConnect Compliance Testing is conducted jointly by Avaya and DevConnect members. The jointly-defined test plan focuses on exercising 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 compliance testing focused on verifying inbound and outbound call flows between Avaya CS1000, Avaya Aura® Session Manager, Avaya SBCE, and the Telstra Enterprise SIP Trunking service.

The compliance testing was based on the standard Avaya DevConnect SIP Trunk test plan and the Telstra SIP Connect Accreditation Test Plan. The testing covered functionality required for compliance as a solution supported on the Telstra Enterprise SIP Trunk network. Calls were made to and from the PSTN across the Telstra network. The following standard features were tested as part of this effort:

- Inbound PSTN calls to various phone types including Unistim, SIP, digital and analog telephones at the enterprise. All inbound calls from PSTN are routed to the enterprise across the SIP trunk from the service provider.
- Outbound PSTN calls from various phone types including Unistim, SIP, digital and analog telephones at the enterprise. All outbound calls to PSTN are routed from the enterprise across the SIP trunk to the service provider.
- Inbound and outbound PSTN calls to/from Avaya i2050 softphone.
- Inbound and outbound Avaya CS1000 calls from/to Telstra IP Telephony (TIPT phones).
- Inbound and outbound Avaya CS1000 calls from/to Telstra Digital Office Technology (DOT phones).
- Dialing plans including local, long distance, international, outbound toll-free calls, etc.
- Calling Party Name presentation and Calling Party Name restriction.
- Codecs G.711A, G.711MU and G.729A.
- Incoming and outgoing fax using G.711 pass-through.
- DTMF tone transmissions as out-of-band RTP events as per RFC2833.
- Voicemail navigation for inbound and outbound calls.
- User features such as hold and resume, transfer, forward and conference.
- Off-net call forward with Diversion method.
- Avaya CS1000 MobileX feature.
- Response to OPTIONS heartbeat and Registration.
- Response to incomplete call attempts and trunk errors.
- Telstra Enterprise SIP Trunk failover.

2.2 Test Results

Interoperability testing of Telstra Enterprise SIP Trunking Service was completed with successful results for all test cases with the exception of the observations/limitations described below.

Please refer to the test case document for a complete list of solution issues found when tested.

- **Faxing** – Telstra Enterprise SIP Trunking service only supports FAX G.711 pass-through mode. G.711 fax pass-through was successfully tested during the compliance test.
- **Off-net Call Forwarding –** Telstra Enterprise SIP Trunking service requires either the History-info header or the Diversion header in the SIP INVITE message, which is sent to Telstra for call redirection, to have the user part in the SIP URI match a DID number assigned by Telstra. Otherwise, Telstra will reject that call. Avaya CS1000 only supports History-info but the user part in the SIP URI of the History-info header in the redirection INVITE does not match the DID number. Hence, Adaptations must be configured on Avaya Aura® Session Manager for Avaya CS1000 SIP entity and Avaya SBCE SIP entity to convert the History-info header in the redirection INVITE message into a Diversion header.

- **Off-net Call Transfer -** When a PSTN phone called to an Avaya phone, the phone answered the call and performed a blind transfer or consultative transfer to another PSTN endpoint. The expected behavior was that the Avaya phone transferred the call successfully. But in this case, the Avaya phone could not complete the transfer. In order to overcome this issue, plug-in 201 and plug-in 501 must be enabled on Avaya CS1000.
- **If the CS1000 phone holds/resumes an outbound call, the dialed digits were no longer displayed** - This is a known limitation on the CS1000.
- **Calling Line Identification Display (CLID) was not correctly displayed** - After call redirection, namely blind/consultative transfers, was completed with 2-way audio, the CLID on the transferee's phone was not updated accordingly. This is a known CS1000 limitation.
- **CS1000 Mobile-X –** When a PSTN phone calls an Avaya phone that has sim-ring to mobile phone (Mobile-X) enabled, the expected behavior is that both Avaya phone and mobile phone should ring. But in this case, only Avaya phone rang. This is due to a limitation on Avaya Aura® Session Manager. The Adaptation configured for the above off-net Call Forwarding scenario does not convert/replace the History-info header in the redirection INVITE message sent towards mobile phone (i.e., Telstra Enterprise SIP Trunk) with Diversion header. Telstra rejects this INVITE due to missing History-info as well as Diversion header. The only way to overcome this issue is to disable "Call screening" on Telstra. However, Telstra does not allow "Call screening" to be off.

2.3 Support

- **Avaya:** Avaya customers may obtain documentation and support for Avaya products by visiting http://support.avaya.com.
- **Telstra Australia:** Customers should contact their Telstra Business representative or follow the support links available on http://telstra.com.au.

3. Reference Configuration

The reference configuration used in these Application Notes is shown in the diagram below and consists of several components.

- Avaya Aura® Session Manager running on VMware ESXi 5.5.
- Avaya Aura® System Manager running on VMware ESXi 5.5.
- Avaya CS1000 CPPM co-resident.
- Avaya CallPilot 201i.
- Avaya IP phones are represented with Avaya 1100 Series IP Telephones running Unistim/SIP software.
- Avaya 3904 digital phone.
- Avaya i2050 softphone.
- The Avaya SBCE provided Session Border Controller functionality, including, Network Address Translation, SIP header manipulation, and Topology Hiding between the Telstra SIP Trunking service and the enterprise internal network.
- Telstra Enterprise SIP Trunking service provided two groups for SIP trunks. The solution as detailed in these Application Notes was a dual-trunk setup, with the single SBC

configured with two separate trunks, originating from two separate SBC's within the Telstra lab network ('sbc-cw.ipvs.net' and 'sbc-exh.ipvs.net'). Each trunk had different registration credentials, and was provisioned with a separate number range (Trunk Pilot numbers and DID's). DID range assigned by Telstra for this testing: 0353xxxxx (10 digits).

The following is a summary of the requirements for Telstra Enterprise SIP Trunk to process the incoming SIP INVITE to Telstra:

- The Enterprise Trunk pilot number is required to be substituted into the P-Asserted-Identity Header.
- Calls originating from the customer equipment with the From Header as 'anonymous@anonymous.invalid' or 'anonymous@customer.sip.domain' (example) are no longer accepted. The From header always needs to be a valid DID number that is associated with the Enterprise SIP trunks.
- Signaling Manipulation scripts are added on Avaya SBCE to satisfy above requirements.

All IP addresses shown in the diagram are private IP addresses.

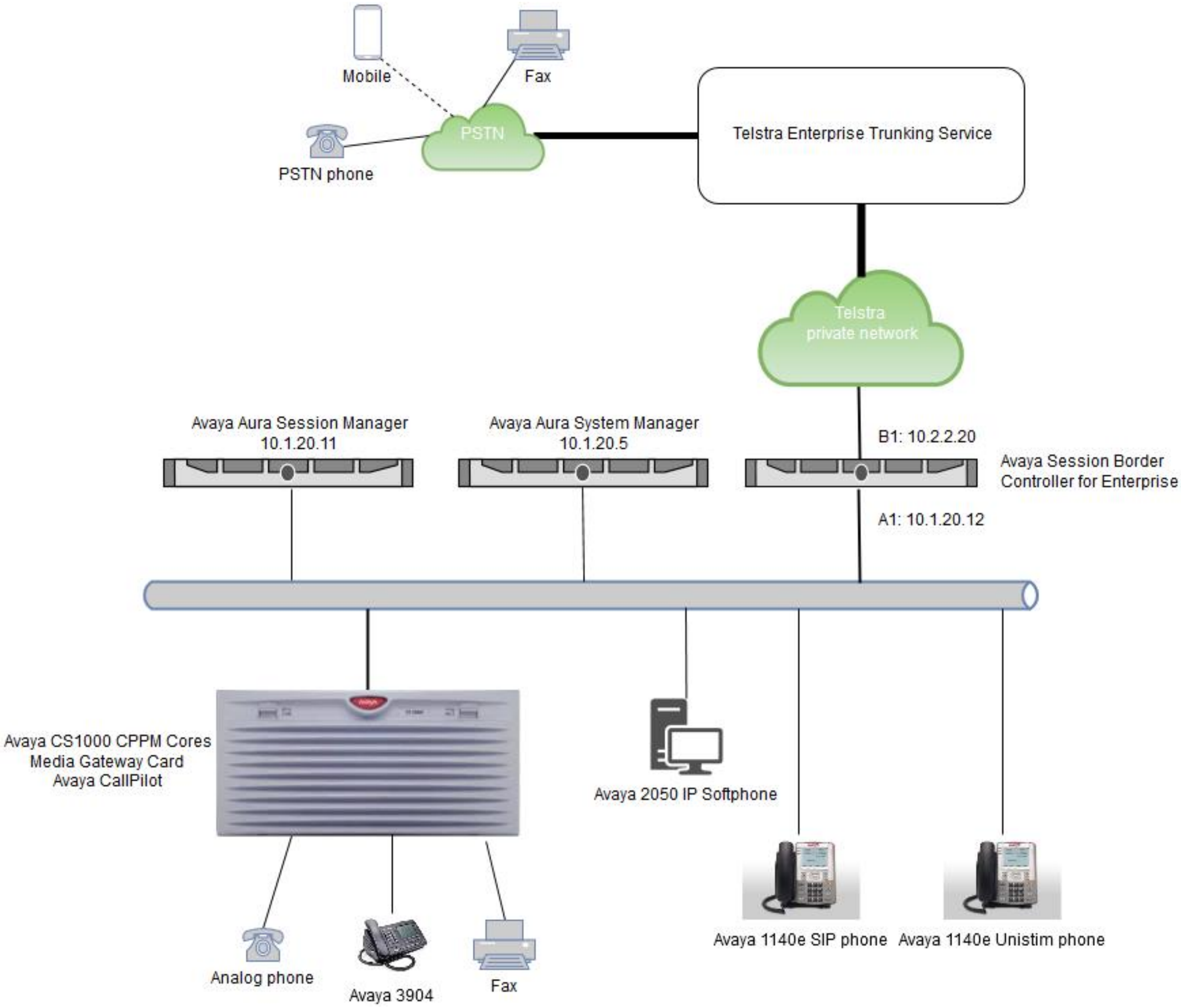


Figure 1: Network Components as Tested

4. Equipment and Software Validated

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

Component	Version
Avaya	
Avaya Aura System Manager	6.3.15
Avaya Aura Session Manager	6.3.15
Avaya Session Border Controller for Enterprise	6.3 SP6
Avaya Communication Server 1000 (CPPM)	Call Server 7.65 SP8 Signaling Server 7.65 SP8
Avaya CallPilot	5.0
Avaya 11xx SIP phone	4.4.5
Avaya 11xx Unistim phone	5.5.6
Avaya 2050 IP softphone	4.4.6
Avaya 3904 digital phone	9.3
Analog phone	N/A
Service Provider	
Broadsoft	R19 SP1

5. Configure Avaya CS1000

The configuration of the CS1000 outlined in these Application Notes uses the Incoming Digit Translation feature to receive calls, and the Special Number (SPN) feature to route calls from the CS1000 to the PSTN via SIP trunks to the Telstra Enterprise SIP Trunking service network.

These Application Notes assume that the basic CS1000 configuration has already been administered. For further information on CS1000, please consult the references in **Section 10**.

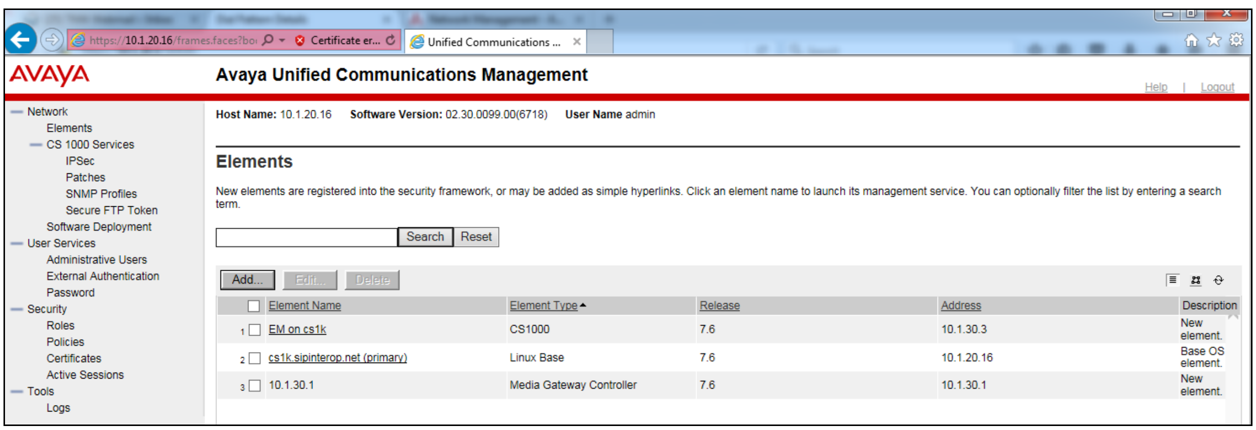
The procedures below describe the configuration details for configuring the CS1000.

5.1 Access to CS1000 System

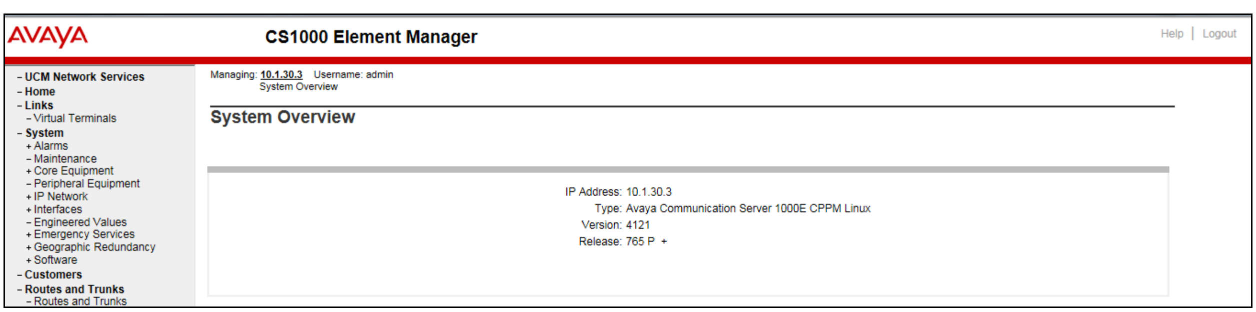
Changes to CS1000 can be made using Element Manager, which is accessible from Unified Communications Management (UCM) and offers the user a Web GUI for making changes. Changes to CS1000 can also be made using the Command Line Interface (CLI) offered using PuTTY to make an SSH connection.

5.1.1 Access to CS1000 Element Manager

Open an instance of a web browser and connect to UCM using the following address: https://<UCM IP address>/network-login/. Log in using an appropriate User ID and Password (not shown). The UCM screen is displayed.



Click on the **Element Name** of the CS1000 Element: "**EM on cs1k**". The CS1000 Element Manager **System Overview** page is displayed as shown below:



5.1.2 Access CS1000 Call Server by using CLI

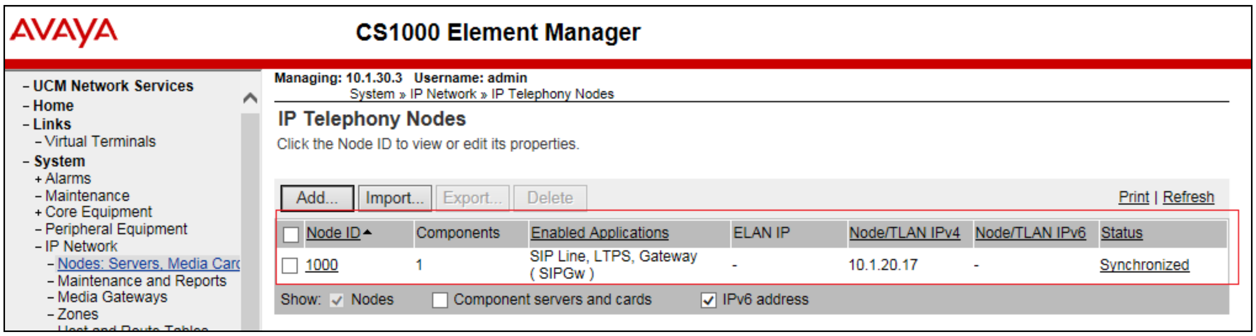
Using Putty to open a SSH session to the IP address of the CS1000 Signaling Server then log in with administrator credentials. Run the command **cslogin** and log in with the appropriate user account and password. Sample output is shown below.

```
login as: admin

            Avaya Inc. Linux Base  7.65
The software and data stored on this system are the property of, or licensed to, Avaya Inc. and
are lawfully available only to authorized users for approved purposes. Unauthorized access to
any software or data on this system is strictly prohibited and punishable under appropriate laws.
If you are not an authorized user then do not try to login. This system may be monitored for
operational purposes at any time.

admin@10.1.20.16's password:
Last login: Tue Sep 20 16:57:20 2016 from 10.1.20.3
[admin@cs1k ~]$
[admin@cs1k ~]$
[admin@cs1k ~]$
[admin@cs1k ~]$ cslogin

SEC054 A device has connected to, or disconnected from, a pseudo tty without authentica
ting

TTY 07 SCH MTC BUG OSN   10:46
OVL111 IDLE   0
>
```

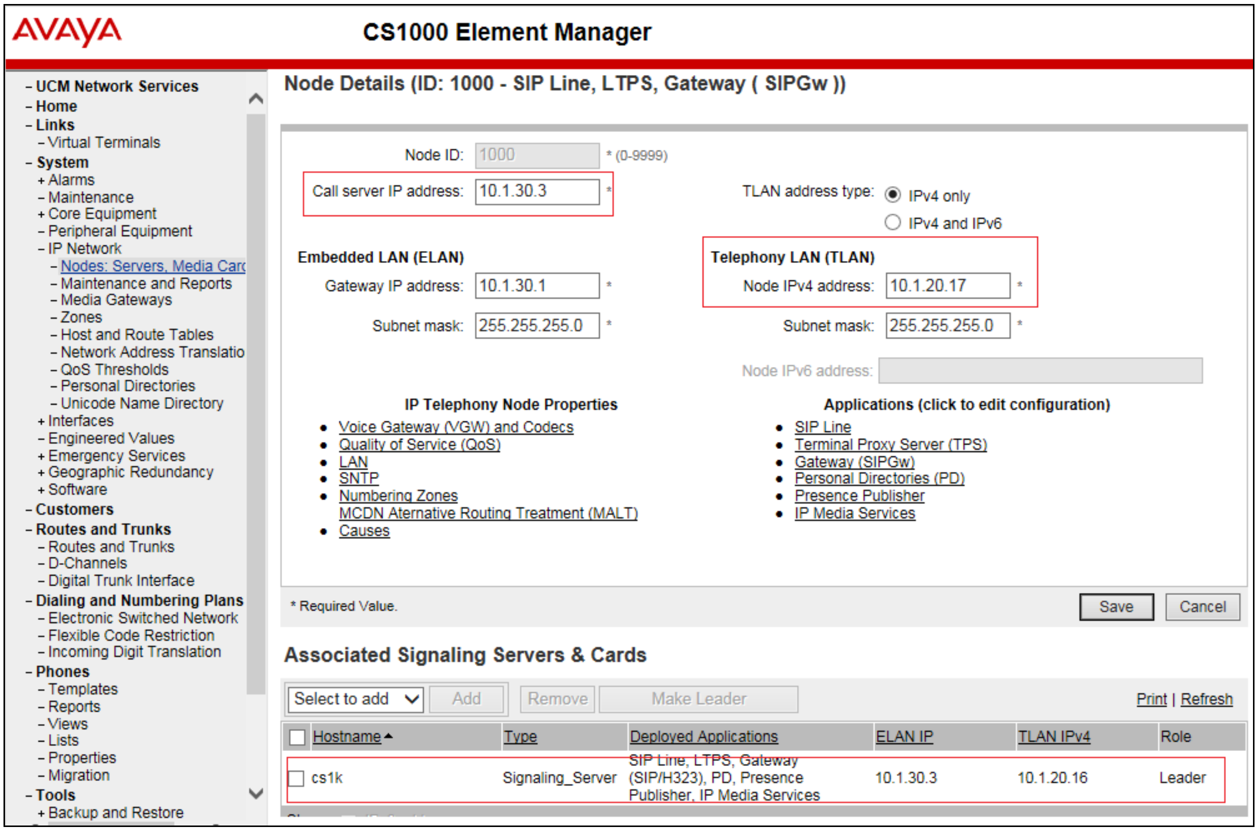
5.2 Administer IP Telephony Node

5.2.1 Obtain Node IP address

These Application Notes assume that the basic CS1000 configuration has already been administered and that a Node has already been created. This section describes the steps for configuring a Node (**Node ID 1000**) in CS1000 IP network to work with Telstra Enterprise SIP Trunking service. For further information on CS1000, please consult the references in **Section 10**. **Access** Element Manager as per **Section 5.1.1**. Select **System** > **IP Network** > **Nodes: Servers, Media Cards** and then click on the **Node ID** as shown below**:**

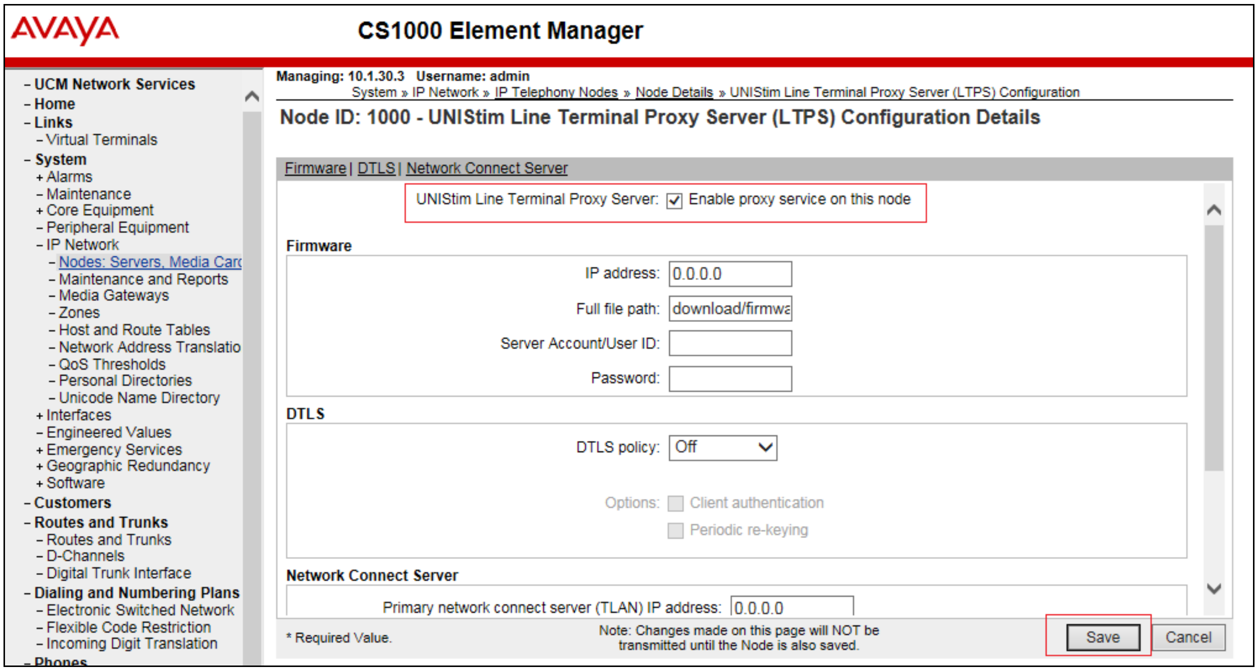


The **Node Details** screen is displayed with the IP address of the CS1000 node: **Call server IP address: 10.1.30.3**. The **Node IPv4 address 10.1.20.17** for **Telephony LAN (TLAN)** is a virtual address which corresponds to the **TLAN IPv4** address **10.1.20.16** of the Signaling Server/SIP Signaling Gateway. The SIP Signaling Gateway uses this Node IP address to communicate with other components to process SIP calls.



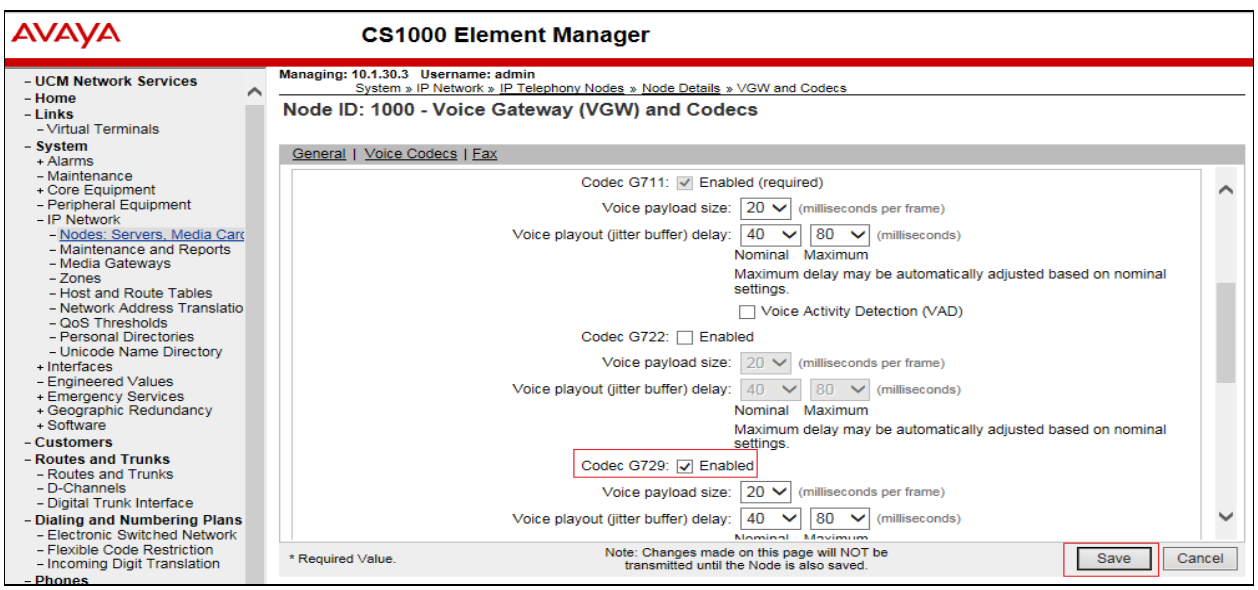
5.2.2 Administer Terminal Proxy Server (TPS)

Continuing from **Section 5.2.1**, on the **Node Details** page, select the **Terminal Proxy Server** (**TPS**) link then check the **UNIStim Line Terminal Proxy Server** box to enable proxy service on this node and click **Save** button:



5.2.3 Administer Voice Codecs

On the **Node Details** page shown in **Section 5.2.1**, click on **Voice Gateway (VGW) and Codecs**. Check **Codec G.729** box then click **Save** button:



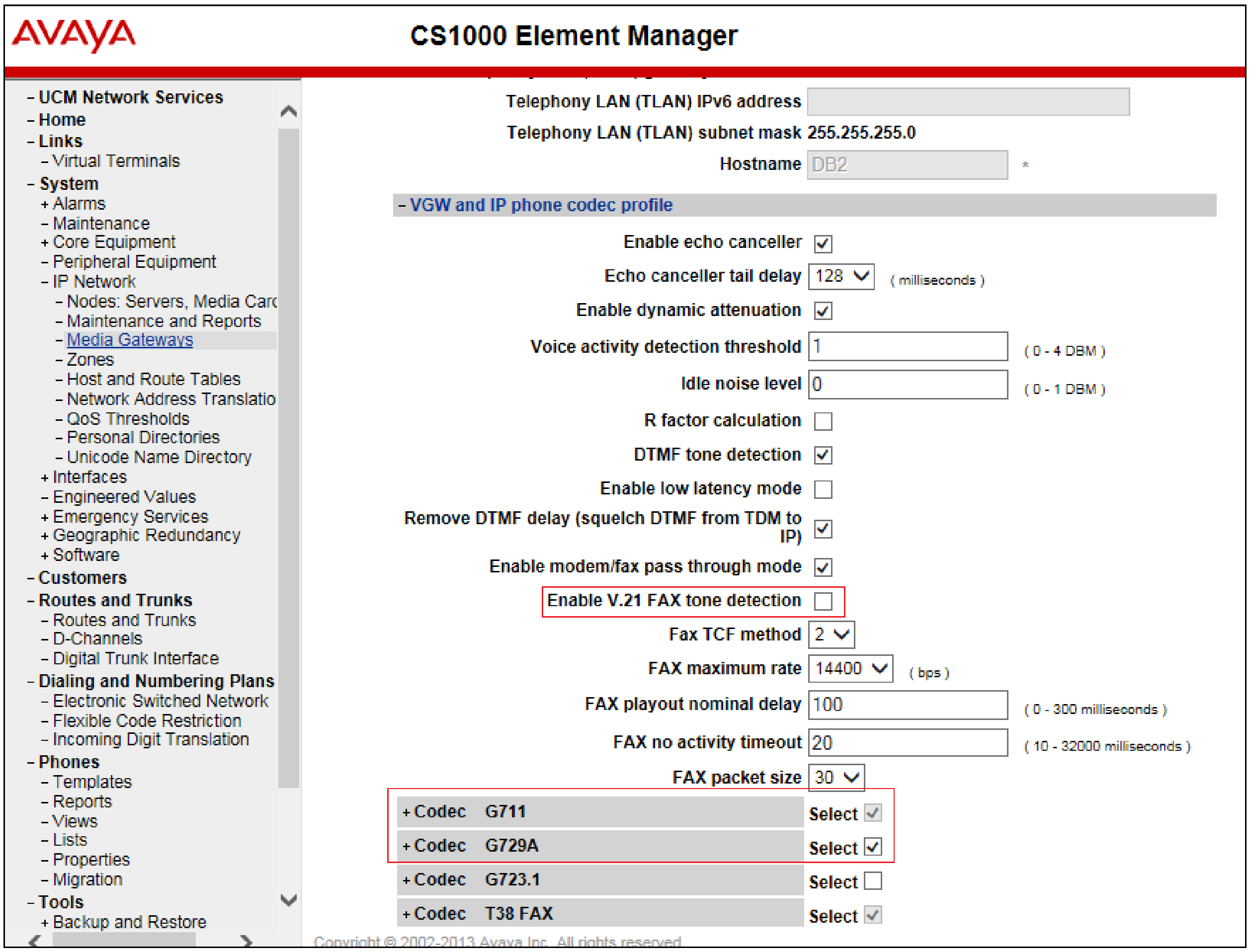
5.2.4 Synchronize New Configuration

On **Node Details** page shown in **Section 5.2.1**, click on the **Save** button. The **Node Saved** screen is displayed. Click on **Transfer Now** (not shown).

The **Synchronize Configuration Files (Node ID <1000>)** screen is displayed (not shown). Check the **cs1k** box and click on **Start Sync**. When the synchronization completes, check the **cs1k** box and click on the **Restart Applications** (not shown).

5.2.5 Enable Voice Codec on Media Gateways

From the left menu of the **Element Manager** page, select **System > IP Network > Media Gateways**. The Media Gateways page will appear (not shown). Click on the **MGC** which is located on the right of the page. In the following screen, uncheck **Enable V.21 FAX tone detection** box then scroll down to select the Codec **G.711** (by default on CS1000) and **G.729A**. Scroll down to the bottom of the page and click on the **Save** button (not shown).



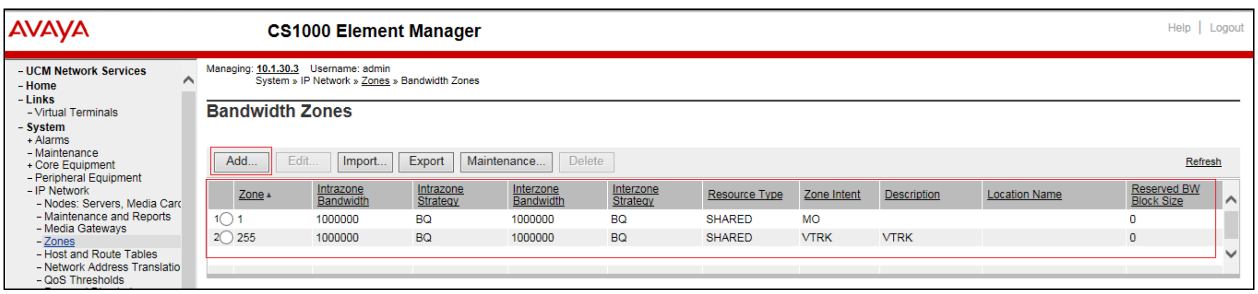
5.3 Zones and Bandwidth Management

Select **System > IP Network > Zones** from the left pane (not shown), click on **Bandwidth Zones** (not shown). Click **Add** to create new zones for IP Phones and Virtual Trunk.

Input these values for **Zone 1** which is used for IP Phones and Voice Gateway:

- **Intrazone Bandwidth** (**INTRA_BW**): **1000000**.
- **Intrazone Strategy (INTRA_STGY**): Set codec for local calls. Select **Best Bandwidth (BB)** to use **G.729** as the first priority codec for negotiation or select **Best Quality (BQ)** to use **G.711** as the first priority codec for negotiation. In this example, **BQ** was chosen.
- **Interzone Bandwidth (INTER_BW)**: **1000000**.
- **Interzone Strategy (INTER_STGY)**: Set codec for the calls over trunk. Select **Best Bandwidth (BB)** to use **G.729** as the first priority codec for negotiation or select **Best Quality (BQ)** to use **G.711** as the first priority codec for negotiation. In this example, **BQ** was chosen.
- **Zone Intent (ZBRN)**: Select **MO** for IP phones, and Voice Gateway.

Use the same above values for **Zone 255** which is used for virtual trunk except for **Zone Intent (ZBRN)** field. Select **VTRK** for this field.

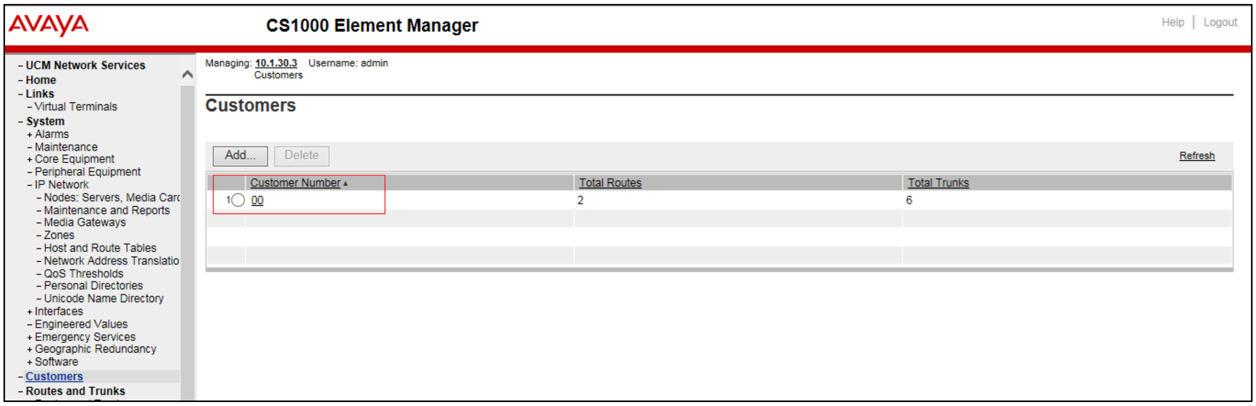


5.4 Administer SIP Trunk

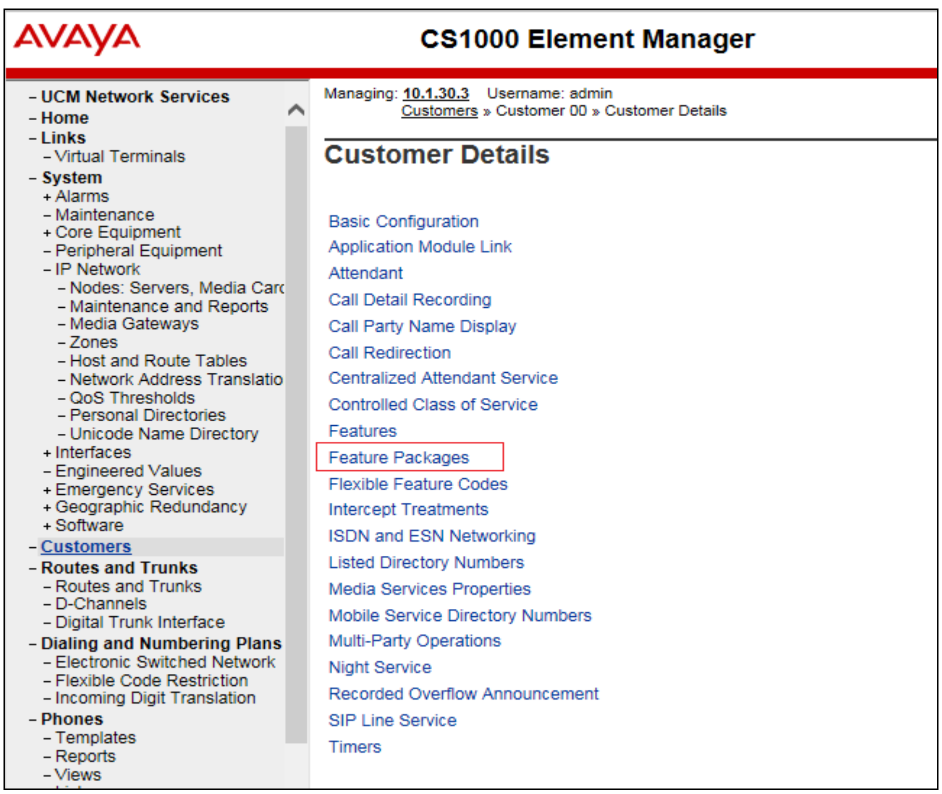
This section describes the steps for establishing a SIP connection between the SIP Signaling Gateway and Avaya Aura® Session Manager.

5.4.1 Integrated Services Digital Network (ISDN)

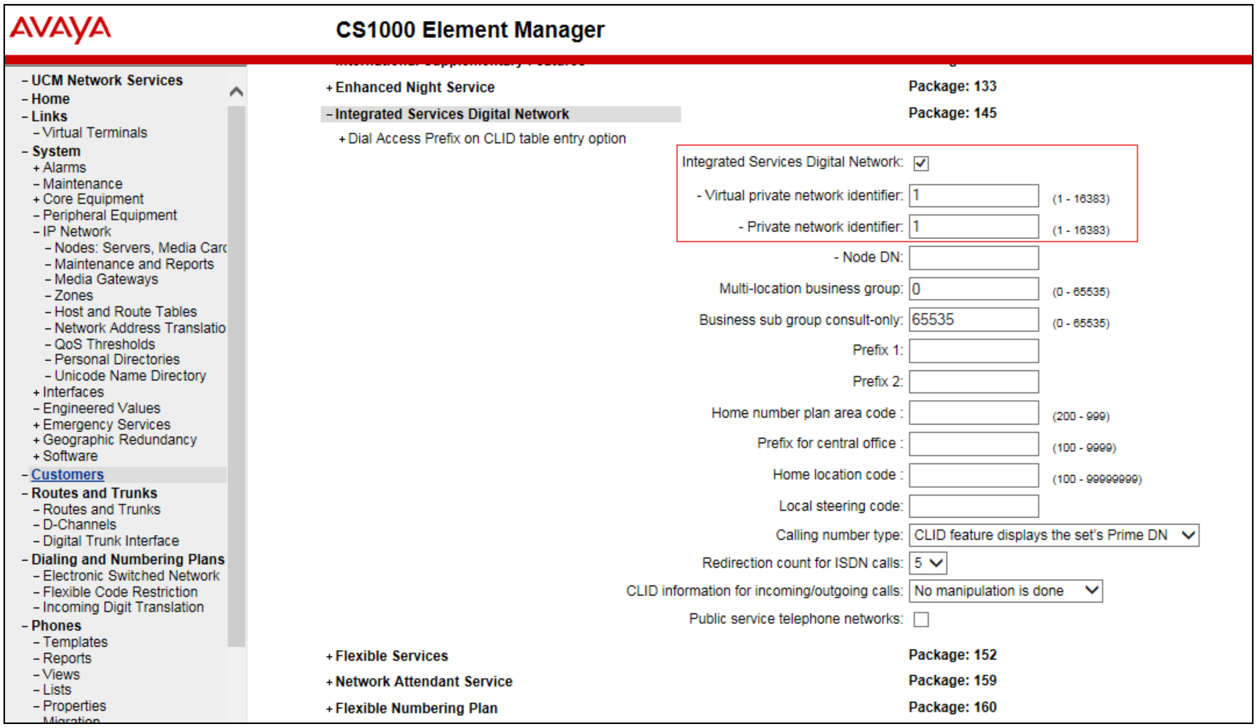
Select **Customers** in the left pane. The **Customers** screen is displayed. Click on the link associated with the appropriate customer, in this case **00**.



The **Customer Details** page will appear. Select the **Feature Packages** option from **Customer Details** page.



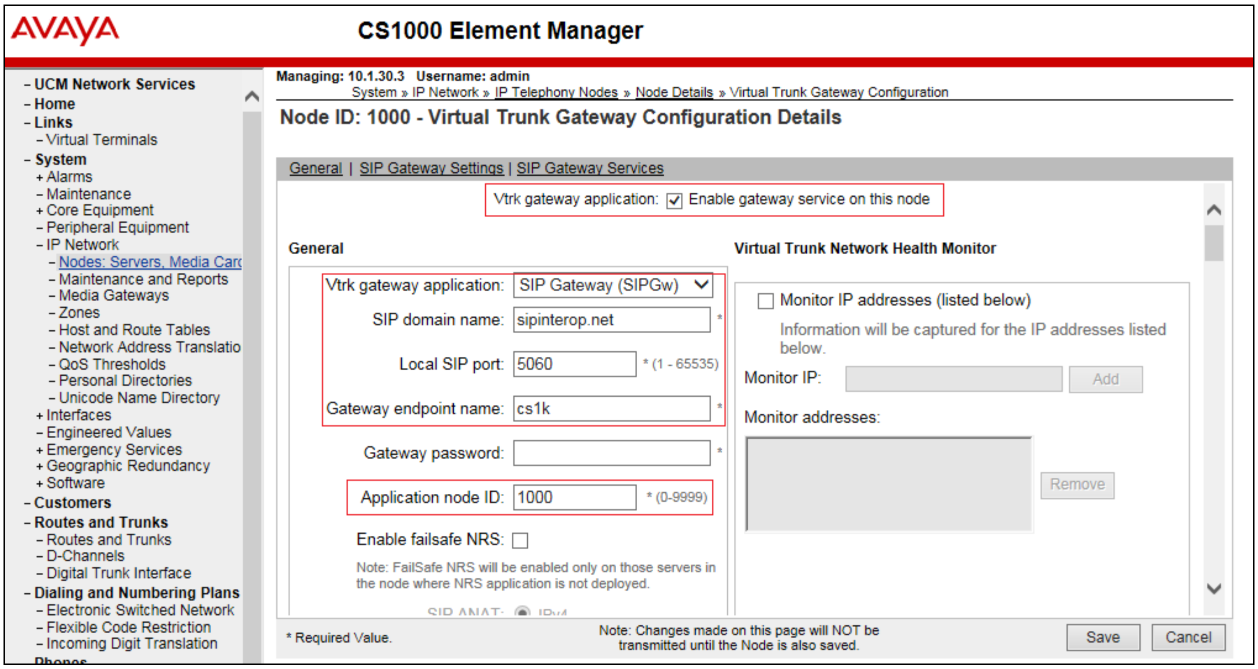
The screen is updated with a list of available **Feature Packages**. Select **Integrated Services Digital Network** to edit the parameters shown below. Check the **Integrated Services Digital Network** option, enter **1** into **Virtual private network identifier** and **Private network identifier**, then click on the **Save** button (not shown).



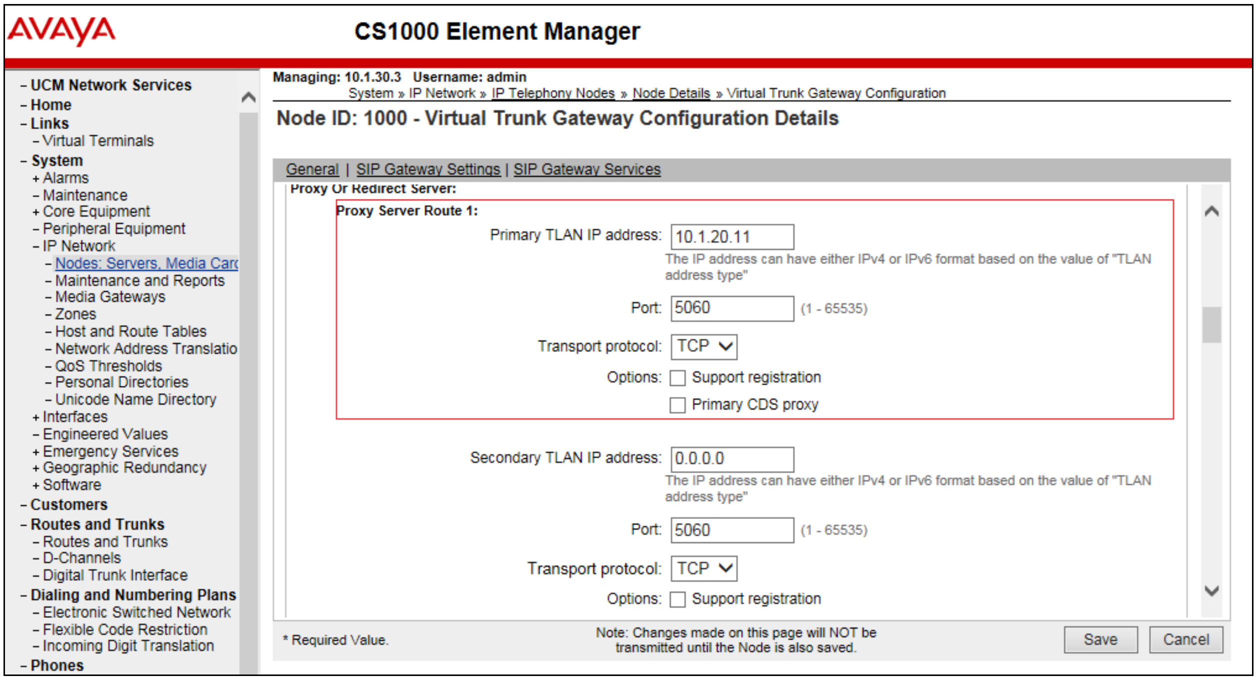
5.4.2 Administer SIP Trunk Gateway

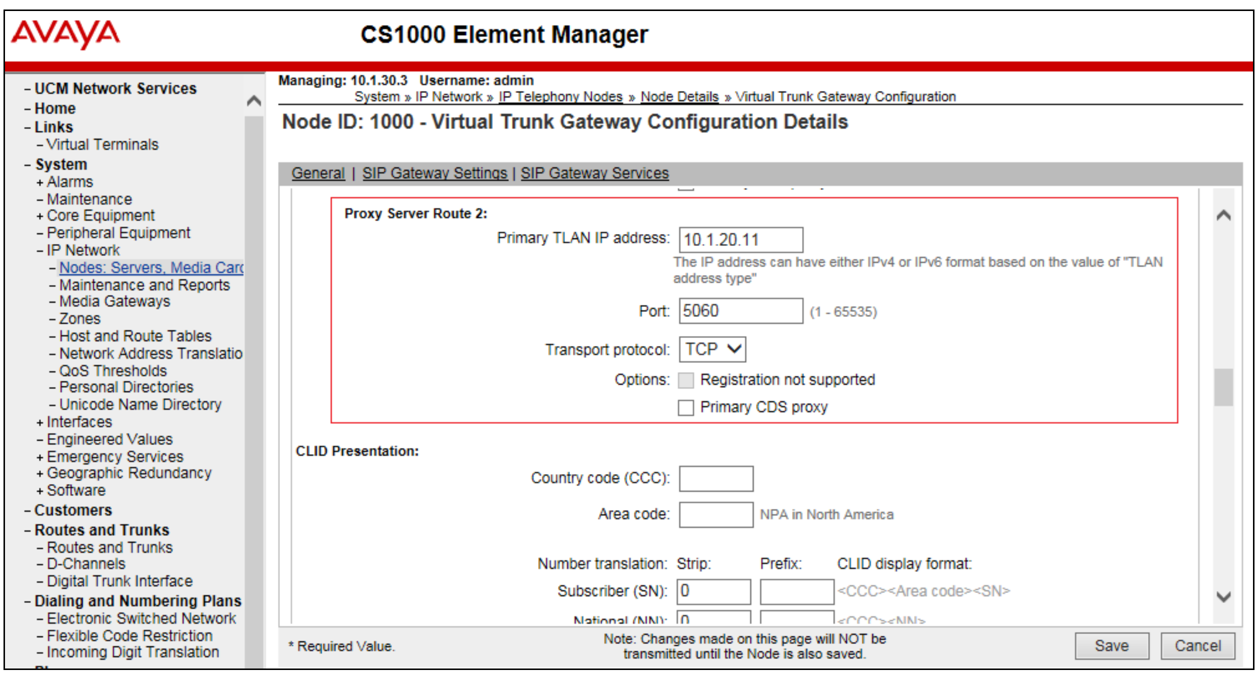
Select **System > IP Network > Nodes: Servers, Media Cards** from the left pane. In the **IP Telephony Nodes** screen displayed (not shown), select the **Node ID** of the CS1000 system. The **Node Details** screen is displayed as shown in **Section 5.2.1**.

On the **Node Details** screen, select **SIP Gateway (SIPGw)** for the **Vtrk gateway application** field. Under the **General tab** of the **Virtual Trunk Gateway Configuration Details** screen, enter the following values (highlighted in red boxes) for the specified fields, and retain the default values for the remaining fields as shown below. The **SIP domain name** and **Local SIP port** should be matched with the configuration of Avaya Aura® Session Manager in **Section 6.2**, and **6.6**.



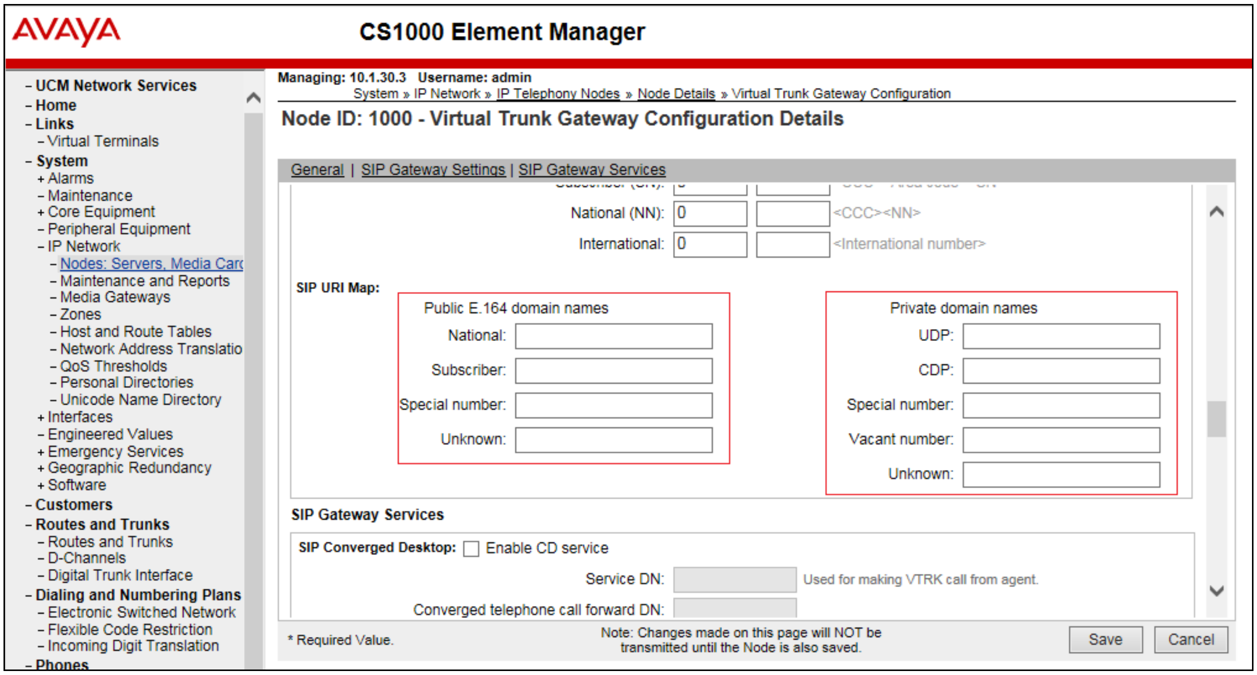
Click on the **SIP Gateway Settings** tab. Under **Proxy or Redirect Server**, enter the following values (highlighted in red boxes) for the specified fields and retain the default values for the remaining fields, as shown below. Enter the IP address of Avaya Aura® Session Manager in the **Primary TLAN IP address** field. Enter **5060** for **Port** and select **TCP** for **Transport protocol**. This should be matched with the configuration of Avaya Aura® Session Manager (see in **Section 6.5.1**). Uncheck the **Support registration** checkbox.





Scroll down to the **SIP URI Map** section. Under **Public E.164 domain names**, leave blank for: **National, Subscriber, Special Number, Unknown**.

Under **Private domain names**, leave blank for: **UDP, CDP, Special Number, Vacant number, Unknown**.



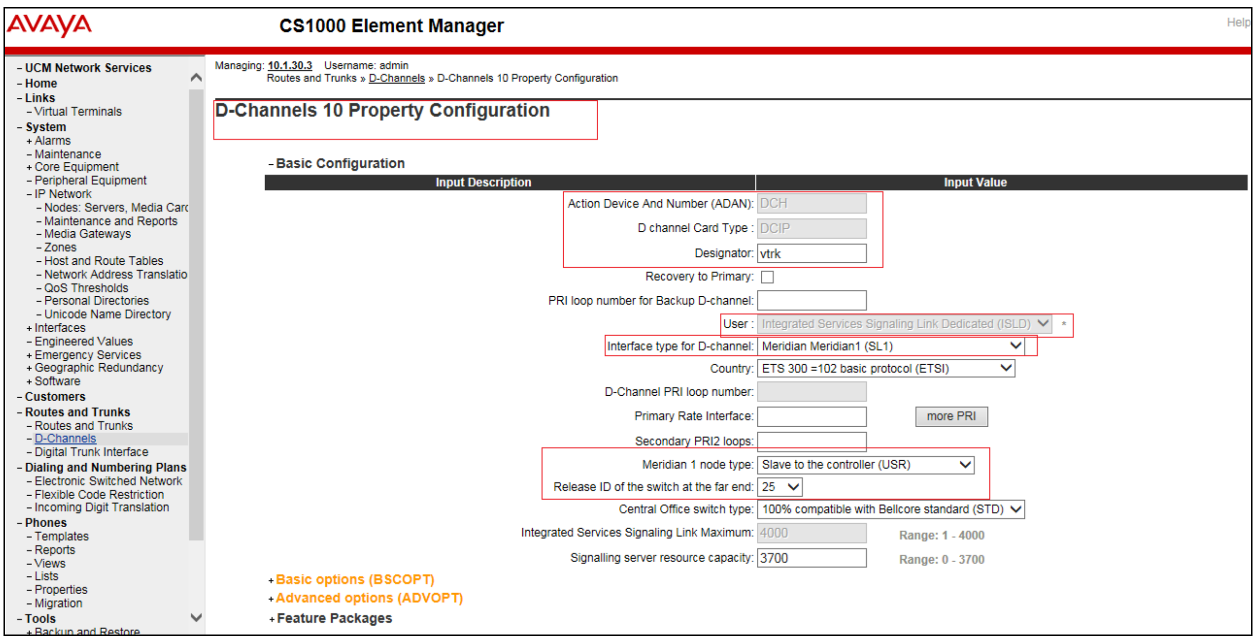
Synchronize the new configuration (please refer to **Section 5.2.4**).

5.4.3 Administer Virtual D-Channel

Select **Routes and Trunks > D-Channels** (not shown) from the left pane to display the **D-Channels** screen (not shown) . In the **Choose a D-Channel Number** field, select an available **D-channel** from the drop-down list and type **DCH**. Click **Add** button (not shown).

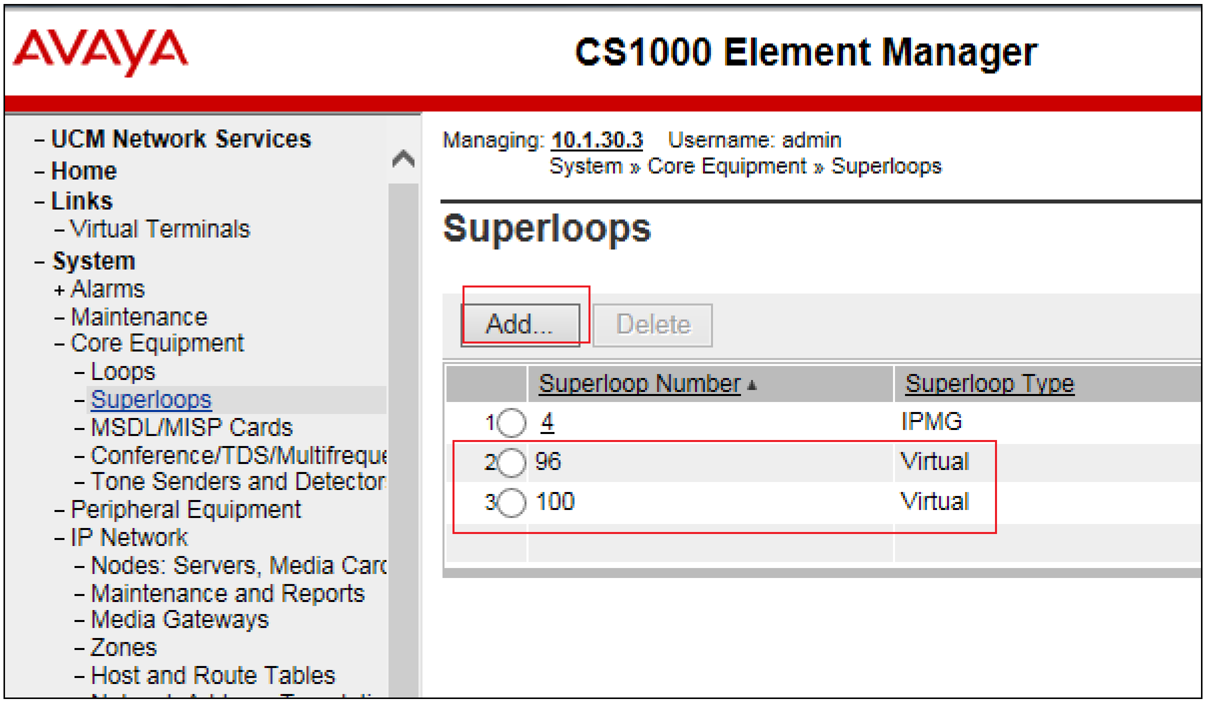
The **D-Channels 10 Property Configuration** screen is displayed next, as shown below. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **D-channel Card Type**: **D-Channel is over IP (DCIP)**.
- **Designator**: A descriptive name.
- **User: Integrated Services Signaling Link Dedicated (ISLD)**.
- **Interface type for D-channel: Meridian Meridian1 (SL1)**.
- **Meridian 1 node type: Slave to the controller (USR)**.
- **Release ID of the switch at the far end: 25**.



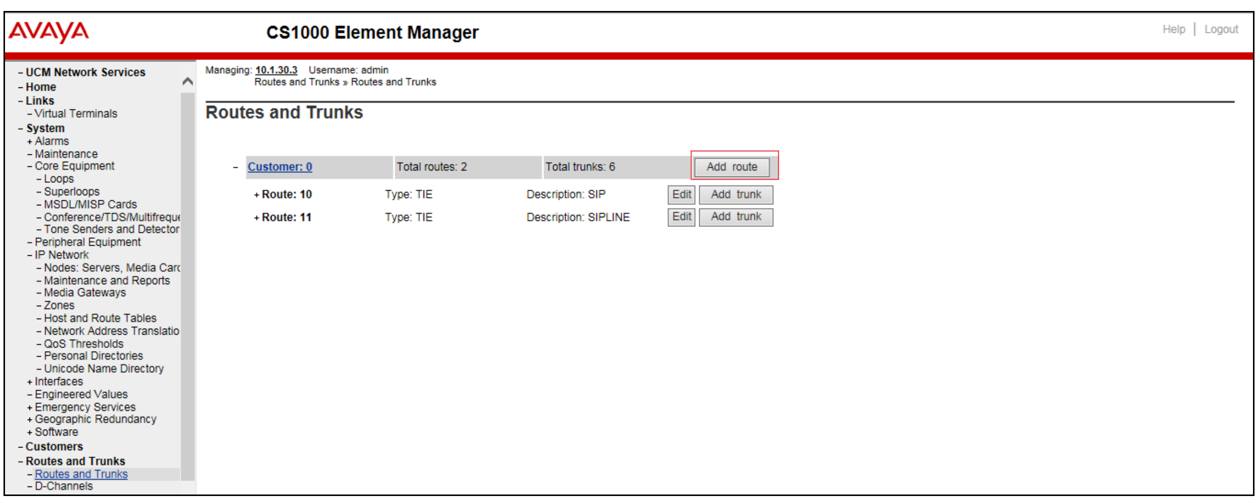
5.4.4 Administer Virtual Super-Loop

Select **System > Core Equipment > Superloops** from the left pane to display the **Superloops** screen. If the Superloop does not exist, click the **Add** button to create a new one as shown below. In this example, **Virtual Superloops 96, 100** have been added and were being used.



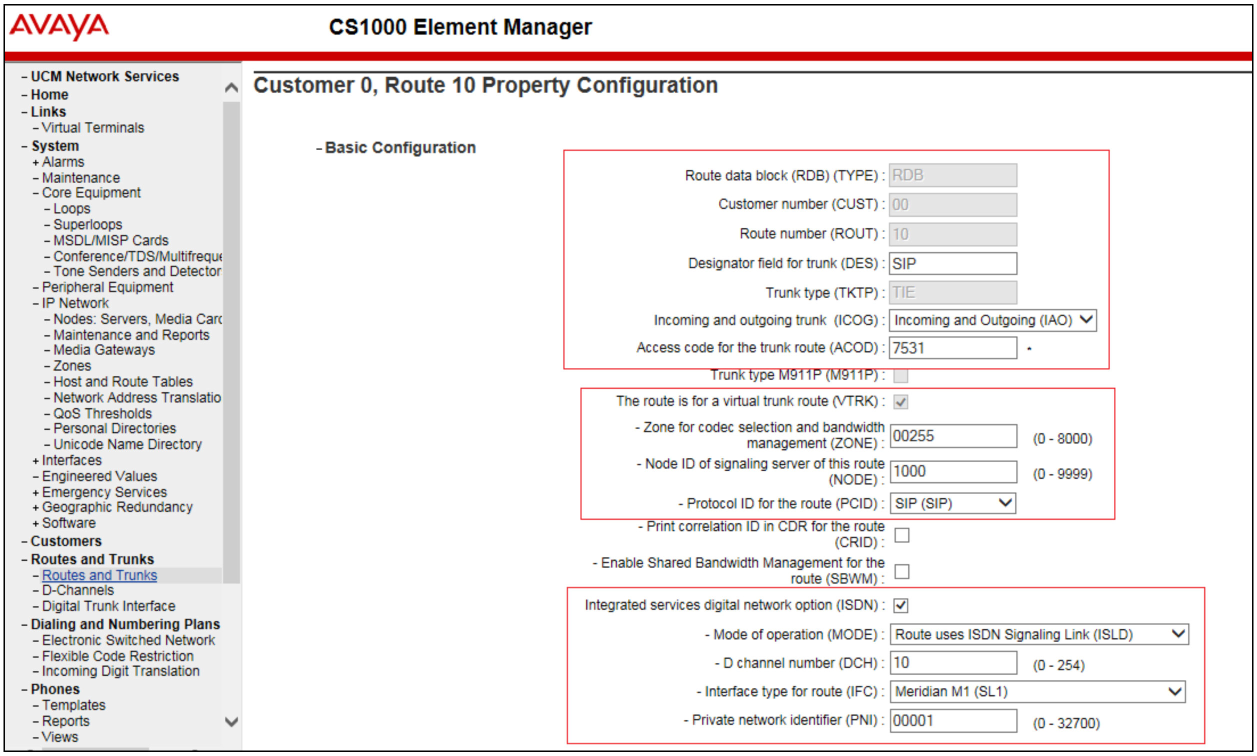
5.4.5 Administer Virtual SIP Routes

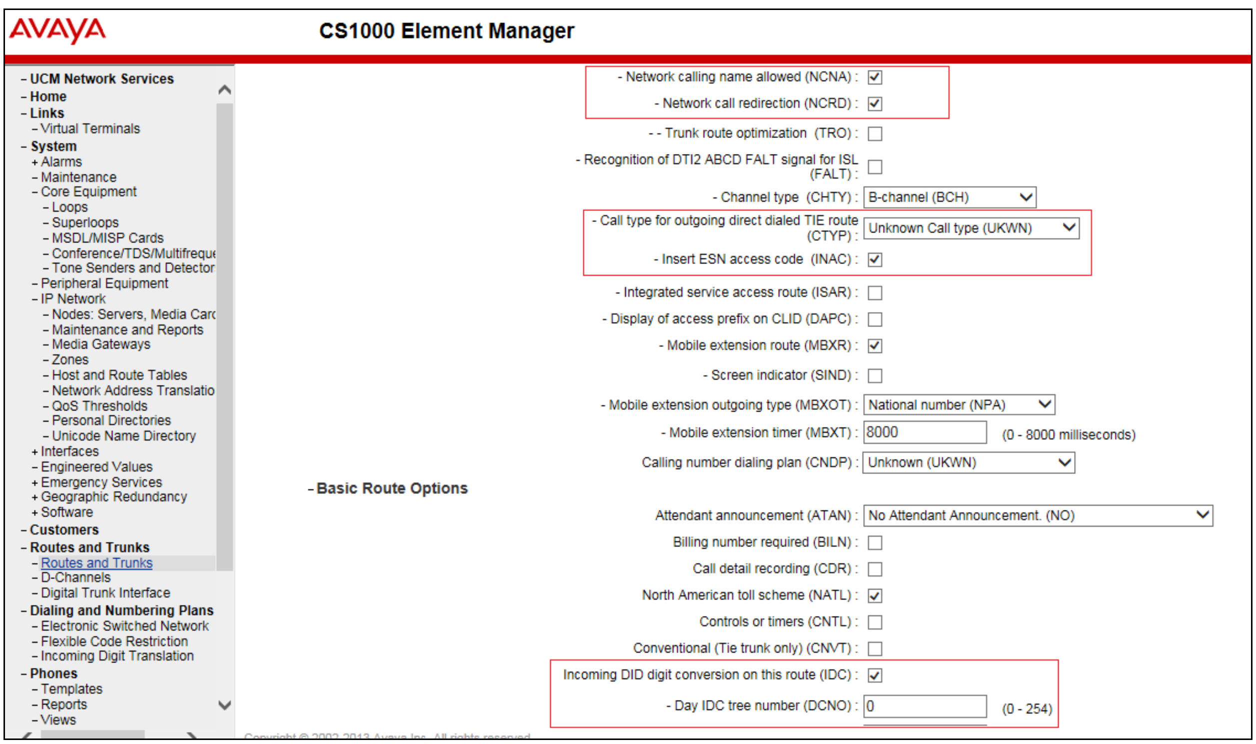
Select **Routes and Trunks > Routes and Trunks** (not shown) from the left pane to display the **Routes and Trunks** screen. In this example, **Customer 0** was being used. Click on the **Add route** button as shown below.



The **Customer 0**, **New Route Configuration** screen is displayed next (not shown). The **Basic Configuration** section is displayed. Enter the following values for the specific fields, and retain the default values for the remaining fields. The screenshot of **Basic Configuration** section of existing **route 10** is displayed to edit as shown below.

- **Route data block (RDB) (TYPE): RDB** as default.
- **Customer number (CUST): 0** as customer 0 is used.
- **Route number (ROUT)**: Enter an available route number (example: route **10**).
- **Designator field for trunk (DES)**: A descriptive text (**SIP**).
- **Trunk type (TKTP): TIE** trunk data block (**TIE**).
- **Incoming and outgoing trunk (ICOG): Incoming and Outgoing (IAO)**.
- **Access code for the trunk route (ACOD)**: An available access code (example: **7531**)
- Check **The route is for a virtual trunk route (VTRK)** field, to enable four additional fields to appear.
- For **Zone for codec selection and bandwidth management (ZONE)** field, enter **255** (created in **Section 5.3**). Note: the Zone value is filled out as 255, but after it is added, the screen is displayed with prefix 00.
- For **Node ID of signaling server of this route (NODE)** field, enter the node number 1000 (created in **Section 5.2.1**).
- Select **SIP (SIP)** from the drop-down list for **Protocol ID for the route (PCID)** field.
- Check **Integrated Services Digital Network option (ISDN)** box to enable additional fields to appear. Scrolling down to the bottom of the screen, enter the following values for the specified fields, and retain the default values for the remaining fields.
    - **Mode of operation (MODE)**: select **Route uses ISDN Signalling Link (ISLD)**.
    - **D channel number (DCH):** enter **10** (created in **Section 5.4.3**).
    - **Interface type for route (IFC):** select **Meridian M1 (SL1)**.
    - **Private network identifier (PNI):** enter **1**. Note: the value is filled out as 1, but after it is added, the screen is displayed with prefix 0000.
    - **Network calling name allowed (NCNA)**: check this option to allow calling name display.
    - **Network call redirection (NCRD)**: check this option to allow call redirection.
    - **Call type for outgoing direct dialed TIE route (CTYP)**: select **Unknown Call type (UKWN)**.
    - **Insert ESN access code (INAC)**: check this option to insert ESN access code.
- Click on **Basic Route Options**, check **Incoming DID digit conversion on this route (IDC)** boxes. Enter 0 for both **Day IDC tree number** and **Night IDC tree number**.


AVAYA
CS1000 Element Manager
Customer 0, Route 10 Property Configuration
- Basic Configuration
Route data block (RDB) (TYPE) : RDB
Customer number (CUST) : 00
Route number (ROUT) : 10
Designator field for trunk (DES) : SIP
Trunk type (TKTP) : TIE
Incoming and outgoing trunk (ICOG) : Incoming and Outgoing (IAO)
Access code for the trunk route (ACOD) : 7531
Trunk type M911P (M911P) :
The route is for a virtual trunk route (VTRK) :
- Zone for codec selection and bandwidth management (ZONE) : 00255 (0 - 8000)
- Node ID of signaling server of this route (NODE) : 1000 (0 - 9999)
- Protocol ID for the route (PCID) : SIP (SIP)
- Print correlation ID in CDR for the route (CRID) :
- Enable Shared Bandwidth Management for the route (SBWM) :
Integrated services digital network option (ISDN) :
- Mode of operation (MODE) : Route uses ISDN Signaling Link (ISLD)
- D channel number (DCH) : 10 (0 - 254)
- Interface type for route (IFC) : Meridian M1 (SL1)
- Private network identifier (PNI) : 00001 (0 - 32700)


AVAYA
CS1000 Element Manager
- Network calling name allowed (NCNA) :
- Network call redirection (NCRD) :
- - Trunk route optimization (TRO) :
- Recognition of DTI2 ABCD FALT signal for ISL (FALT) :
- Channel type (CHTY) : B-channel (BCH)
- Call type for outgoing direct dialed TIE route (CTYP) : Unknown Call type (UKWN)
- Insert ESN access code (INAC) :
- Integrated service access route (ISAR) :
- Display of access prefix on CLID (DAPC) :
- Mobile extension route (MBXR) :
- Screen indicator (SIND) :
- Mobile extension outgoing type (MBXOT) : National number (NPA)
- Mobile extension timer (MBXT) : 8000 (0 - 8000 milliseconds)
Calling number dialing plan (CNDP) : Unknown (UKWN)
- Basic Route Options
Attendant announcement (ATAN) : No Attendant Announcement. (NO)
Billing number required (BILN) :
Call detail recording (CDR) :
North American toll scheme (NATL) :
Controls or timers (CNTL) :
Conventional (Tie trunk only) (CNVT) :
Incoming DID digit conversion on this route (IDC) :
- Day IDC tree number (DCNO) : 0 (0 - 254)

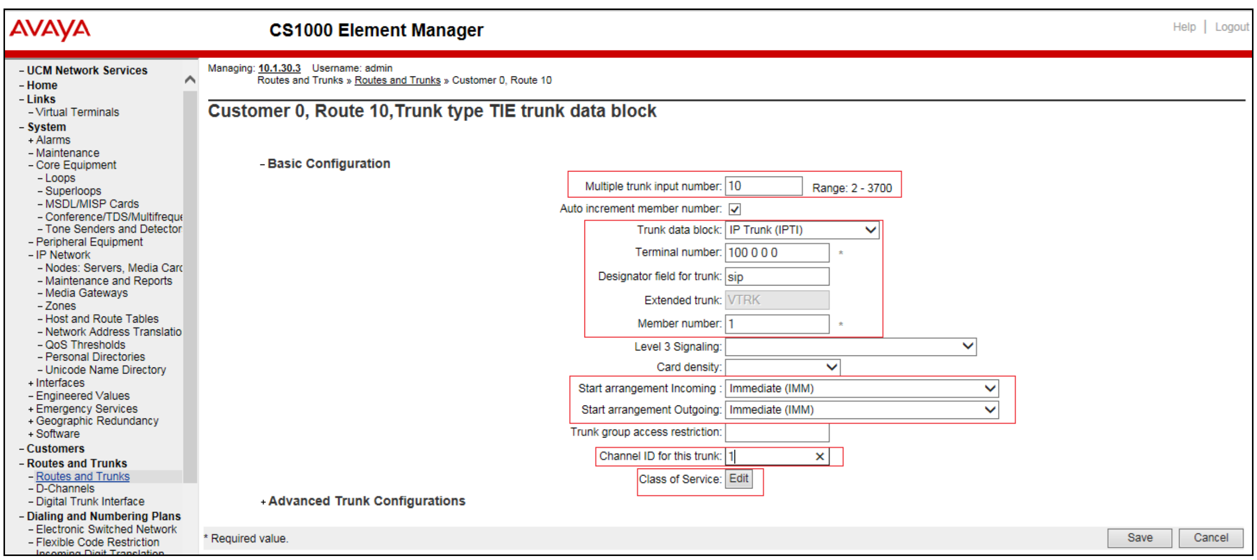
5.4.6 Administer Virtual Trunks

Select **Routes and Trunks > Route and Trunks** (not shown). The Route list is now updated with the newly added routes in **Section 5.4.5**. In the example, **Route 10** was added. Click on the **Add** trunk button (not shown).

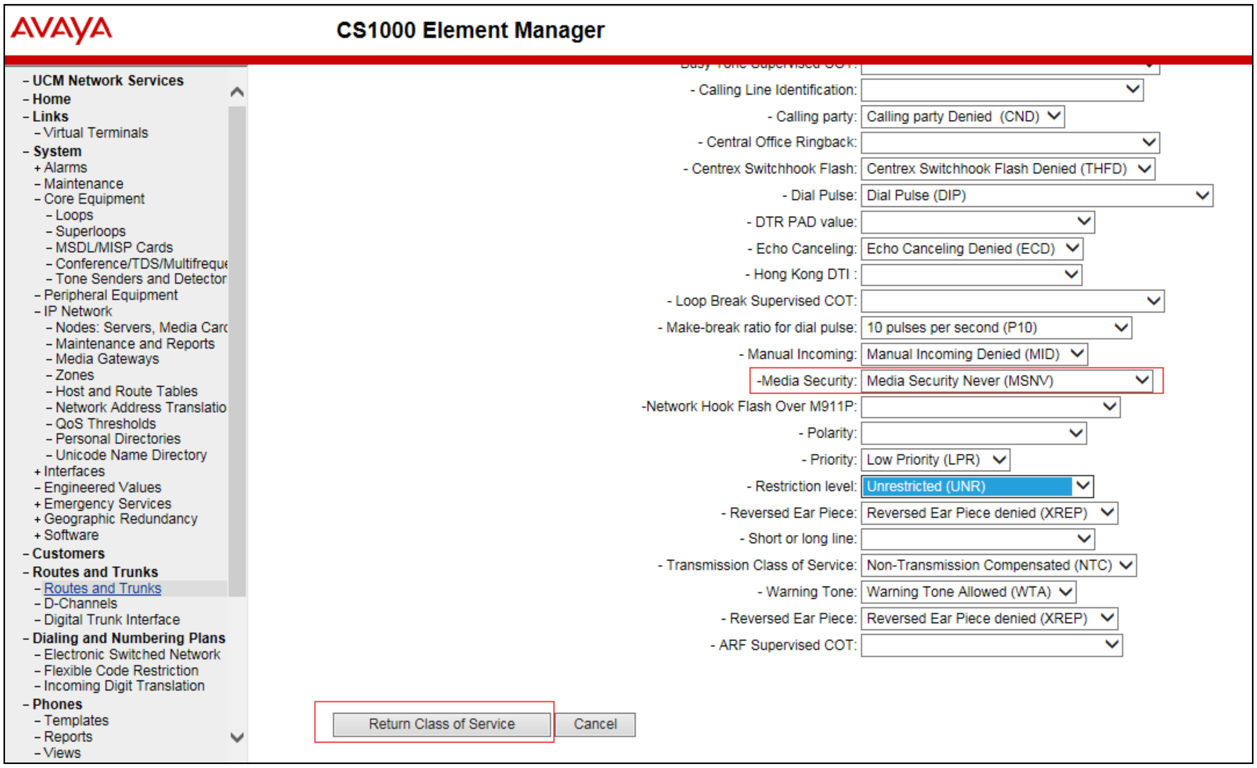
The **Customer 0, Route 10, Trunk type TIE trunk data block** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields. Media Security (sRTP) needs to be disabled at the trunk level by editing the **Class of Service (CLS)** at the bottom of the **Basic Configuration** page. Click on the **Edit** button as shown below.

In the sample configuration, 10 trunks were created.

- **Trunk data block: IP Trunk (IPTI)**.
- **Terminal Number**: available terminal number (**Superloop 100** created in **Section 5.4.4**).
- **Designator field for trunk**: a descriptive text (**sip**).
- **Extended Trunk:** Virtual trunk **(VTRK)**.
- **Member number**: Current route number and starting member.
- **Start arrangement Incoming**: select **Immediate (IMM)**.
- **Start arrangement Outgoing**: select **Immediate (IMM)**.
- **Channel ID for this trunk**: an available starting channel ID.

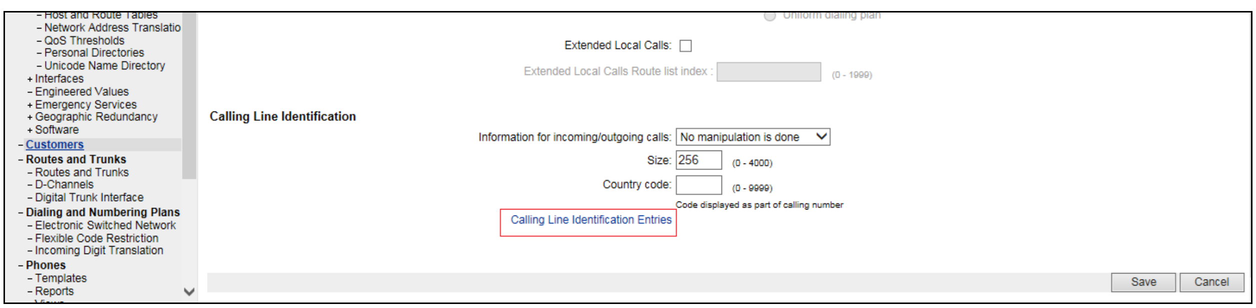


For **Media Security**, select **Media Security Never** (**MSNV)**. Enter the values for the specified fields as shown below. Scroll down to the bottom of the screen and click **Return Class of Service** and then click on the **Save** button.



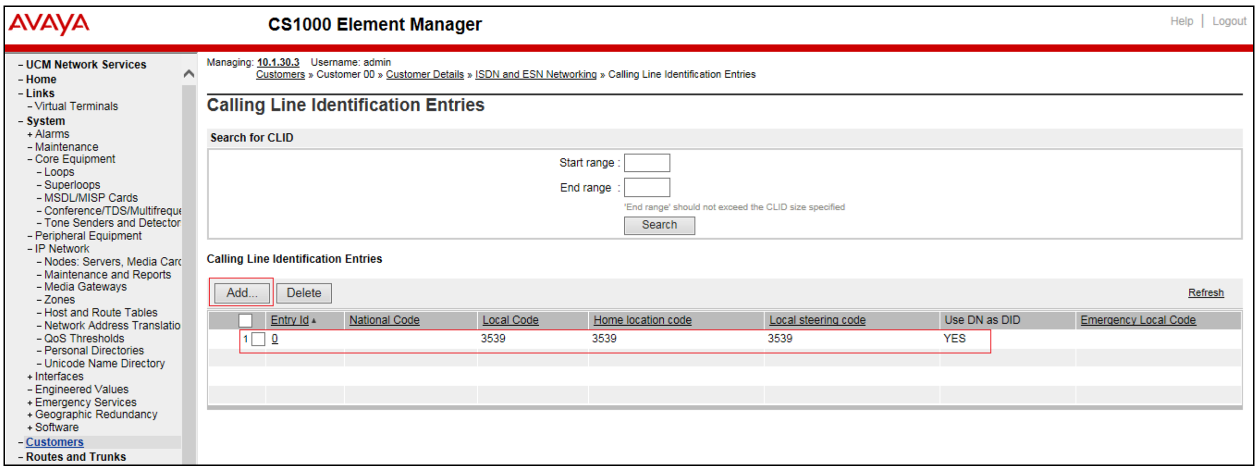
5.4.7 Administer Calling Line Identification Entries

Select **Customers** on the left pane, and then select **00 > ISDN and ESN Networking** (not shown). Click on **Calling Line Identification Entries**:



Click **Add**. The add **entry 0** screen will display. Enter or select the following values for the specified fields and retain the default values for the remaining fields.

- **National Code**: Leave it blank.
- **Local Code**: Input prefix digits assigned by Telstra, in this case 4 digits – **3539**. This Local Code will be used for call display purpose for Call Type = Unknown.
- **Home Location Code**: Input the prefix digits assigned by Telstra, in this case 4 digits – **3539**. This Home Location Code will be used for call display purpose for Call Type = National (NPA).
- **Local Steering Code**: Input prefix digits assigned by Telstra, in this case 4 digits – **3539**. This Local Steering Code will be used for call display purpose for Call Type = Local Subscriber (NXX).
- **Use DN as DID**: **YES**.



5.4.8 Enable External Trunk to Trunk Transfer

External Trunk to Trunk Transfer feature is a mandatory configuration to make call transfer and conference work properly over a SIP trunk.

Access the Call Server Overlay CLI (please refer to **Section 5.1.2** for more details). Allow External Trunk to Trunk Transfer for **Customer Data Block** by using **ld 15**.

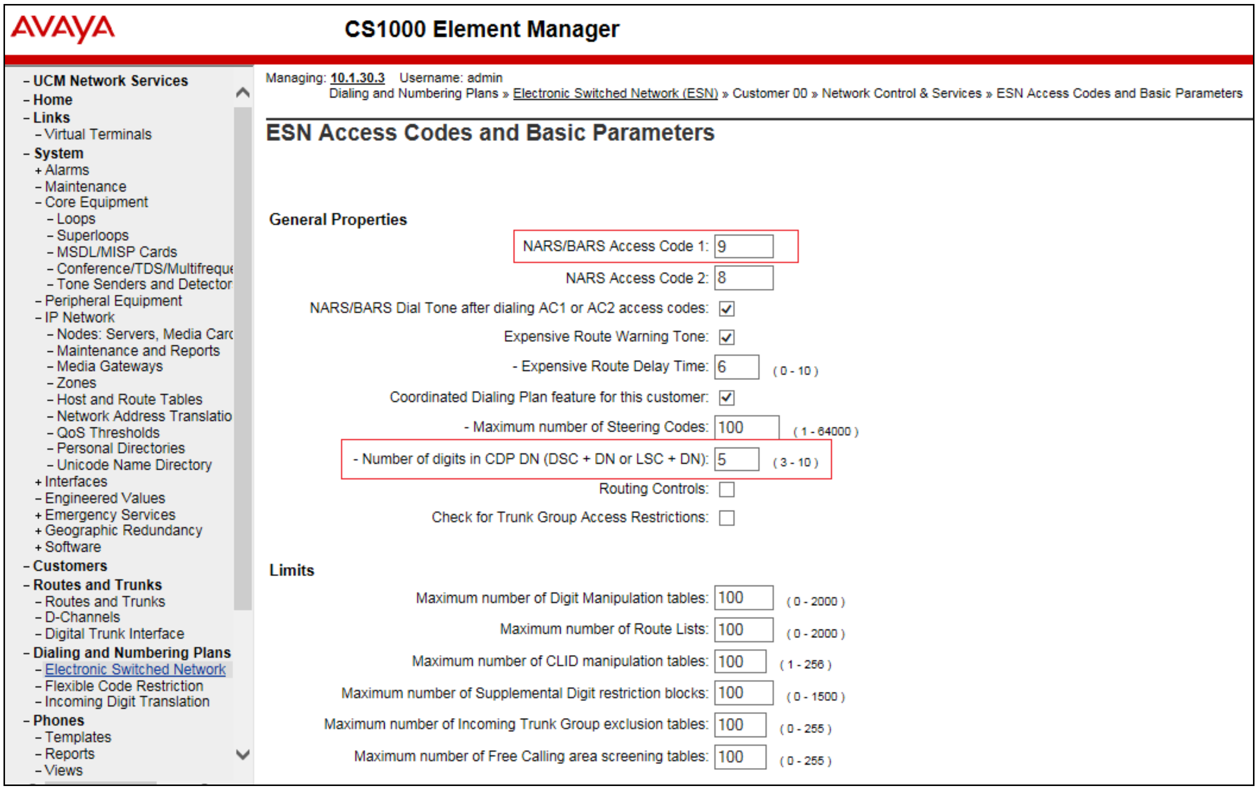
```
>ld 15
CDB000
MEM AVAIL: (U/P): 33600126 USED U P: 8345621 954062 TOT: 45579868
DISK SPACE NEEDED: 1722 KBYTES
REQ: chg
TYPE: net
TYPE NET_DATA
CUST 0
OPT
…
TRNX YES → Enable transfer feature
EXTT YES → Enable external trunk to trunk transfer
…
```

5.5 Administer Dialing Plans

This section describes the steps to configure dialing plans for outbound and inbound calls.

5.5.1 Define ESN Access Codes and Parameters (ESN)

Access the CS1000 Element Manager then select **Dialing and Numbering Plans** > **Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen. Select **ESN Access Codes and Parameters** to define **NARS/BARS Access Code 1** and **Number of digits in CDP DN (DSC+DN or LSC+DN)** as shown below.



5.5.2 Associate NPA and SPN Call to ESN Access Code 1

Access the Call Server CLI, change Customer Net Data block by using **ld 15**. With this setting, NPA and SPN are automatically associated to **ESN Access Code 1**:

```
>ld 15
CDB000
MEM AVAIL: (U/P): 35600086 USED U P: 8325631 954152 TOT: 44879869
DISK SPACE NEEDED: 1722 KBYTES
REQ: chg
TYPE: net
TYPE NET_DATA
CUST 0
OPT
AC2 xNPA xSPN  → Set NPA, SPN not to associate to ESN Access Code 2.
FNP
CLID
…
```

5.5.3 Digit Manipulation Block Index (DMI)

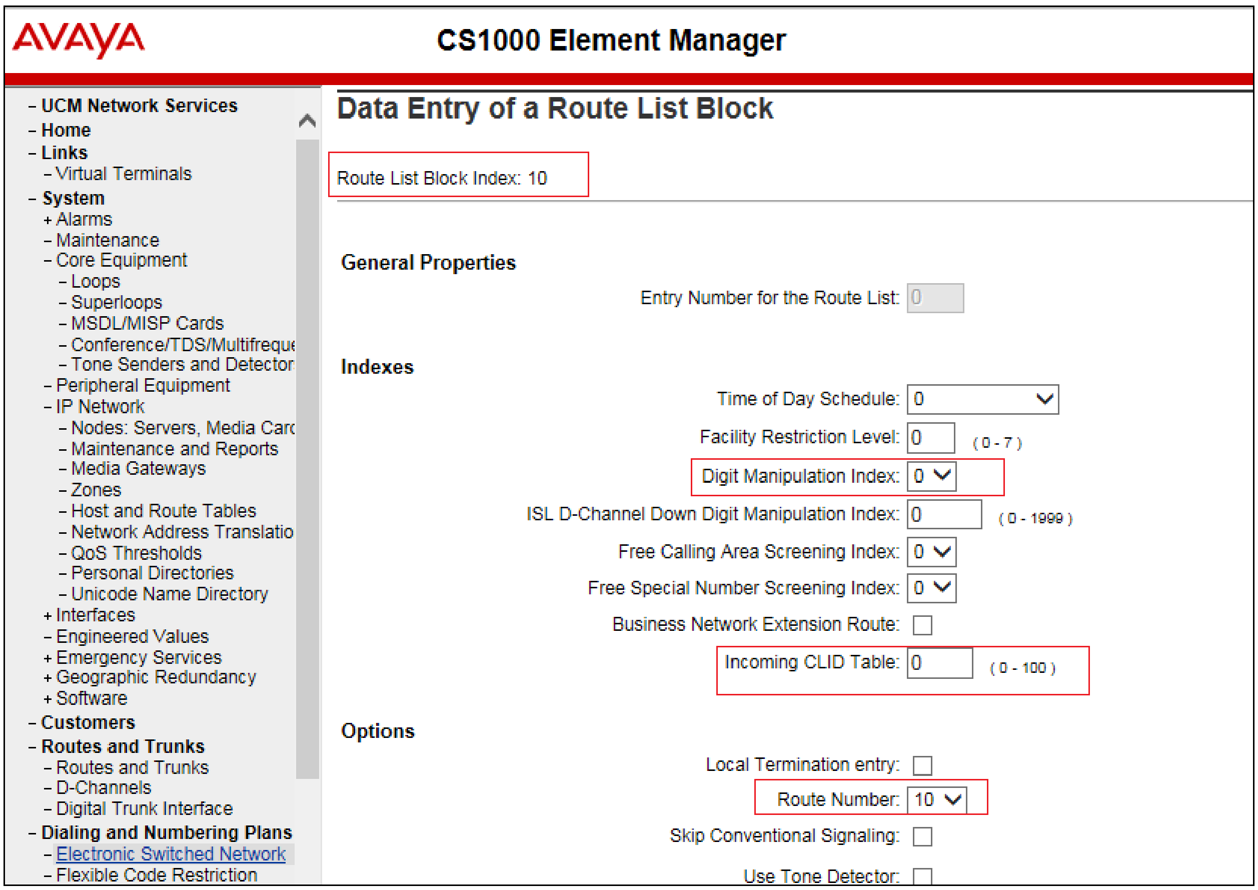
In this sample configuration, there was no digit manipulation required for outbound calls to Telstra so the default **Digit Manipulation Block Index 0** was used.

5.5.4 Route List Block Index

Select **Dialing and Numbering Plans > Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen. Select **Route List Block**. Enter an available value in the textbox for the **Please enter a route list index** (in this example **10**) and click on **Add** (not shown).

Enter the following values for the specified fields, and retain the default values for the remaining fields as shown below.

- Digit Manipulation Index: 0.
- Incoming CLID Table: 0 (created in **Section 5.4.7**).
- Route number: 10 (created in **Section 5.4.5**).



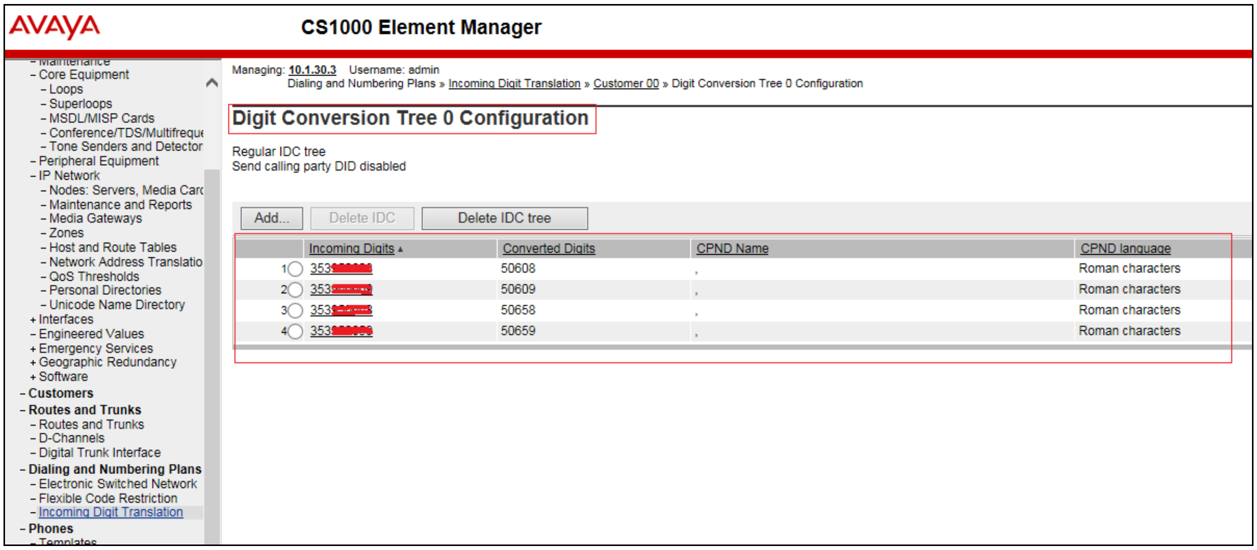
5.5.5 Incoming Digit Translation Configuration

Select **Dialing and Numbering Plans > Incoming Digit Translation** from the left pane to display the **Incoming Digit Translation** screen. Click on the **Edit IDC** button (not shown). Click on the **New DCNO** to create the digit translation mapping. In this example, **Digit Conversion Tree 0** has been previously created (not shown).

Detailed configuration of the **Digit Conversion Tree 0 Configuration** is shown below. The **Incoming Digits** can be added to map to the **Converted Digits** which would be the associated CS1000 system phone DN. This **DCNO** has been configured on **route 10** as shown in **Section 5.4.5**.

In the following configuration, the incoming call from the PSTN to DID with prefix 353xxxxxx will be translated to the associated DN with 5 digits.

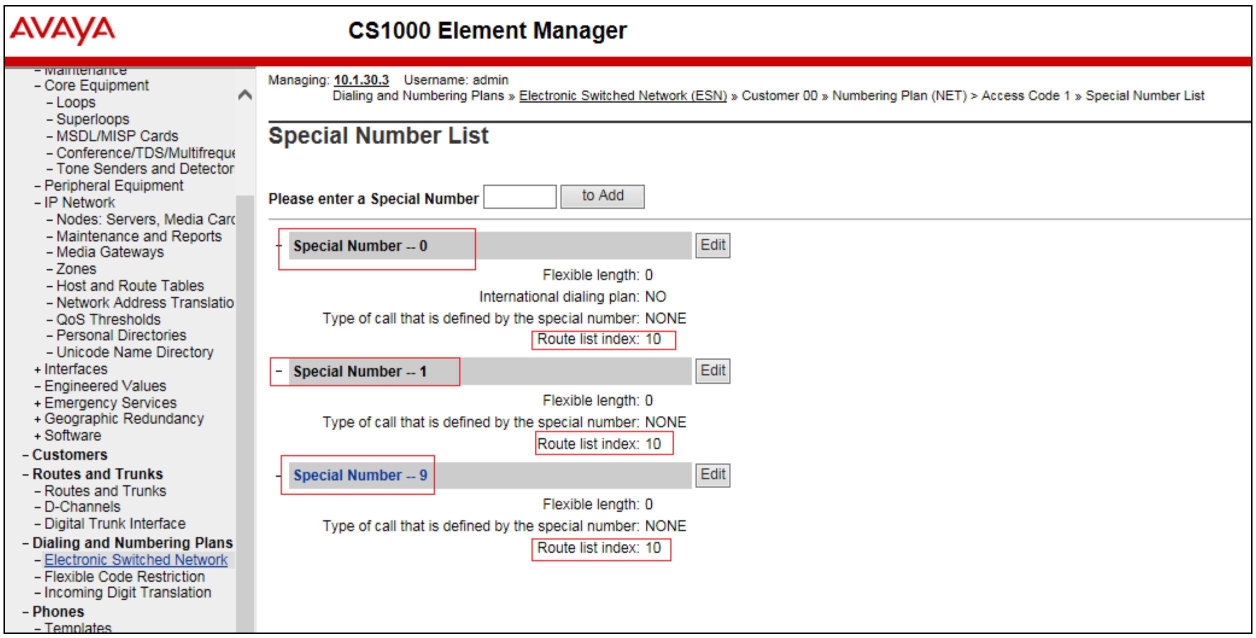
Note: For confidentiality and privacy purposes, the actual 6 remaining digits used for DID numbers in this testing have been masked.



5.5.6 Outbound Call - Special Number Configuration

There are special numbers which have been configured to be used for this testing such as: **0**, **1** and **9**. These special numbers were associated to **Route list index 10** created in **Section 5.5.4**.

Select **Dialing and Numbering Plans > Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen. Select **Special Number (SPN)**. Enter a SPN number and then click on **Add** button. Below figure shows all the special numbers used for this testing.



5.6 Enable Plug-ins on CS1000

In order for off-net call transfer to operate successfully, **plug-in 201** and **plug-in 501** must be enabled on CS1000. Please refer to **CS1000 Plug-in Feature** document which is available at https://downloads.avaya.com/css/P8/documents/100166144 .

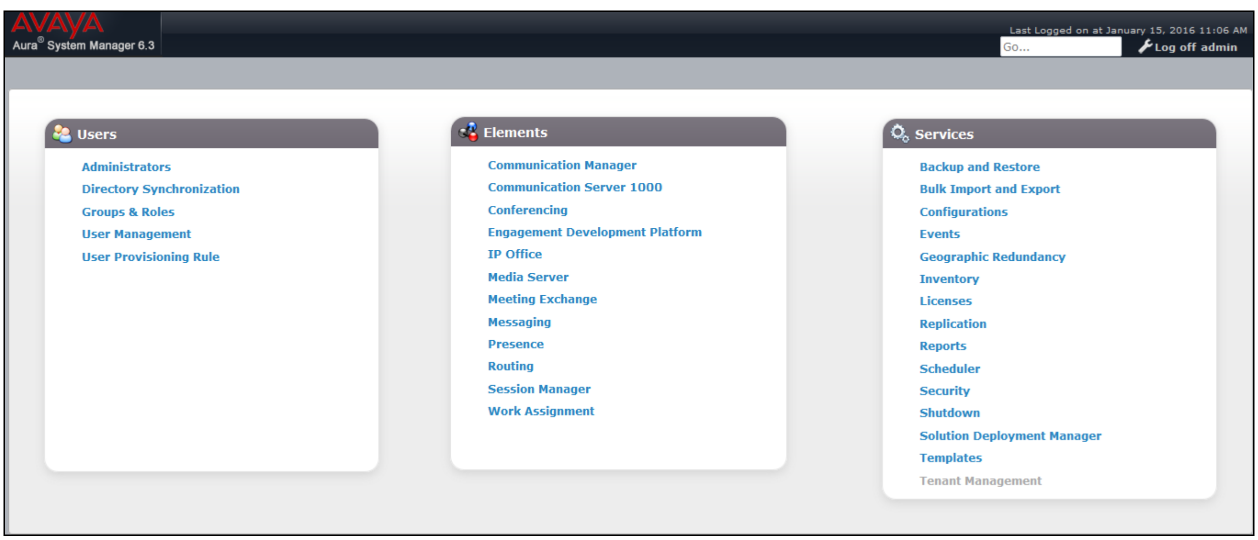
6. Configure Avaya Aura® Session Manager

This section provides the procedures for configuring Session Manager. The procedures include adding the following items:

- SIP domain.
- Adaptations
- Logical/physical Location that can be used by SIP Entities.
- SIP Entities corresponding to CS1000, Session Manager and the Avaya SBCE.
- Entity Links, which define the SIP trunk parameters used by Session Manager when routing calls to/from SIP Entities.
- Routing Policies, which control call routing between the SIP Entities.
- Dial Patterns, which govern to which SIP Entity a call is routed.
- Session Manager, corresponding to the Session Manager server to be managed by System Manager.

It may not be necessary to configure 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.

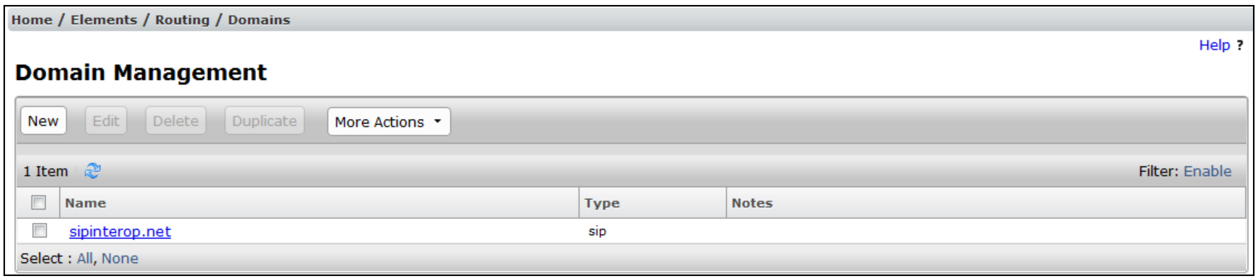
Session Manager configuration is accomplished by accessing the browser-based GUI of System Manager, using the URL **http://<ip-address>/SMGR,** where **<ip-address>** is the IP address of System Manager. In the **Log On** screen (not shown), enter appropriate **User ID** and **Password** and press the **Log On** button. Once logged in, the **Home** screen is displayed. From the **Home** screen, under the **Elements** heading in the center, select **Routing**.



6.1 Configure SIP Domain

Follow the steps shown below:

1. Select **Domains** from the left navigation menu. In the reference configuration, domain **sipinterop.net** was defined.
2. Click **New** (not shown). Enter the following values and use default values for remaining fields.
   - **Name**: enter the enterprise SIP Domain Name. In the sample screen below, **sipinterop.net** is shown.
   - **Type**: verify **sip** is selected.
   - **Notes**: add a brief description.
3. Click **Commit** to save (not shown).

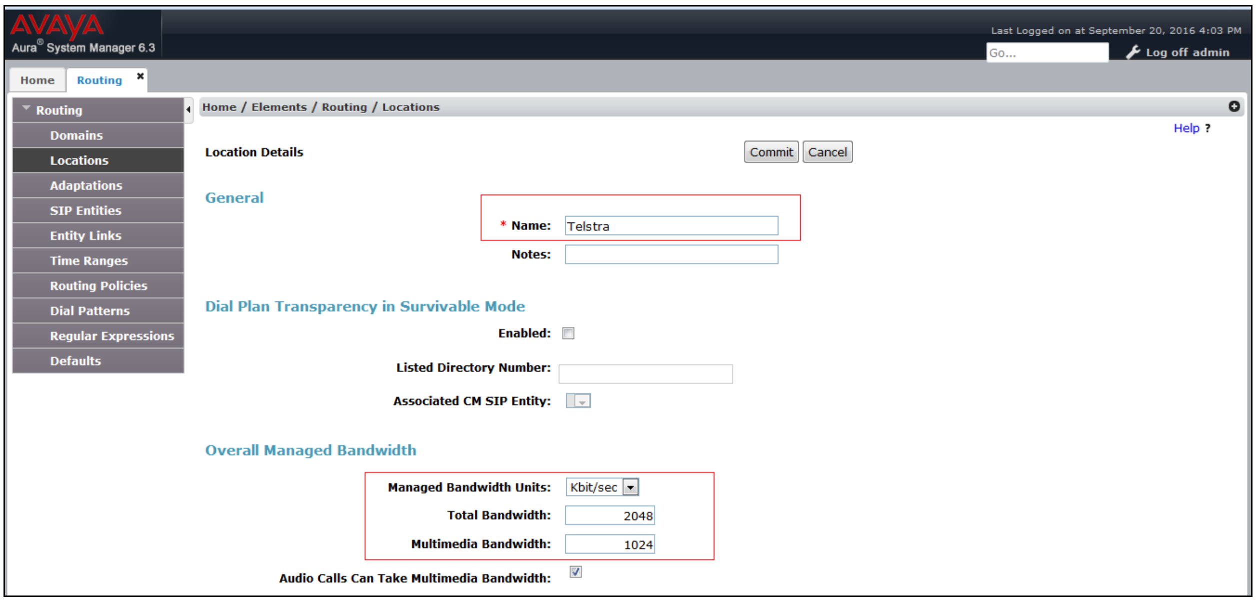


6.2 Configure Locations

Locations are used to identify logical and/or physical locations where SIP Entities reside. In the reference configuration, location **Telstra** is configured.

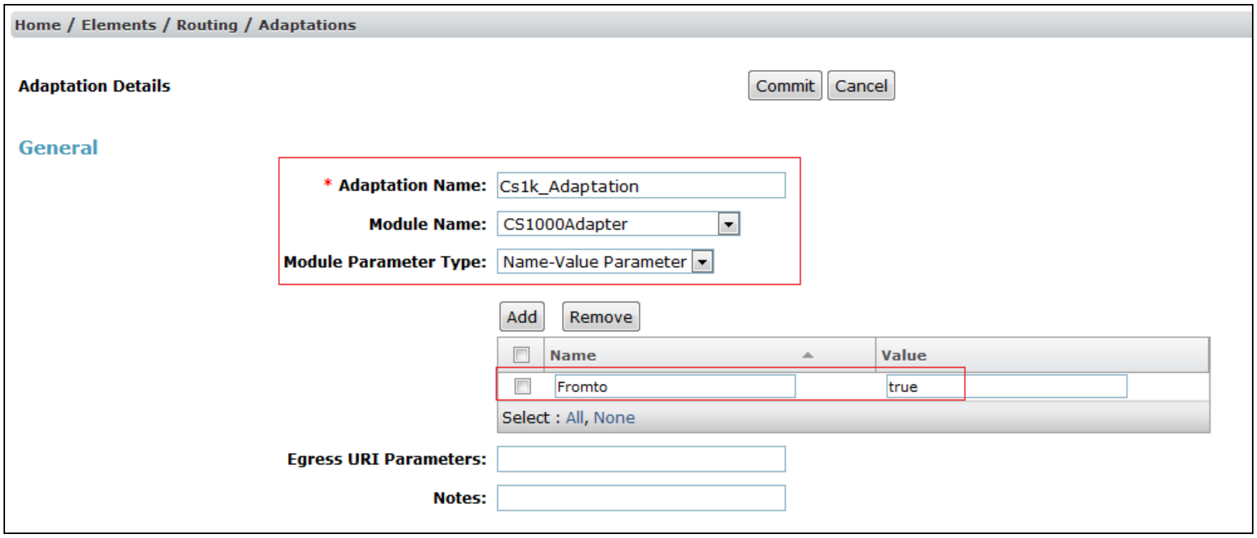
Follow the steps shown below:

1. Select **Locations** from the left navigational menu. Click **New** (not shown). In the **General** section, enter the following values and use default values for remaining fields.
   - **Name**: enter a descriptive name for the Location (e.g., **Telstra**).
   - **Notes**: add a brief description.
2. In the **Overall Managed Bandwidth** section:
   - **Total Bandwidth**: enter a desired value (e.g., **2048**).
   - **Multimedia Bandwidth**: enter a desired value (e.g., **1024**).
3. Click **Commit** to save.

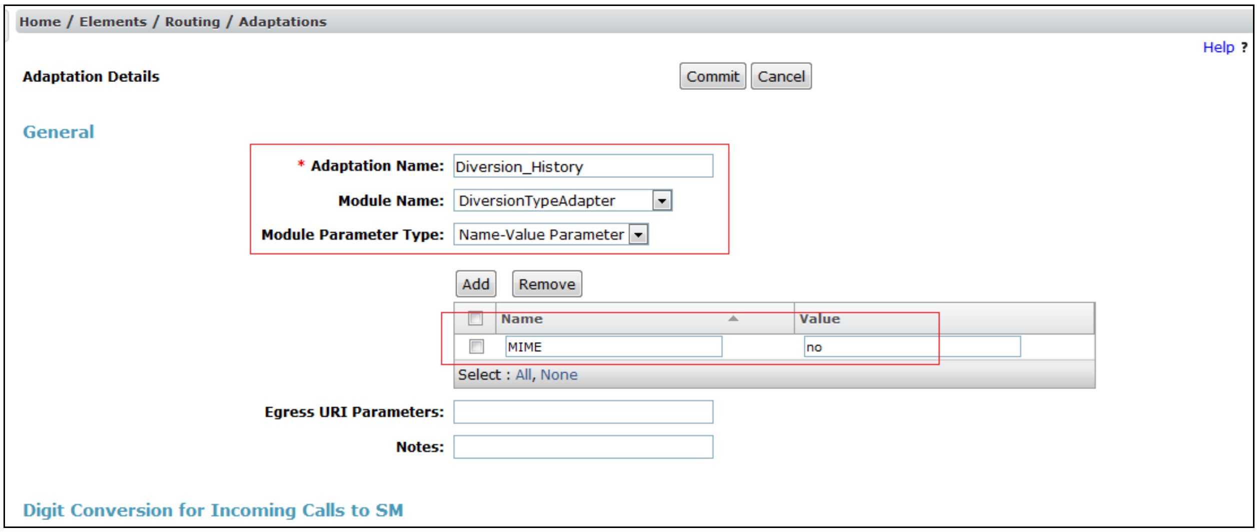


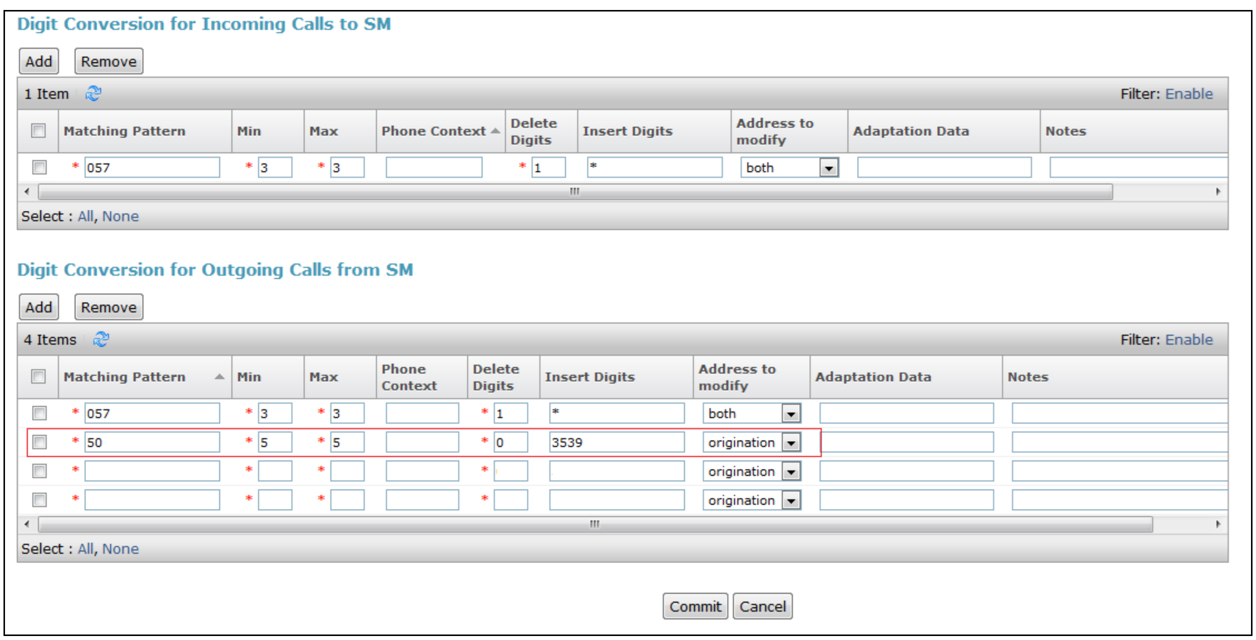
6.3 Configure Adaptations

An Adaptation was configured to format the History Info on CS1000 to be compatible with other Avaya products. To add a new Adaptation, select **Routing > Adaptations**. Click the **New** button in the right pane (not shown). Enter an appropriate **Adaptation Name** to identify the Adaptation. Select **CS1000Adapter** from the **Module Name** drop-down menu. Select **Name-Value Parameter** from the **Module Parameter Type** drop-down menu. Click **Add** button to add **Name** as **Fromto** and **Value** as **true**. Click the **Commit** button after changes are completed.



Another Adaptation was configured to convert the **History Info** to **Diversion Header** and to remove **MIME**. To add a new Adaptation, select **Routing > Adaptations**. Click the **New** button in the right pane (not shown). Enter an appropriate **Adaptation Name** to identify the Adaptation. Select **DiversionTypeAdapter** from the **Module Name** drop-down menu. Select **Name-Value Parameter** from the **Module Parameter Type** drop-down menu. Click **Add** button to add **Name** as **MIME** and **Value** as **no**. Scroll down to **Digit Conversion for Outgoing Calls from SM** to add a record so that **From** header of **INVITE** sent to Telstra has DID numbers assigned by Telstra. Click the **Commit** button after changes are completed.





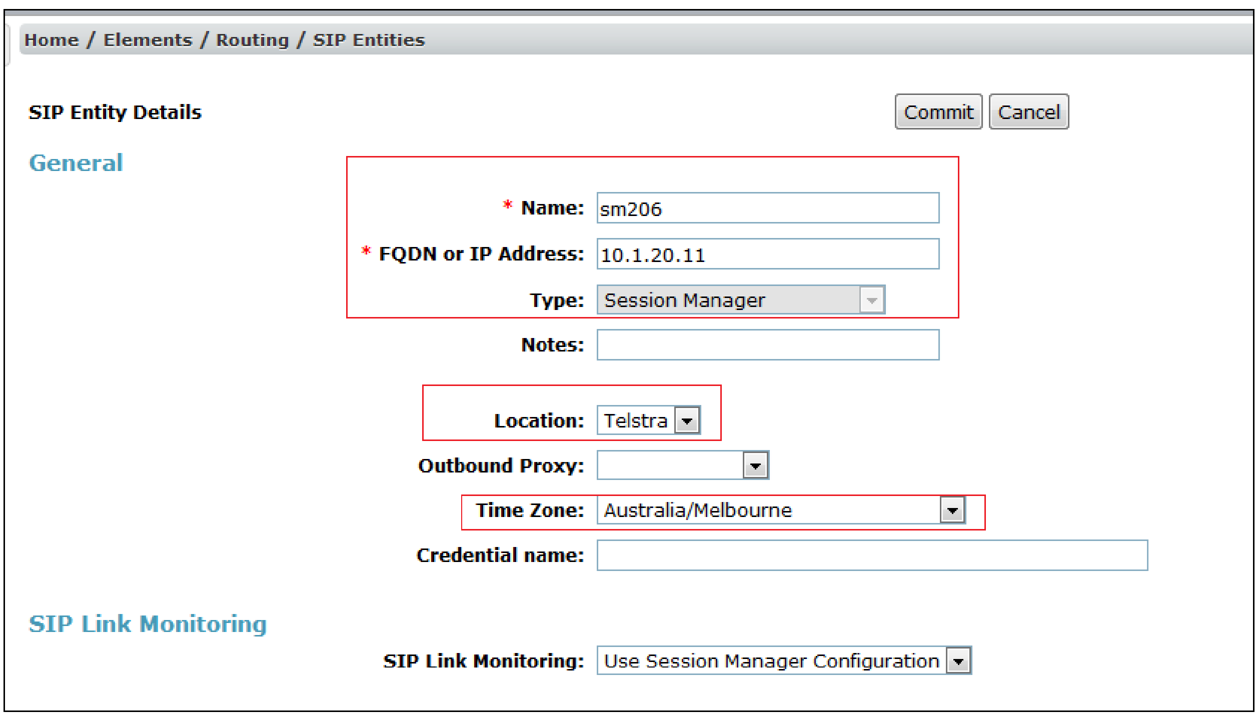
6.4 Configure SIP Entities

A SIP Entity must be added for Session Manager and for each SIP telephony system connected to it which includes CS1000 and Avaya SBCE.

6.4.1 Configure Session Manager SIP Entity

Follow the steps shown below:

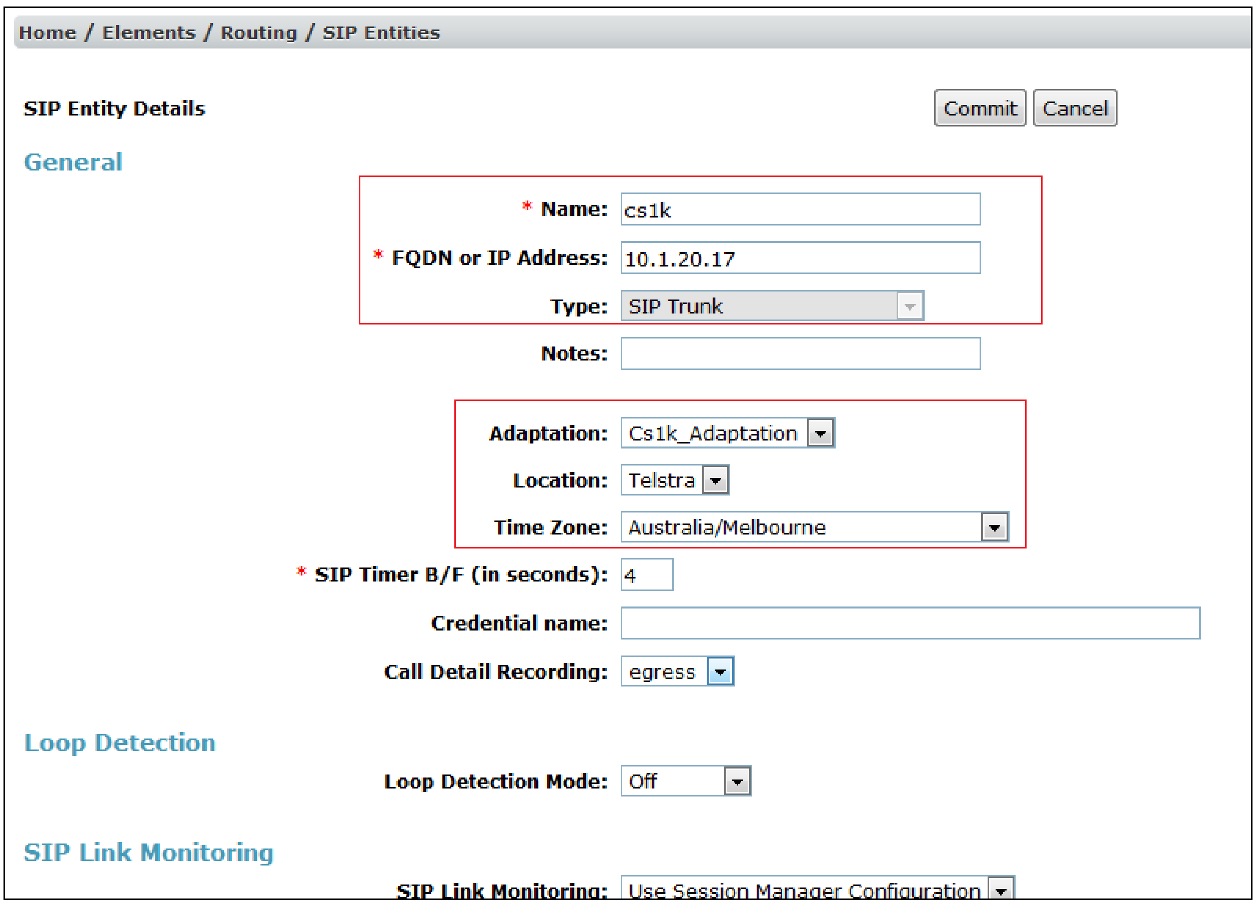
1. In the left pane under **Routing**, click on **SIP Entities**. In the **SIP Entities** page, click on **New** (not shown).
2. In the **General** section of the **SIP Entity Details** page, provision the following:
   - **Name –** Enter a descriptive name (e.g., **sm206**).
   - **FQDN or IP Address –** Enter the IP address of Session Manager signaling interface, (*not* the management interface), provisioned during installation (e.g., **10.1.20.11**).
   - **Type –** Verify **Session Manager** is selected.
   - **Location** – Select location **Telstra.**
   - **Outbound Proxy** – (Optional) Leave blank or select another SIP Entity. For calls to SIP domains for which Session Manager is not authoritative, Session Manager routes those calls to this **Outbound Proxy** or to another SIP proxy discovered through DNS if **Outbound Proxy** is not specified.
   - **Time Zone** – Select the time zone in which Session Manager resides.
3. In the **SIP Monitoring** section of the **SIP Entity Details** page, configure as follows:
   - Select **Use Session Manager Configuration** for **SIP Link Monitoring** field.
   - Use the default values for the remaining parameters.



6.4.2 Configure CS1000 SIP Entity

Follow the steps shown below:

1. In the **SIP Entities** page, click on **New** (not shown).
2. In the **General** section of the **SIP Entity Details** page, provision the following:
   - **Name** – Enter a descriptive name (e.g. **cs1k**).
   - **FQDN or IP Address –** Enter the IP address of CS1000 Node IP as in **Section 5.2.1** (e.g., **10.1.20.17**).
   - **Type –** Select **SIP Trunk**.
   - **Adaptation** – Select **Cs1k_Adaptation** created in **Section 6.3**.
   - **Location** – Select Location **Telstra** administered in **Section 6.2**.
   - **Time Zone** – Select the time zone in which CS1000 resides.
   - In the **SIP Link Monitoring** section of the **SIP Entity Details** page select:
     - Select **Use Session Manager Configuration** for **SIP Link Monitoring** field, and use the default values for the remaining parameters.
3. Click on **Commit**.

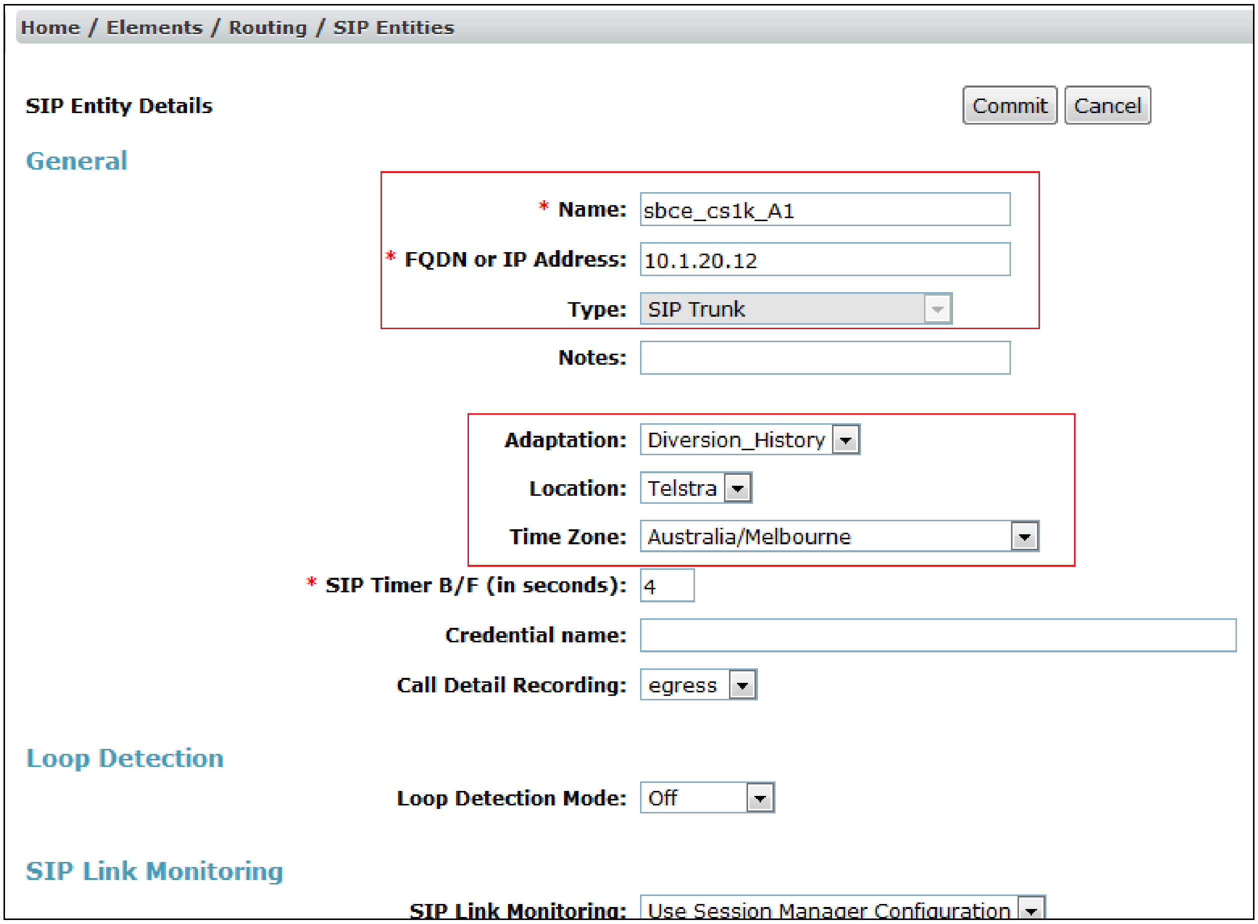


6.4.3 Configure Avaya SBCE SIP Entity

Repeat the steps in **Section 6.4.2** with the following changes:

- **Name –** Enter a descriptive name (e.g., **sbce_cs1k_A1**).

- **FQDN or IP Address –** Enter the IP address of the A1 (private) interface of the Avaya SBCE (e.g., **10.1.20.12**).
- **Adaptation** – Select **Diversion_History** created in **Section 6.3**.



6.5 Configure Entity Links

A SIP trunk between Session Manager and a telephony system is described by an Entity Link. During compliance testing, two Entity Links were created, one for CS1000 and another one for Avaya SBCE. To add an Entity Link, navigate to **Routing → Entity Links** in the left navigation pane and click **New** button in the right pane (not shown). Fill in the following fields in the new row that is displayed:

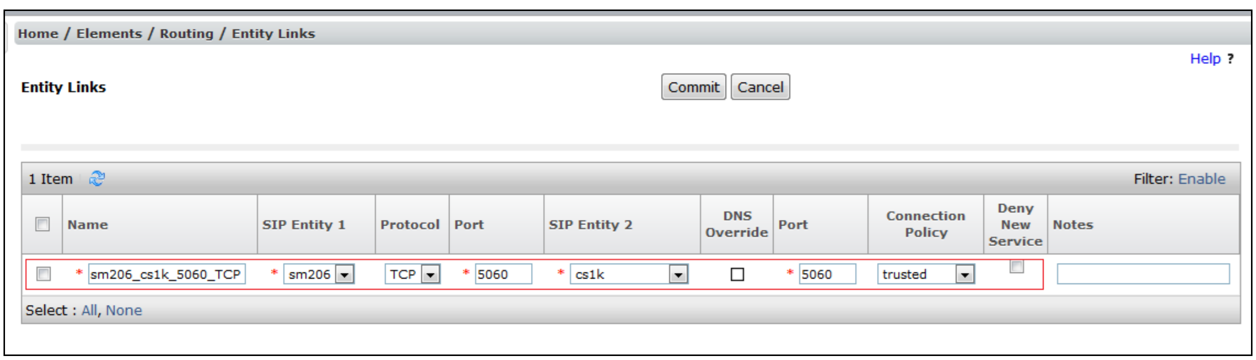
- **Name:** Enter a descriptive name.
- **SIP Entity 1:** Select the Session Manager defined in **Section 6.4.1**.
- **Protocol:** Select the transport protocol used for this link, ***TCP*** for the Entity Link to CS1000 and the Avaya SBCE.
- **Port:** Port number on which Session Manager will receive SIP requests from the far-end. **SIP Entity 2:** Select the name of the other systems. For CS1000, select the CS1000 SIP Entity defined in **Section 6.4.2**. For Avaya SBCE, select Avaya SBCE SIP Entity defined in **Section 6.4.3**.

- **Port:** Port number on which the other system receives SIP requests from Session Manager. For Communication Manager, this must match the **Near-end Listen Port** defined on the Communication Manager.
- **Connection Policy:** Select **Trusted**.
- Click **Commit** to save.

6.5.1 Configure Entity Link to CS1000

Follow the steps shown below:

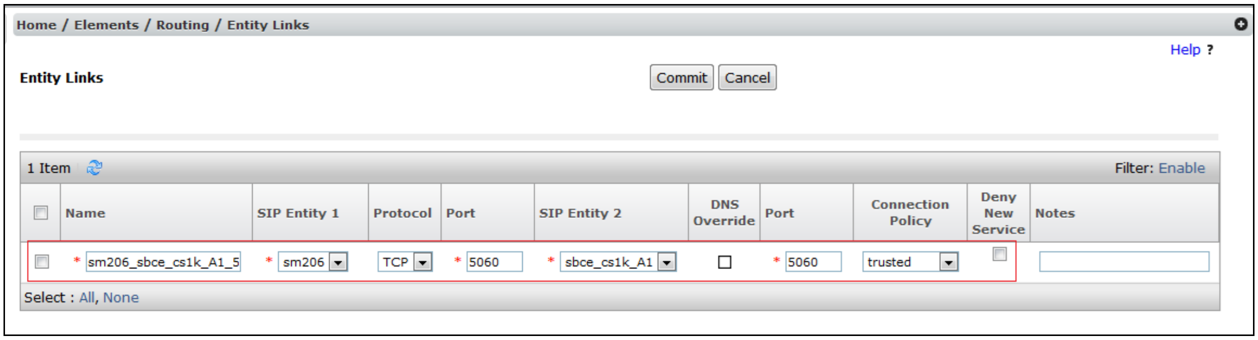
1. In the left pane under **Routing**, click on **Entity Links**, then click on **New** button (not shown).
2. Continuing in the **Entity Links** page, provision the following:
   - **Name** – Enter a descriptive name (or have it created automatically) for this link to CS1000 (e.g., **sm206_cs1k_5060_TCP**).
   - **SIP Entity 1** – Select the SIP Entity administered in **Section 6.4.1** for Session Manager (e.g., **sm206**).
   - **SIP Entity 1 Port** – Enter **5060**.
   - **Protocol – ** Select **TCP.**
   - **SIP Entity 2** –Select the SIP Entity administered in **Section 6.4.2** for the CS1000 entity (e.g., **cs1k**).
   - **SIP Entity 2 Port** - Enter **5060.**
   - **Connection Policy** – Select **Trusted**.
3. Click on **Commit**.



6.5.2 Configure Entity Link for Avaya SBCE

To configure this Entity Link, repeat the steps in **Section 6.5.1**, with the following changes:

- **Name** – Enter a descriptive name (or have it created automatically) for this link to the Avaya SBCE (e.g., **sm206_sbce_cs1k_A1_5060_TCP**).
- **SIP Entity 2** – Select the SIP Entity administered in **Section 6.4.3** for the Avaya SBCE entity (e.g., **sbce_cs1k_A1**).



6.6 Configure Routing Policies

Routing Policies describe the conditions under which calls will be routed to the SIP Entities specified in **Section 6.5**. Two routing policies were added, one for CS1000 and another one for Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left navigation pane and click **New** button in the right pane (not shown).

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

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

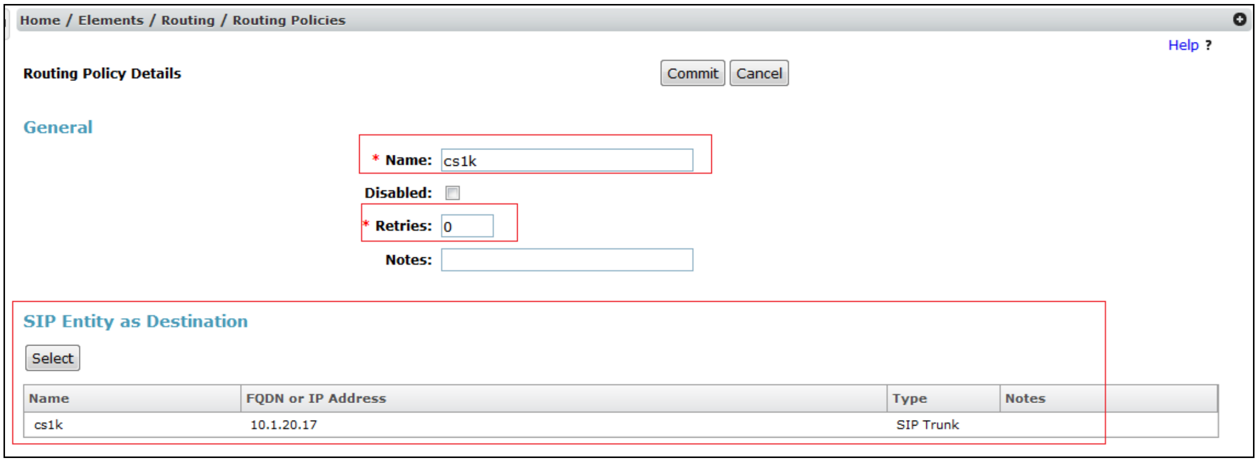
In the **SIP Entity as Destination** section, click **Select.** The **SIP Entity List** page opens (not shown). Select appropriate SIP entity to which this routing policy applies and click **Select**. The selected SIP Entity is displayed in the **Routing Policy Details** page as shown below. Use default values for remaining fields. Click **Commit** to save.

6.6.1 Configure Routing Policy for CS1000

This Routing Policy was used for inbound calls from Telstra.

1. In the left pane under **Routing**, click on **Routing Policies**. In the **Routing Policies** page click on **New** button (not shown).
2. In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** for routing calls from Telstra to CS1000 (e.g., **cs1k**), and ensure that the **Disabled** checkbox is unchecked to activate this Routing Policy.
3. **Retries**: **0**.
4. In the **SIP Entity as Destination** section of the **Routing Policy Details** page, click on **Select** and the SIP Entity list page will open.
5. In the **SIP Entity List** page, select the SIP Entity administered in **Section 6.3.2** for the CS1000 SIP Entity (**cs1k**), and click on **Select**.

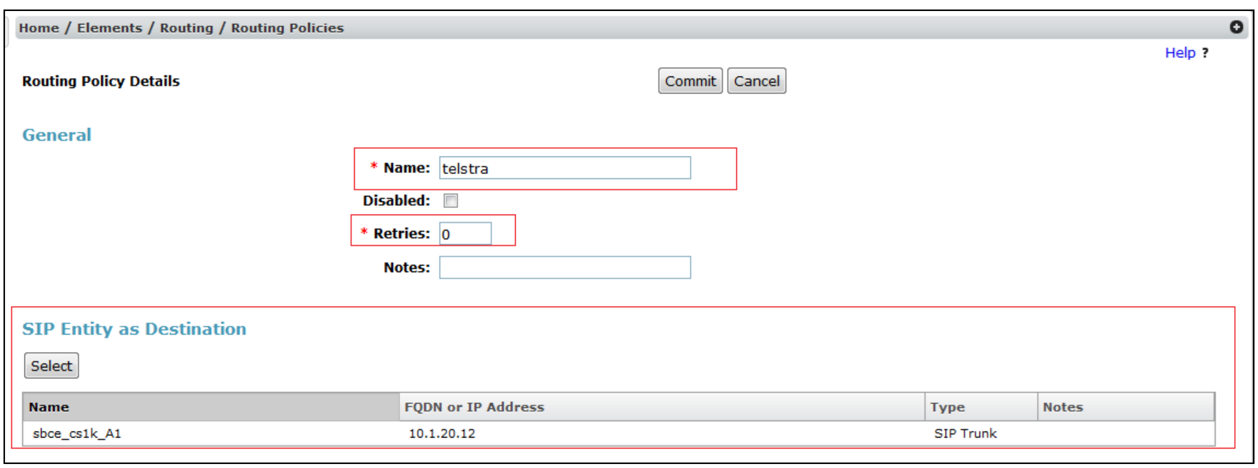
6. Note that once the **Dial Patterns** are defined they will appear in the **Dial Pattern** section of this form.
7. No **Regular Expressions** were used in the reference configuration.
8. Click on **Commit**.



6.6.2 Configure Routing Policy for Avaya SBCE

This Routing Policy is used for outbound calls to the service provider. Repeat the steps in **Section 6.6.1**, with the following changes:

- **Name** – Enter a descriptive name for this link to the Avaya SBCE (e.g., **telstra**).
- **SIP Entity List** –Select the SIP Entity administered in **Section 6.4.3** for the Avaya SBCE entity (e.g., **sbce_cs1k_A1**).



6.7 Configure Dial Patterns

Dial Patterns are needed to route specific calls through Session Manager. For the compliance testing, dial patterns were needed to route calls from CS1000 to Telstra and vice versa. Dial Patterns define which routing policy will be selected for a particular call based on the dialed digits, destination domain and originating location. To add a dial pattern, navigate to **Routing → Dial Patterns** in the left navigation pane and click **New** button in the right pane (not shown).

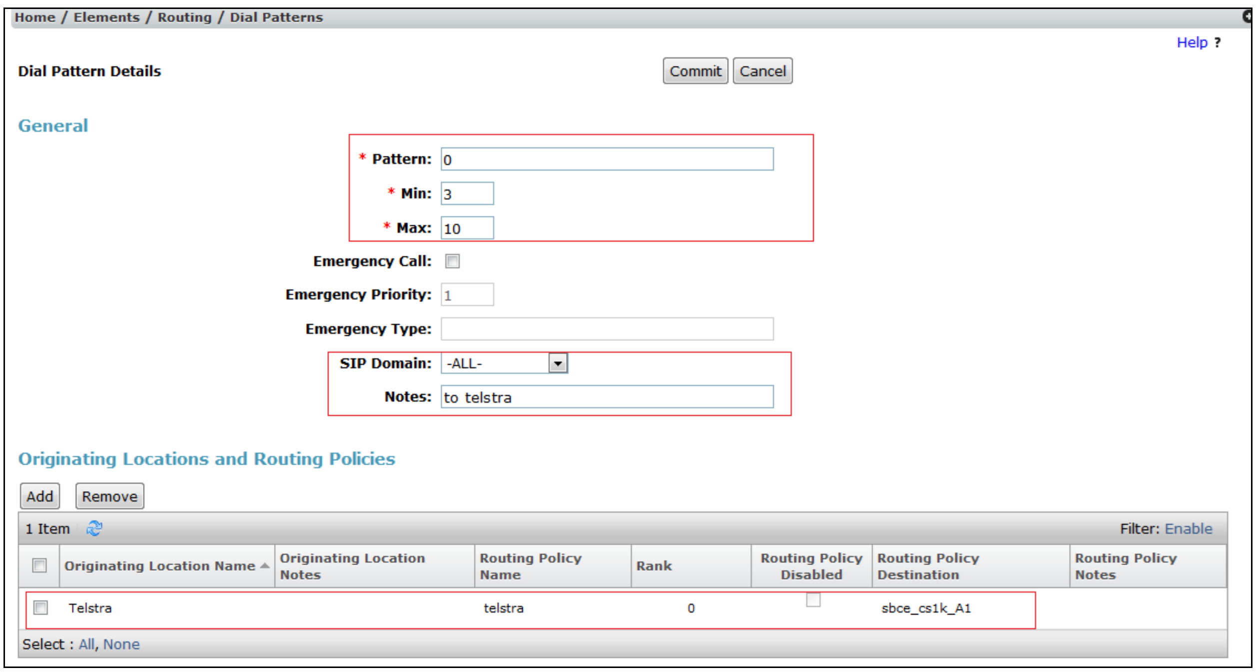
In the **General** section, enter the following values:

- **Pattern:** Enter a dial string that will be matched against the “Request-URI” of the call.
- **Min:** Enter a minimum length used in the match criteria.
- **Max:** Enter a maximum length used in the match criteria.
- **SIP Domain:** Enter the destination domain used in the match criteria.
- **Notes:** Add a brief description (optional).

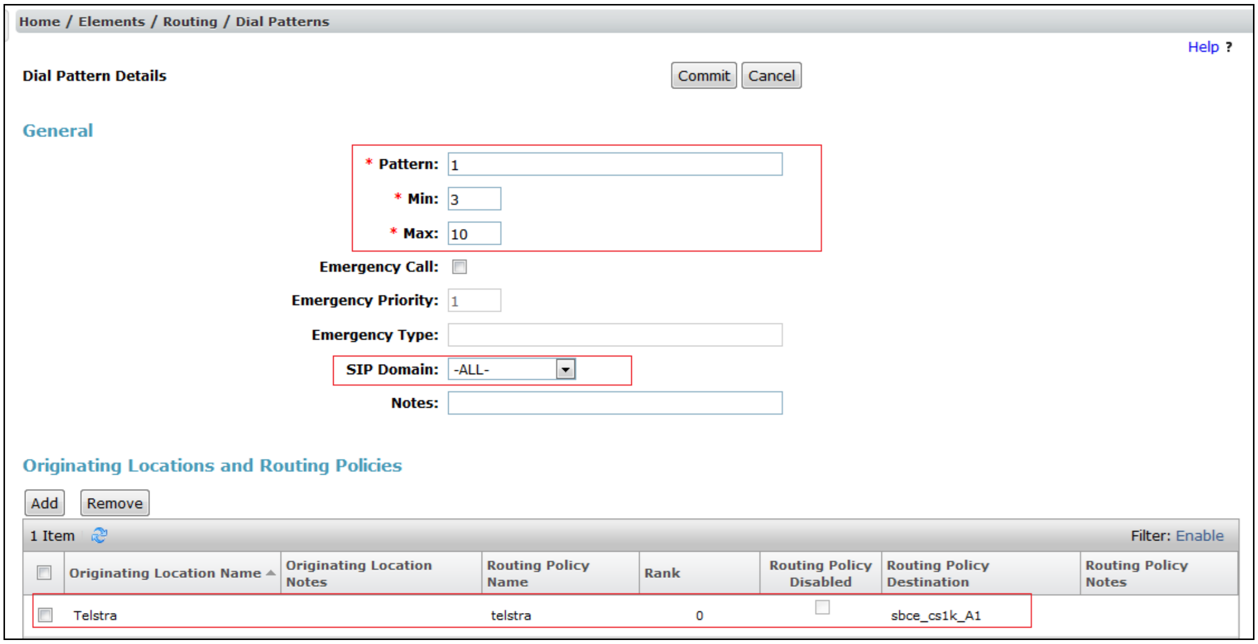
In the **Originating Locations and Routing Policies** section, click **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria. Lastly, select the routing policy from the list that will be used to route all calls that match the specified criteria. Click **Select**.

Default values can be used for the remaining fields. Click **Commit** to save.

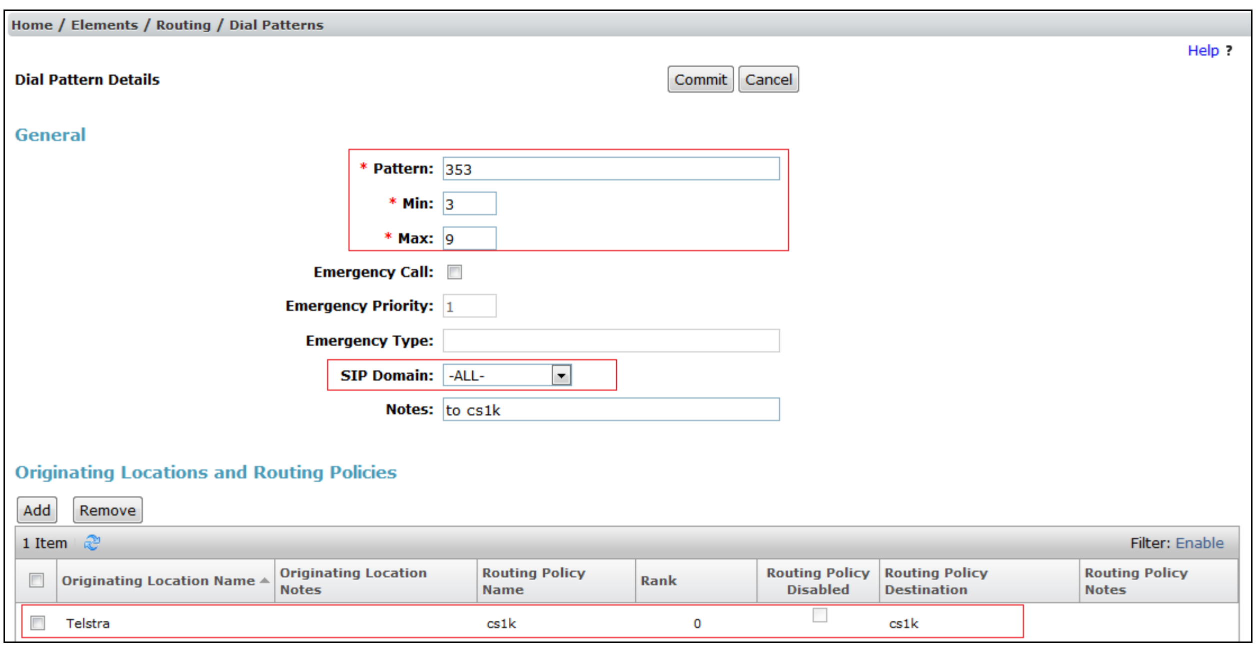
The first example shows that 3-digit to 10-digit dialed numbers that begin with 0 and have a destination domain of “All” uses route policy to Telstra as defined in **Section 6.6.2**



The second example shows that outbound 3-digit to 10-digit numbers that start with 1 uses route policy to Telstra as defined in **Section 6.6.2** for calls to 1800/1900 service numbers**.**



The third example shows that 3 to 9 digit pattern that start with 353 is used for inbound calls from Telstra to DID numbers on CS1000.



7. Configure Avaya Session Border Controller for Enterprise

Note: The installation and initial provisioning of the Avaya SBCE is beyond the scope of this document.

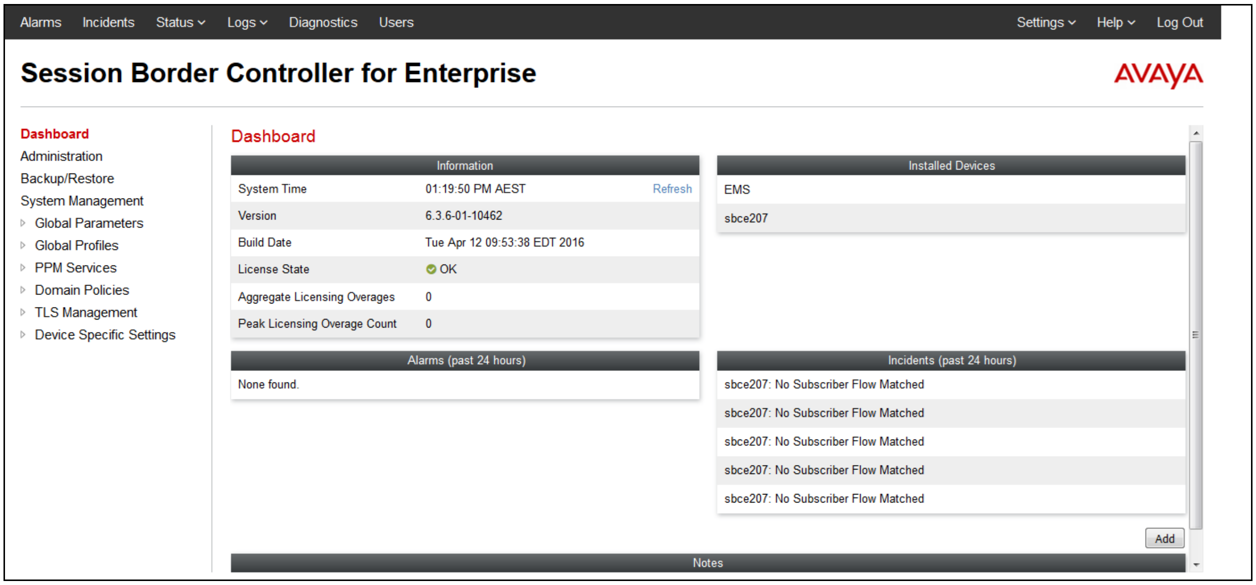
IMPORTANT! – During the Avaya SBCE installation, the Management interface of the Avaya SBCE must be provisioned on a different subnet than either of the Avaya SBCE private and public network interfaces (e.g., A1 and B1).

As described in **Section 3**, the reference configuration places the private interface (A1) of the Avaya SBCE in the enterprise site (10.1.20.12). The connection to Telstra uses the Avaya SBCE public interface B1 (IP address 10.2.2.21). The follow provisioning is performed via the Avaya SBCE GUI interface, using the "M1" management LAN connection on the chassis.

1. Access the web interface by typing "**https://x.x.x.x**" (where x.x.x.x is the management IP address of the Avaya SBCE).
2. Enter the **Username** and click on **Continue**.

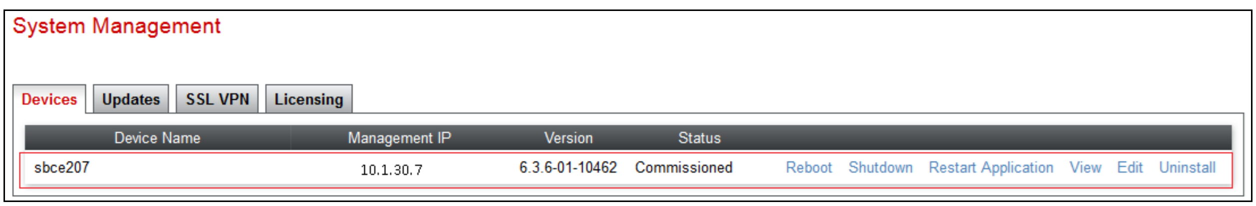
3. Enter the password and click on **Log In**.

The main menu window will open. Note that the installed software version is displayed. Verify that the **License State** is **OK**. The SBCE will only operate for a short time without a valid license. Contact your Avaya representative to obtain a license.

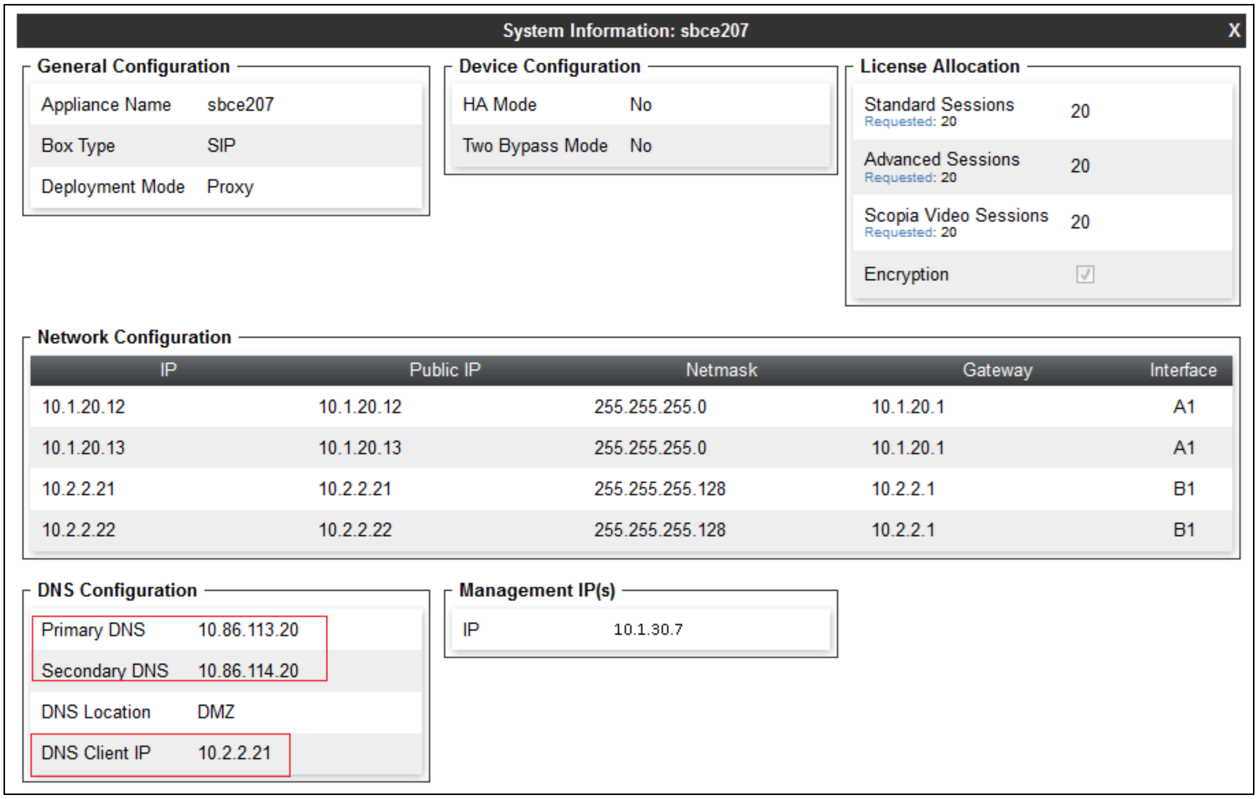


7.1 System Management – Status

1. Select **System Management** and verify that the **Status** column says **Commissioned**. If not, contact your Avaya representative.



2. Click on **View** (shown above) to display the **System Information** screen. Note that the DNS servers are Telstra DNS servers and the DNS client must be the B1 IP address that is used for the SIP trunk with Telstra.



7.2 Global Profiles

The Global Profiles Menu, on the left navigation pane, allows the configuration of parameters across all Avaya SBCE appliances.

7.2.1 Uniform Resource Identifier (URI) Groups

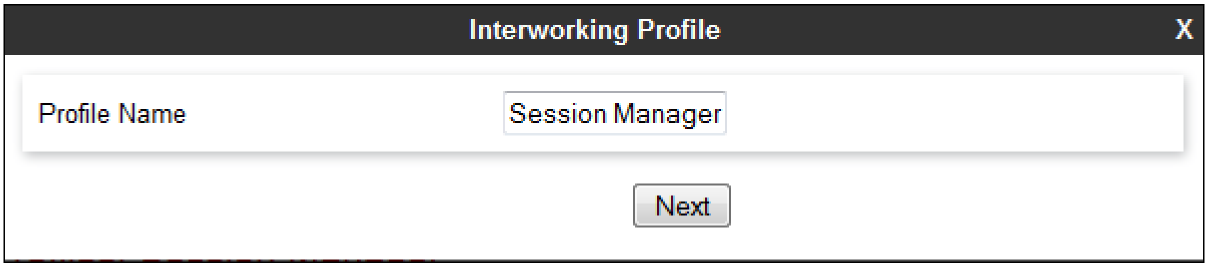
URI Group feature allows a user to create any number of logical URI Groups that are comprised of individual SIP subscribers located in that particular domain or group. These groups are used by the various domain policies to determine which actions (Allow, Block, or Apply Policy) should be used for a given call flow.

For this configuration testing, “*” is used for all incoming and outgoing traffic.

7.2.2 Server Interworking – Session Manager

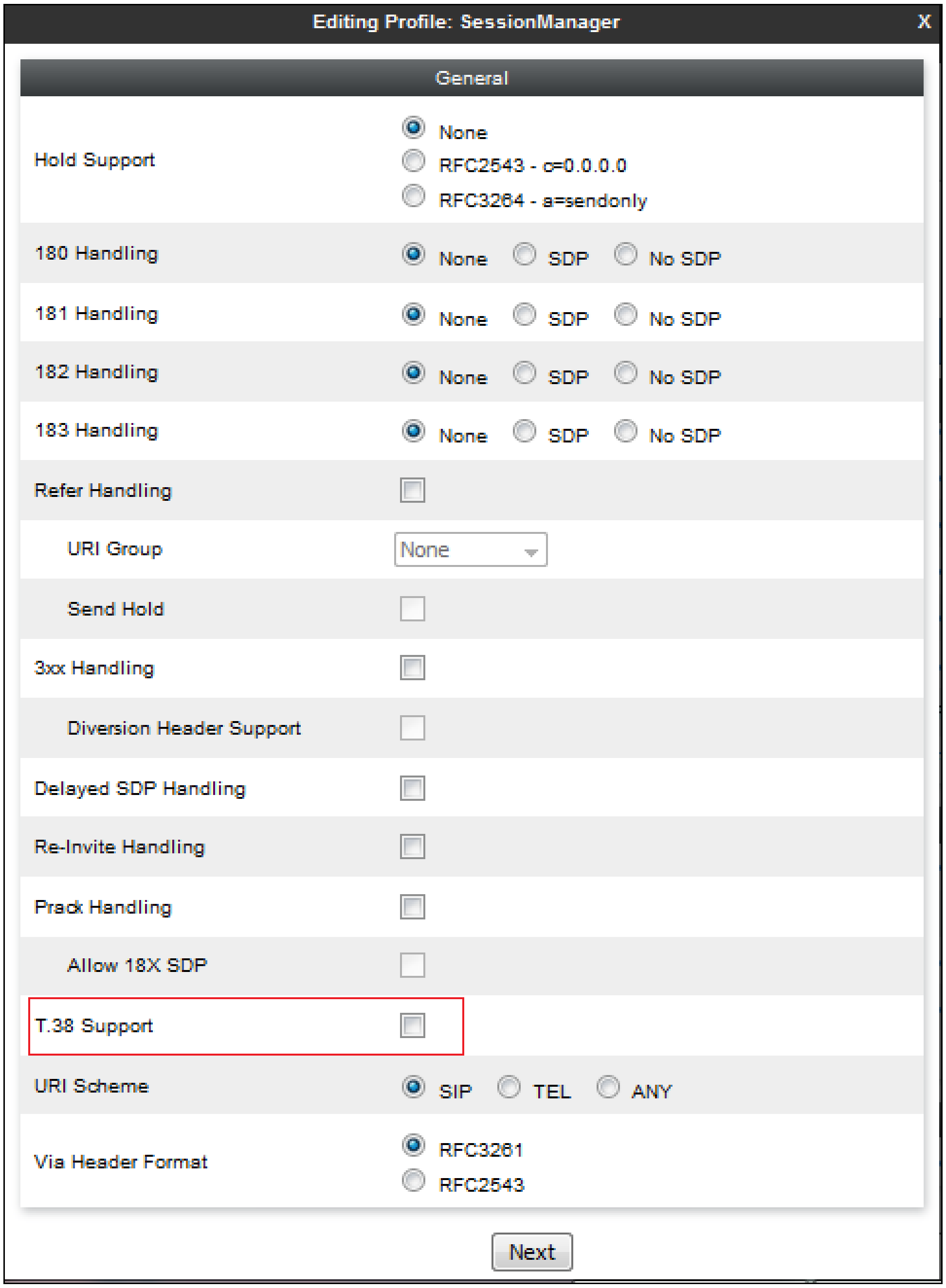
Server Interworking allows users to configure and manage various SIP call server-specific capabilities such as call hold and T.38 faxing. This section defines the profile for the connection to Session Manager.

1. Select **Global Profiles → Server Interworking** from the left-hand menu.
2. Click the **Add** button.
3. Enter profile name: (e.g., **SessionManager**), and click **Next**.



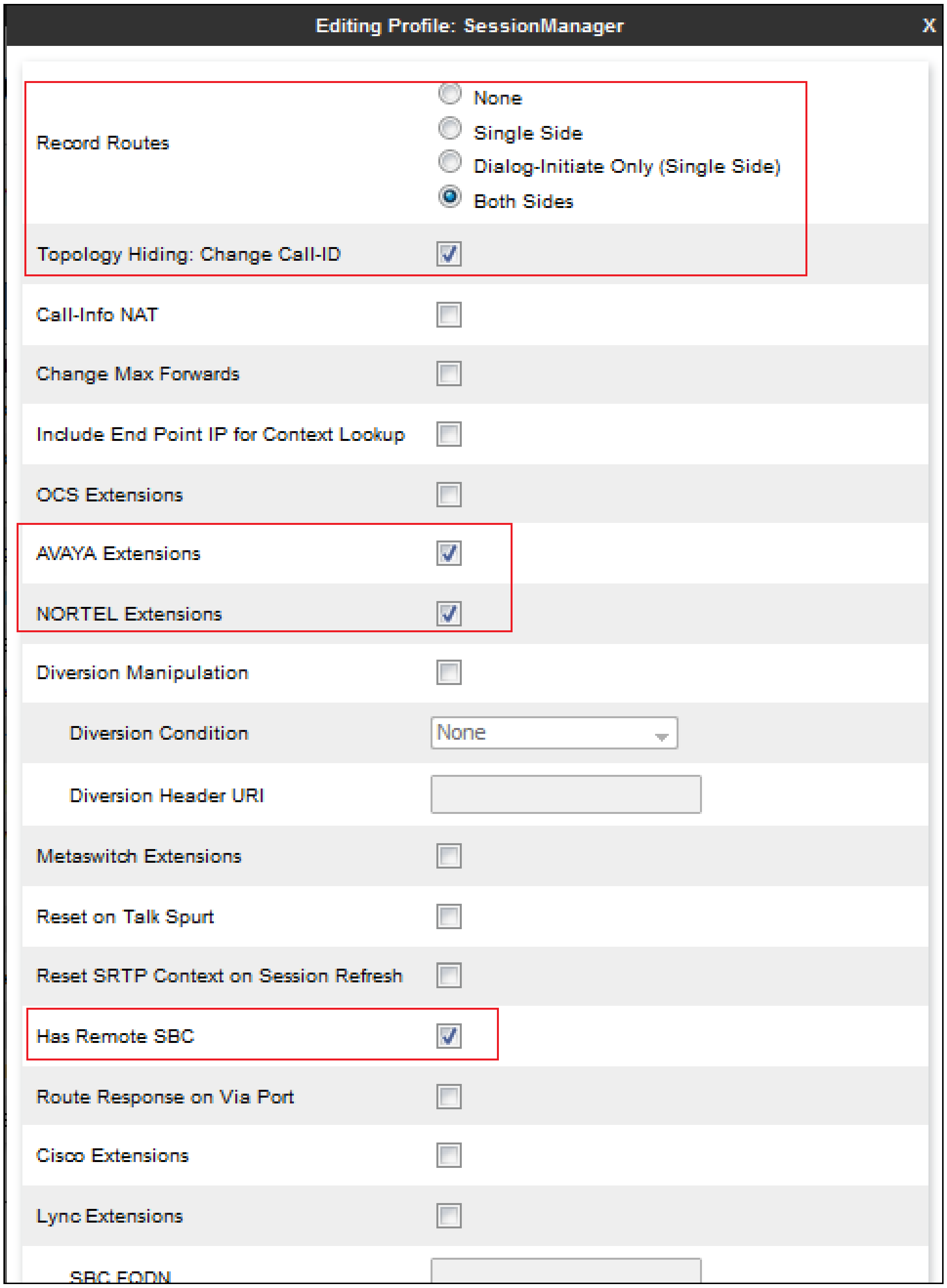
4. The **General** screen will open.

- Uncheck **T38 Support** box.
- All other options can be left with default values, and click **Next**.



5. On the **Timers** and **Privacy** windows, select **Next** to accept default values.

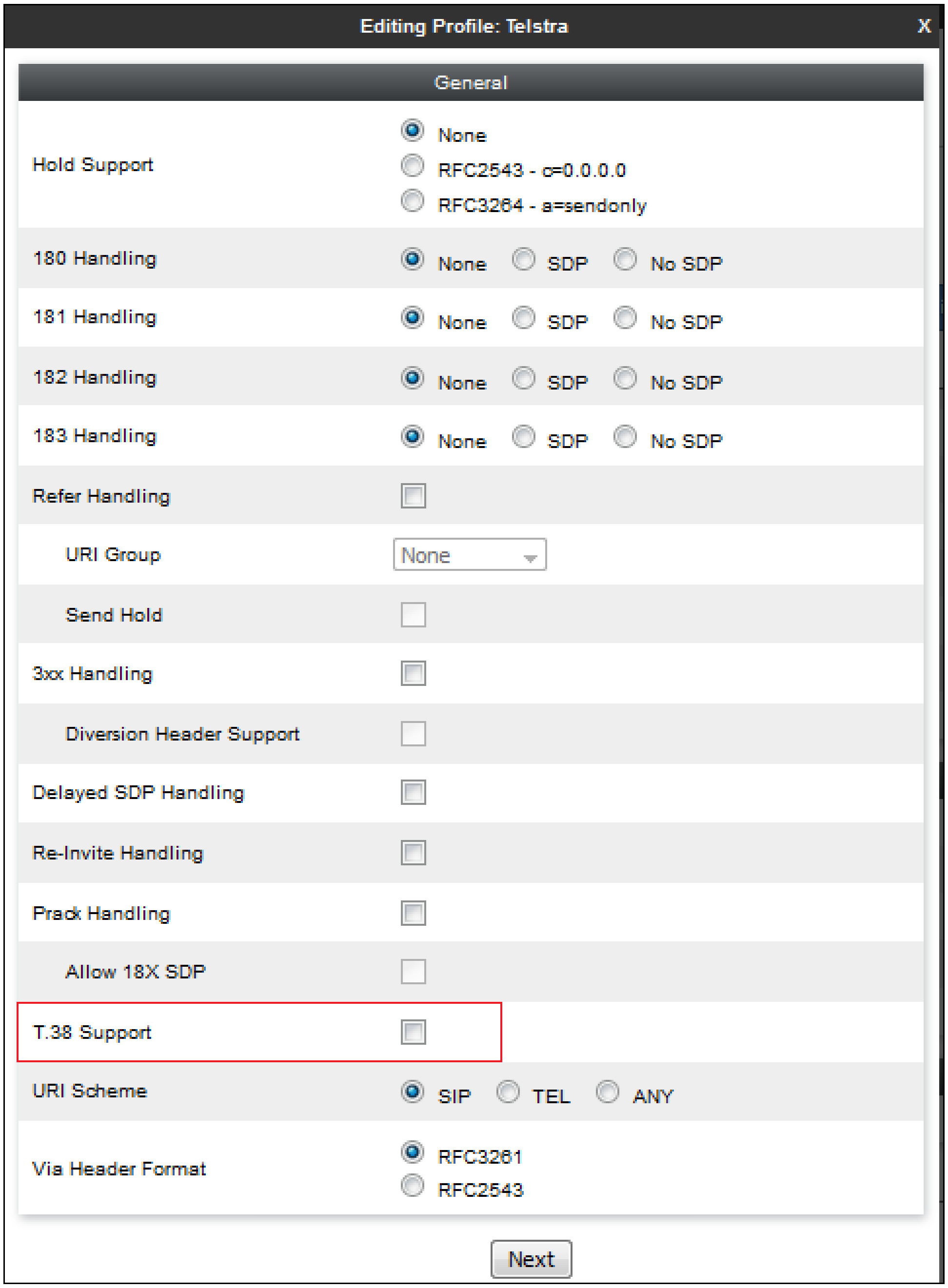
6. On the **Advanced** window, configure as below while other fields can be left as default:
   - Record Routes: choose **Both Sides**.
   - Check to **Topology Hiding: Change Call-ID** box.
   - Check to **AVAYA Extensions** box.
   - Check to **NORTEL Extensions** box.
   - Has Remote SBC: choose **Yes**.



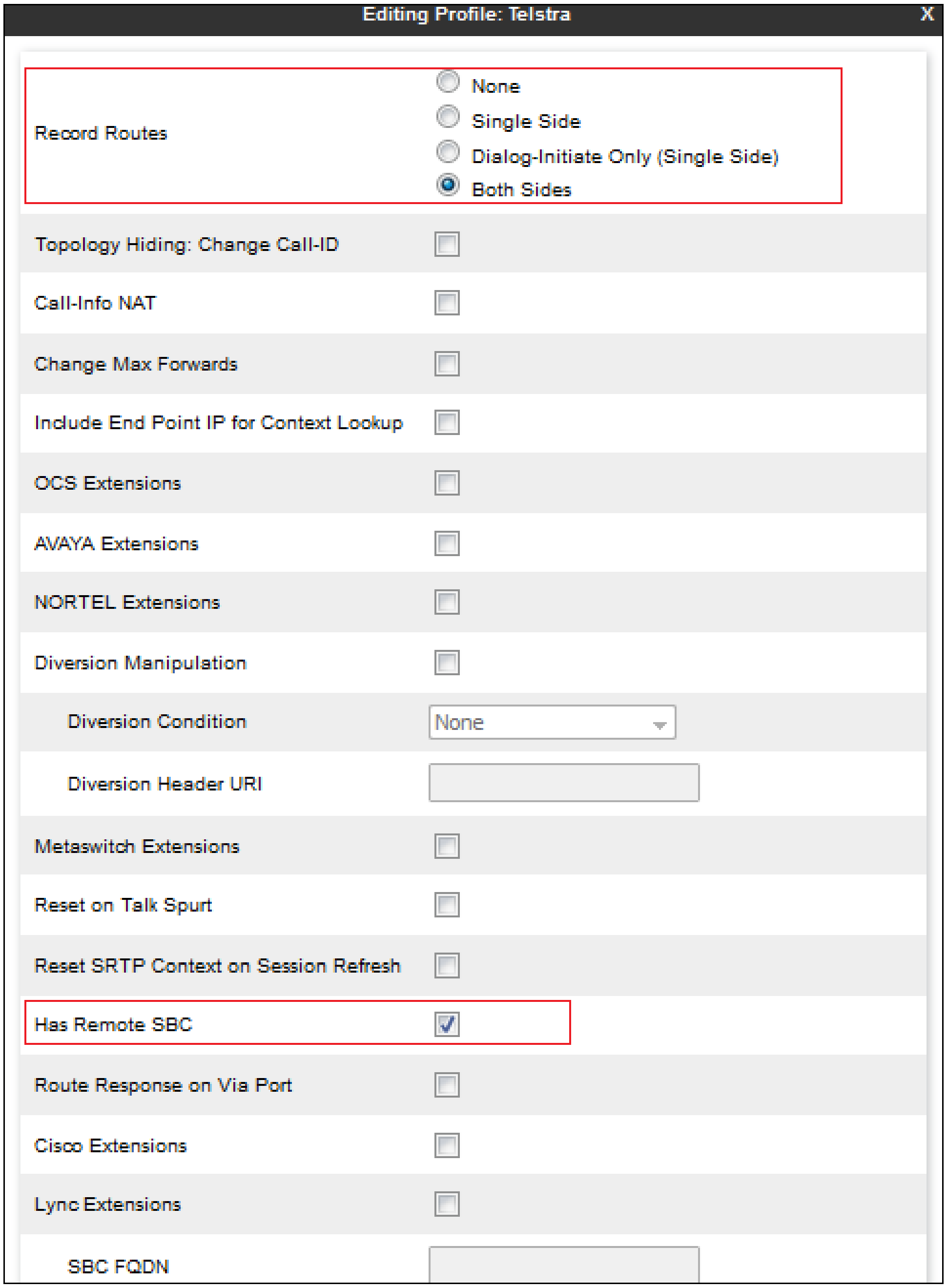
7.2.3 Server Interworking – Telstra

Repeat the steps shown in **Section 7.2.2** to add an Interworking Profile for the connection to Telstra network, with the following changes:

1. Enter **Telstra** as the **profile name** (not shown).



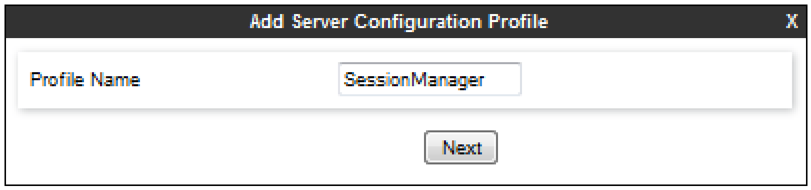
2. **Advanced** window is configured as below, click **Finish** to save the profile:



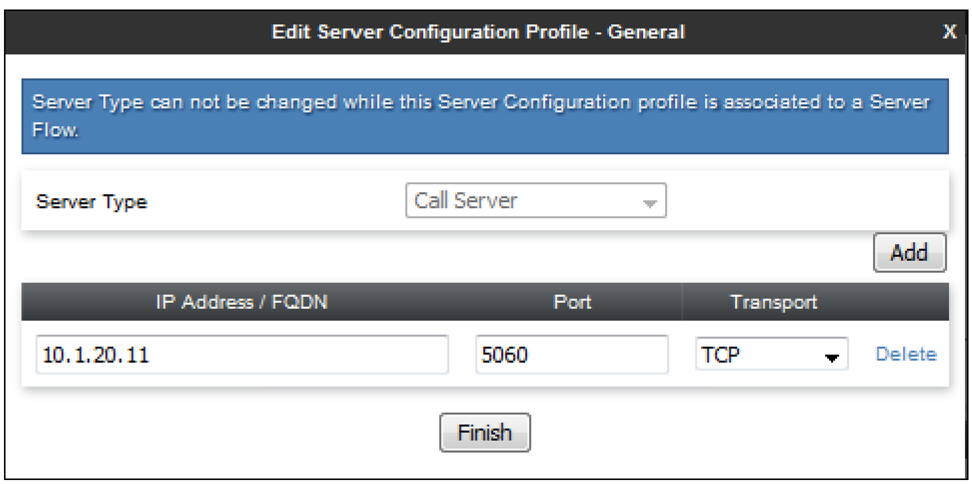
7.2.4 Server Configuration – Session Manager

This section defines the Server Configuration for the Avaya SBCE connection to Session Manager.

1. Select **Global Profiles → Server Configuration** from the left-hand menu.
2. Select **Add Profile** and the **Profile Name** window will open. Enter a Profile Name (e.g., **Session Manager**) and click **Next**.

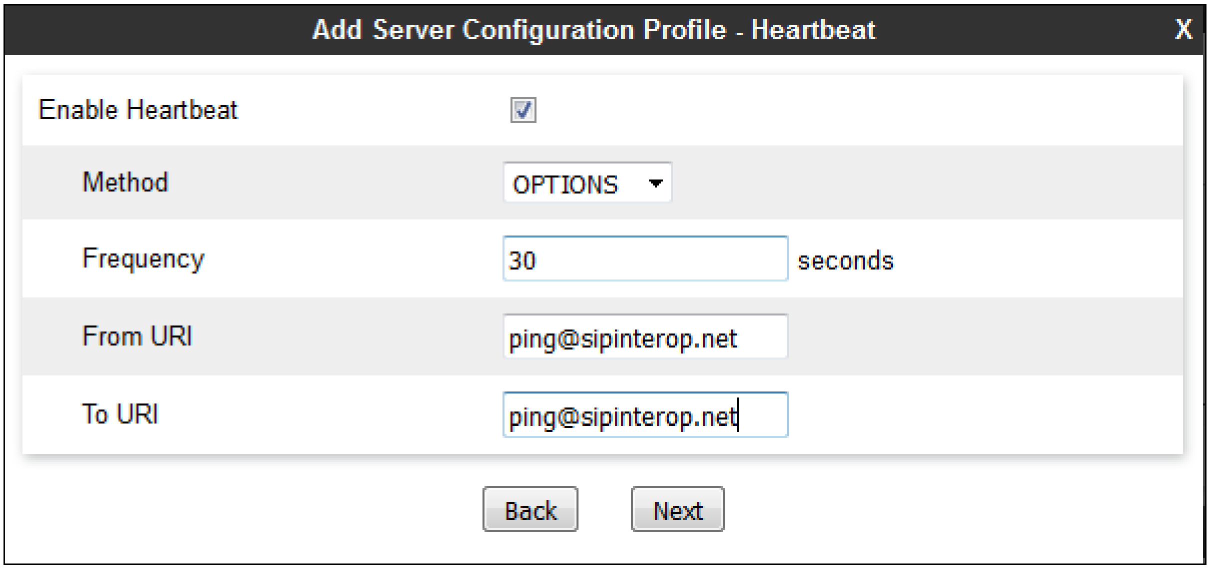


3. The **Add Server Configuration Profile** window will open.
   - Select **Server Type**: **Call Server**.
   - **IP Address / FQDN**: **10.1.20.11** (Session Manager signaling IP Address as configured in **Section 6.4.1**).
   - **Transport**: Select **TCP**.
   - **Port**: **5060**.
   - Select **Next** (not shown).

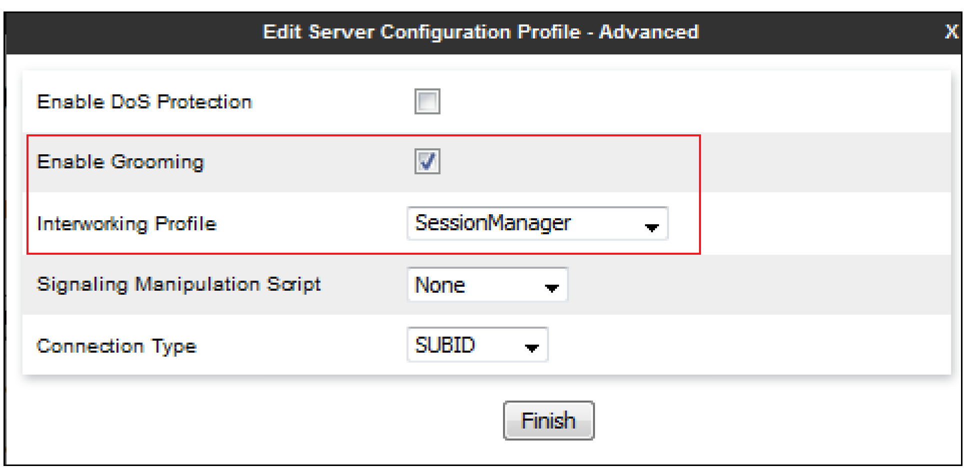


4. The **Authentication** window will open (not shown).
   - Select **Next** to accept default values.

5. The **Heartbeat** window will open.
    - Check to **Enable Heartbeat** box.
    - **Method**: select **OPTIONS**.
    - **Frequency**: enter **30** (or more).
    - **From URI** and **To URI**: enter **ping@sipinterop.net**
    - Click on **Next** button.



6. The **Advanced** window will open.
    - Check **Enable Grooming** box.
    - For **Interworking Profile**, select the profile created for Session Manager in **Section 7.2.2**.
    - Click on **Finish**.



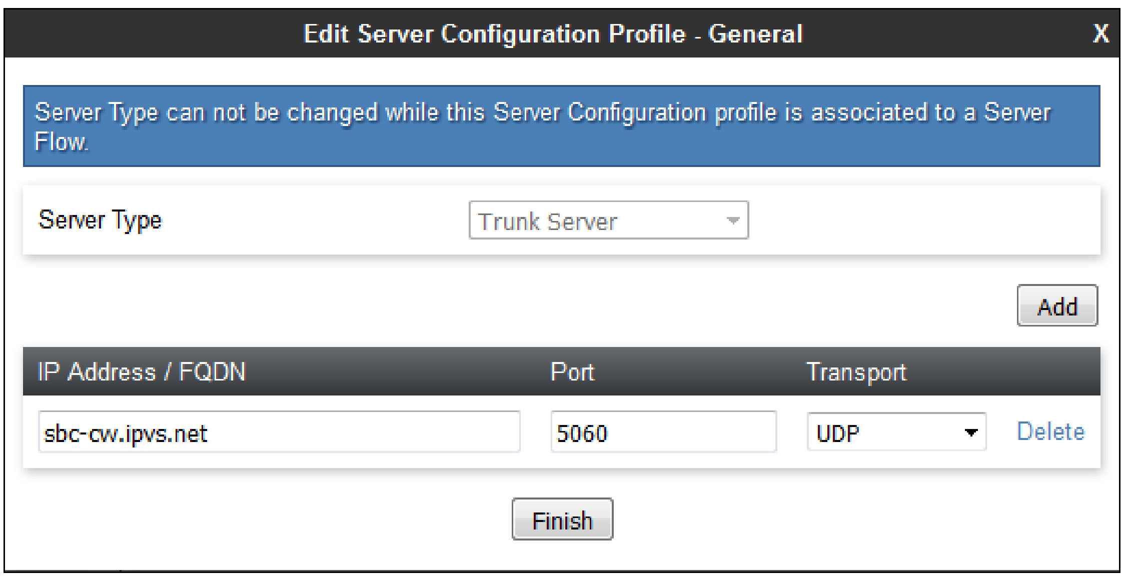
7.2.5 Server Configuration – Telstra

Telstra provided two trunk groups for Enterprise SIP Trunking service. These two trunk groups were connected to two outbound proxies. Telstra Enterprise SIP Trunking service requires authentication so Enterprise Trunk credentials must be provided by Telstra.

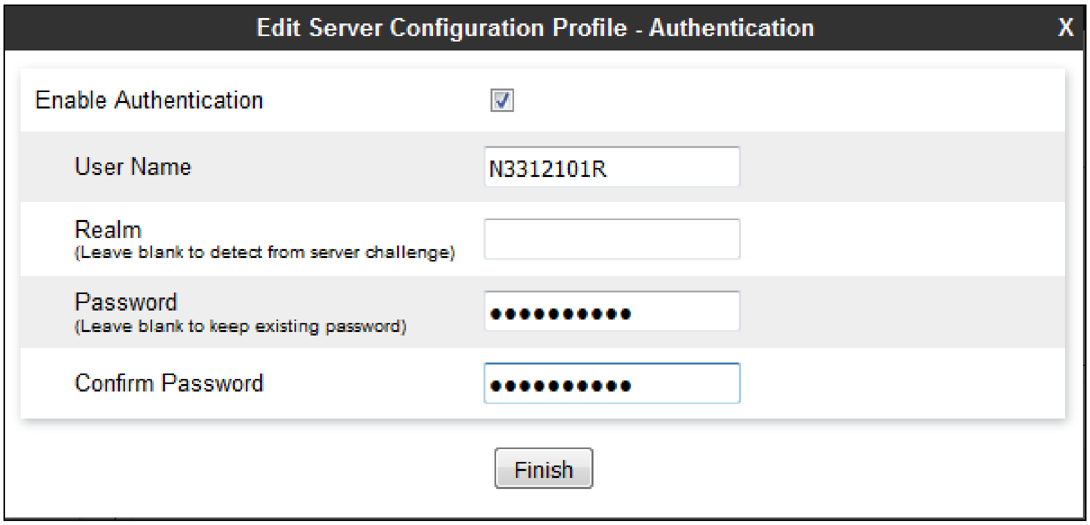
7.2.5.1 Telstra primary

Repeat the steps in **Section 7.2.4**, with the following changes, to create a Server Configuration for the Avaya SBCE connection to Telstra Trunk Group 1.

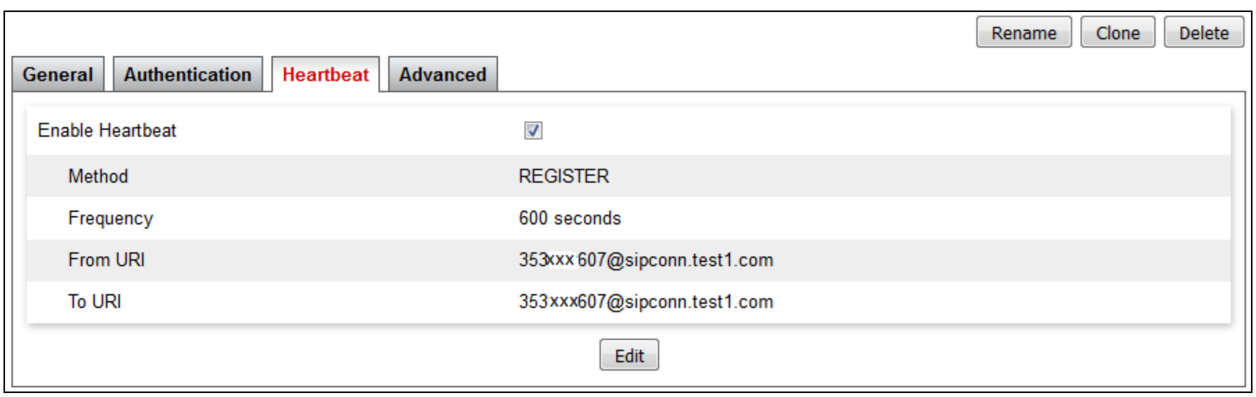
1. Select **Add Profile** and enter a Profile Name (e.g., **Telstra_pri**) and select **Next** (not shown).
2. On the **General** window, enter the following.
   - Select Server Type**: Trunk Server**.
   - **IP Address / FQDN: sbc-cw.ipvs.net** (outbound proxy 1 of Telstra)
   - **Transport**: Select **UDP**.
   - **Port: 5060**.
   - Select **Next** (not shown).



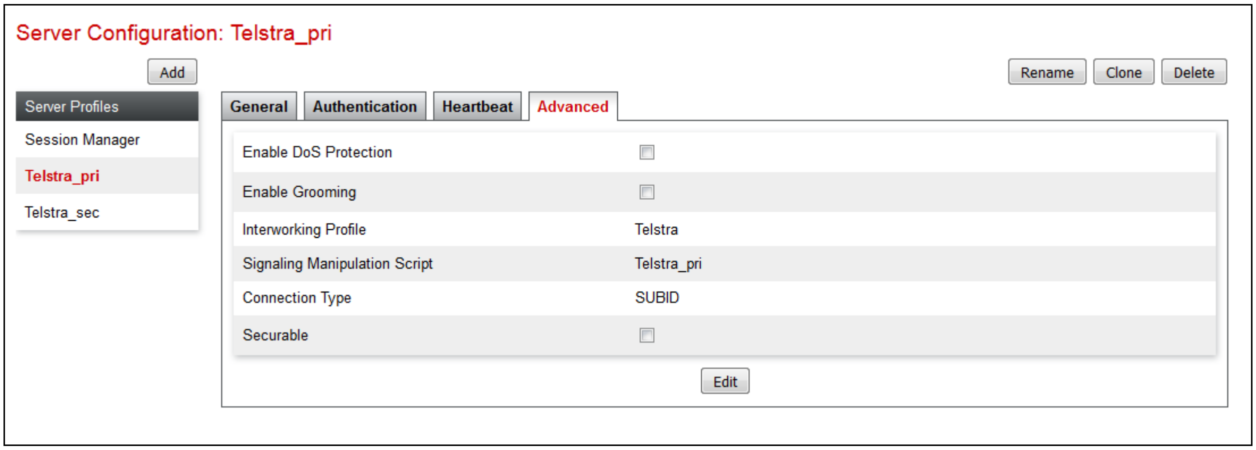
3. Under Authentication window:
   - Select **Enable Authentication**
   - User Name: enter Authentication name for outbound proxy 1.
   - Realm: leave blank.
   - Password and Confirm Password: enter Password provided by Telstra.



4. Under Heartbeat window:
   - Select **Enable Heartbeat**.
   - Method: choose **REGISTER**.
   - Frequency: enter **600**.
   - From URI and To URI: enter Pilot number provided by Telstra.



5. Under Advanced window:
    - Select **Telstra** for Interworking Profile.
    - Select **Telstra_pri** for Signaling Manipulation Script (see **Notice 1**).



<u>Notice 1:</u>
Note that Signaling Manipulation Script **Telstra_pri** is required to:

- Add the primary Trunk Pilot number into the PAI Header on outgoing calls.
- If the FROM header is ‘anonymous’, then re-write the FROM with the primary Trunk Pilot number.

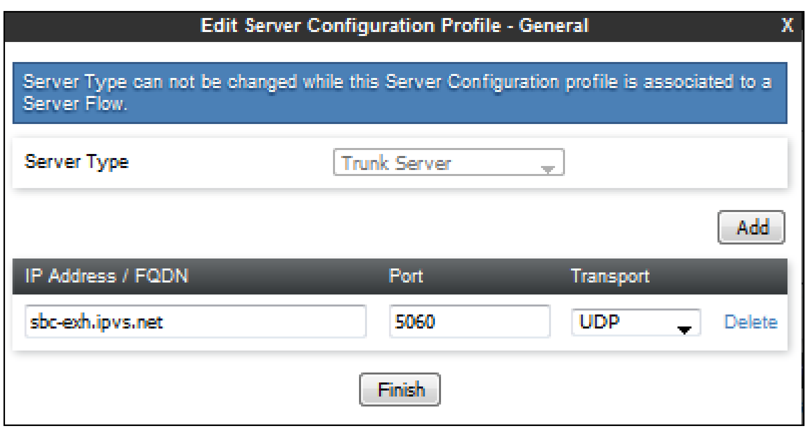
Navigate to **Global Profiles** > **Signaling Manipulation** to add **Telstra_pri** script:

```
within session "INVITE"
{
act on request where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
{
%HEADERS["P-Asserted-Identity"][1].URI.USER = "353xxx607";
}
}
within session "ALL"
{
act on request where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
{
if(%HEADERS["FROM"][1].URI.USER = "anonymous")then
{
%HEADERS["FROM"][1].URI.USER = "353xxx607";
}
}
}
```

7.2.5.2 Telstra secondary

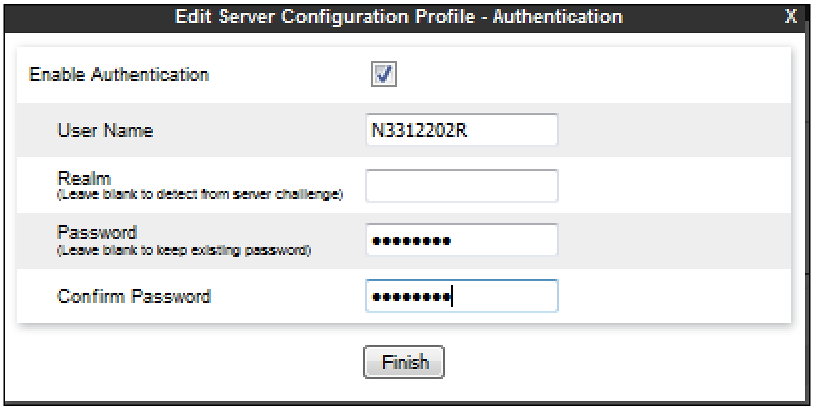
Repeat the steps in **Section 7.2.5.1**, with the following changes, to create a Server Configuration for the Avaya SBCE connection to Telstra Trunk Group 2.

1. Select **Add Profile** and enter a Profile Name (e.g., **Telstra_sec**) and select **Next** (not shown).
2. On the **General** window, enter the following.
   - Select Server Type**: Trunk Server**.
   - **IP Address / FQDN: sbc-exh.ipvs.net** (outbound proxy 2 of Telstra)
   - **Transport**: Select **UDP**.
   - **Port: 5060**.
   - Select **Next** (not shown).

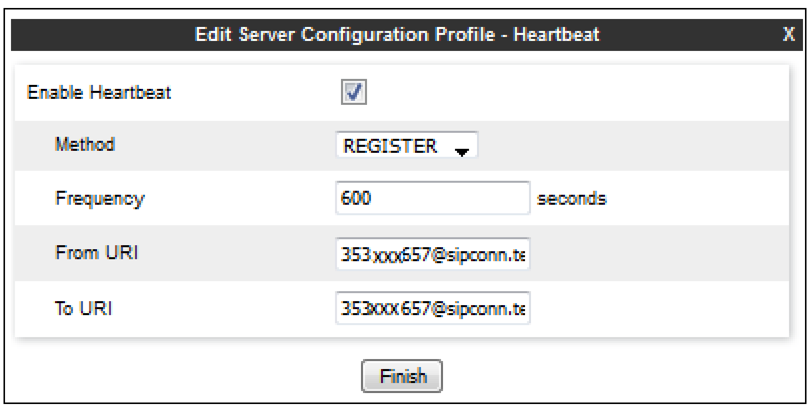


3. Under Authentication window:
   - Select **Enable Authentication**.
   - User Name: enter Authentication name for outbound proxy 2.
   - Realm: leave blank.

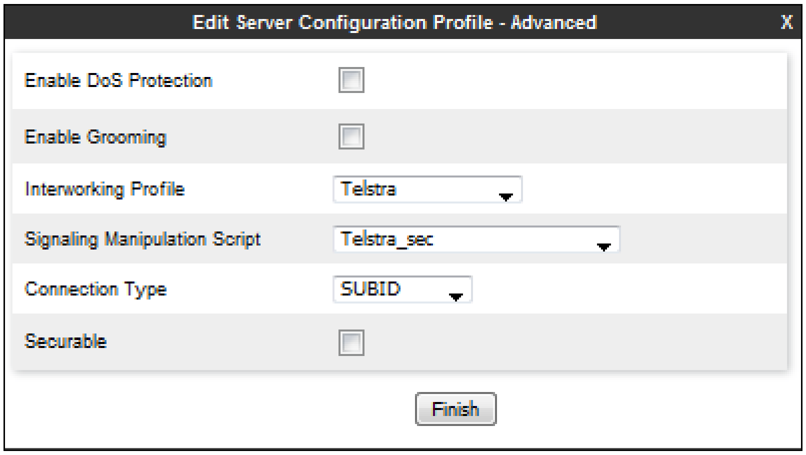
- Password and Confirm Password: enter Password provided by Telstra.



4. Under Heartbeat window:
   - Select **Enable Heartbeat**.
   - Method: choose **REGISTER**.
   - Frequency: enter **600**.
   - From URI and To URI: enter Pilot number provided by Telstra.



5. Under Advanced window:
    - Select **Telstra** for Interworking Profile.
    - Select **Telstra_sec** for Signaling Manipulation Script (see **Notice 2**).

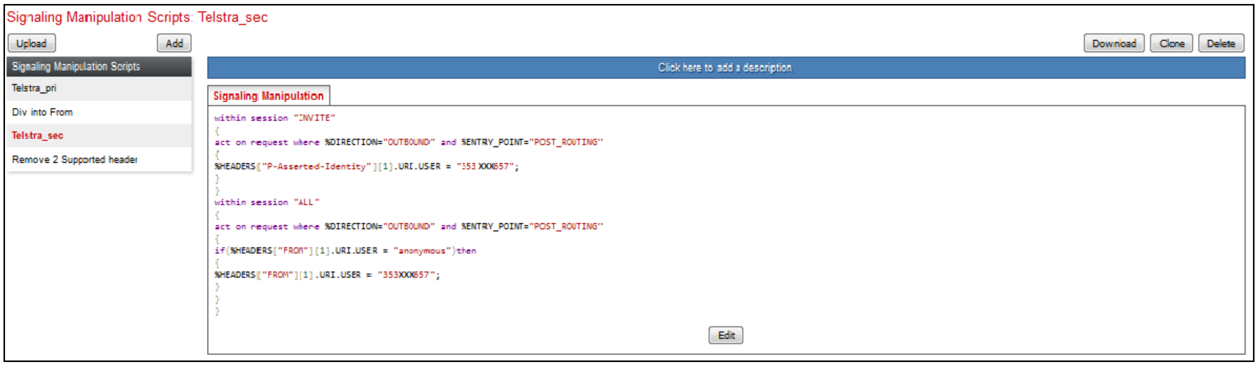


<u>Notice 2:</u>
Note that Signaling Manipulation Script **Telstra_sec** is required to:

- Add the second Trunk Pilot number into the PAI Header on outgoing calls.
- If the FROM header is 'anonymous', then re-write the FROM with the second Trunk Pilot number.

Repeat steps in **Notice 1** in **Section 7.2.5.1** to add **Telstra_sec** script:

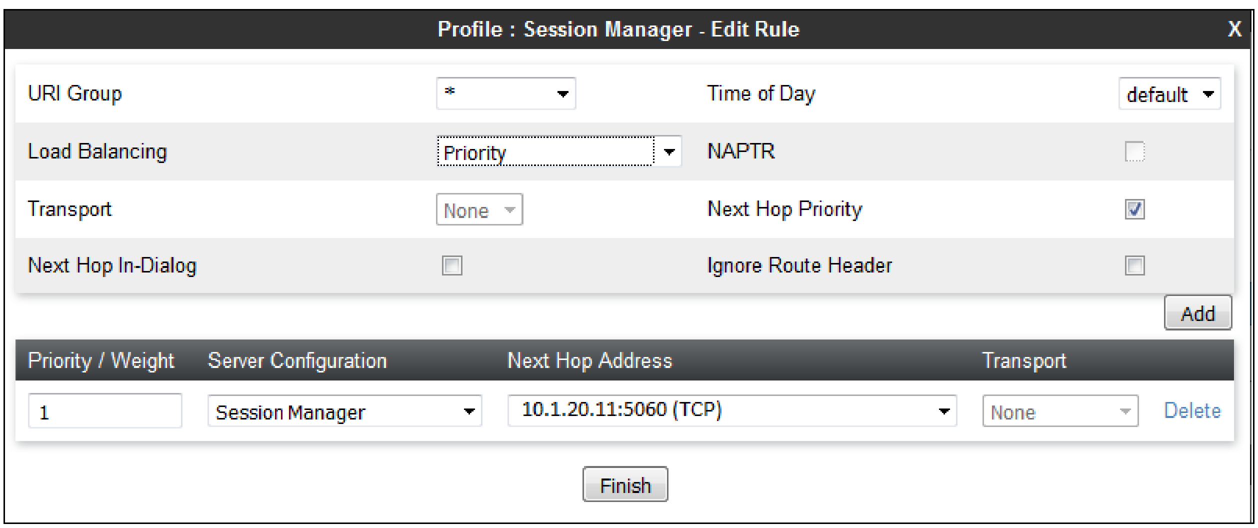
```
within session "INVITE"
{
act on request where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
{
%HEADERS["P-Asserted-Identity"][1].URI.USER = "353xxx657";
}
}
within session "ALL"
{
act on request where %DIRECTION="OUTBOUND" and
%ENTRY_POINT="POST_ROUTING"
{
if(%HEADERS["FROM"][1].URI.USER = "anonymous")then
{
%HEADERS["FROM"][1].URI.USER = "353xxx657";
}
}
}
```



7.2.6 Routing – To Session Manager

This provisioning defines the Routing Profile for the connection to Session Manager.

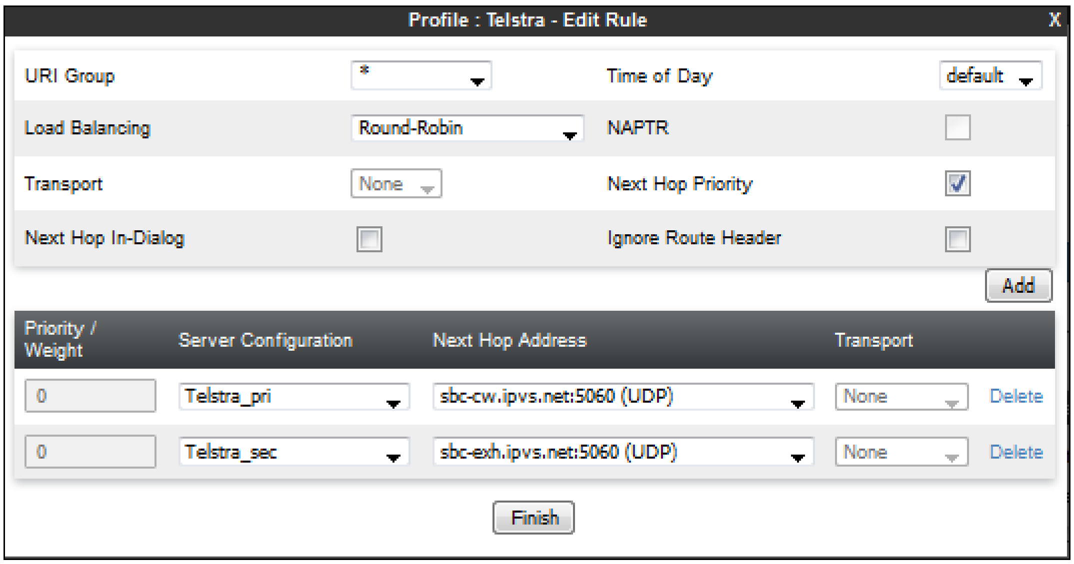
1. Select **Global Profiles → Routing** from the left-hand menu, and select **Add** (not shown).
2. Enter a **Profile Name**: (e.g., **Session Manager)** and click **Next**.
3. The Routing Profile window will open. Using the default values shown, click on **Add.**
4. The Next-Hop Address window will open. Populate the following fields:
   - **Priority/Weight** = **1**.
   - **Server Configuration** = **SessionManager**.
   - **Next Hop Address:** Verify that the **10.1.20.11:5060 (TCP)** entry from the drop down menu is selected (Session Manager IP address). Also note that the **Transport** field is grayed out.



7.2.7 Routing – To Telstra

Repeat the steps in **Section 7.2.6**, with the following changes, to add a Routing Profile for the Avaya SBCE connection to Telstra.

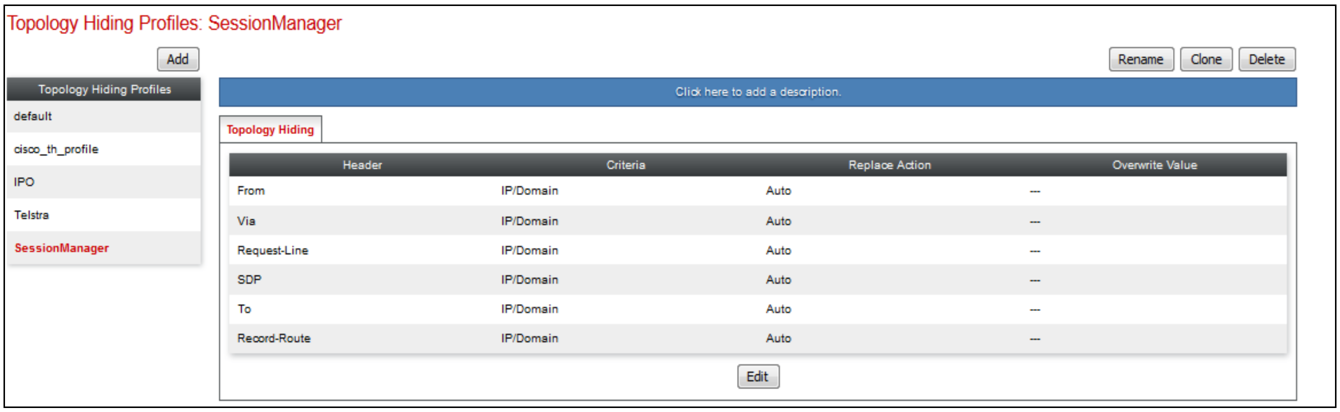
1. On the **Global Profiles → Routing** window (not shown), enter a **Profile Name**: (e.g., **Telstra)**.
2. Load Balancing: select **Round-Robin**.
3. Uncheck **Next Hop In-Dialog** box.
4. On the **Next-Hop Address** window (not shown), populate the following fields:
   - **Server Configuration: Telstra_pri**.
   - **Next Hop Address:** Verify that the **sbc-cw.ipvs.net:5060 (UDP)** entry from the drop down menu is selected.
5. Add another record for **Telstra_sec.**



7.2.8 Topology Hiding – Session Manager

The **Topology Hiding** screen allows users to manage how various source, destination and routing information in SIP and SDP message headers are substituted or changed to maintain the security of the network. It hides the topology of the enterprise network from external networks.

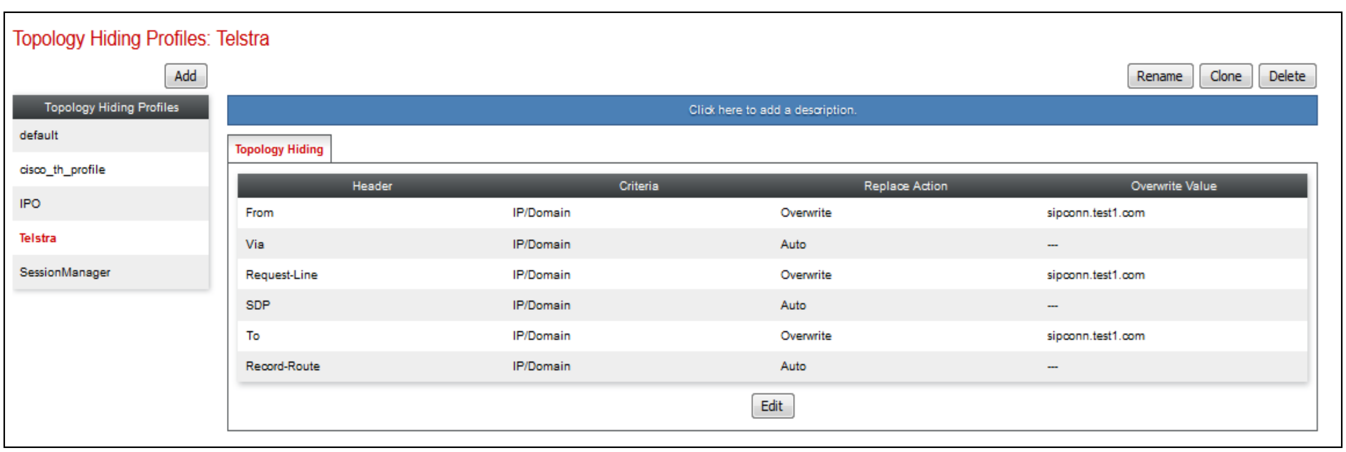
1. Select **Global Profiles → Topology Hiding** from the left-hand side menu.
2. Select the **Add** button, enter **Profile Name**: (e.g., **SessionManager**), and click **Next**.
3. The **Topology Hiding Profile** window will open. Click on the **Add Header** button repeatedly to add headers.
4. Populate the fields as shown below, and click **Finish** (not shown).



7.2.9 Topology Hiding – Telstra

Repeat the steps in **Section 7.2.8,** with the following changes, to create a Topology Hiding Profile for the Avaya SBCE connection to Telstra.

1. Enter a **Profile Name**: (e.g., **Telstra**).
2. Click on the **Add Header** button repeatedly to add headers.
3. Populate the fields as shown below, and click **Finish** (not shown). Note that the **Overwrite Value** is **sipconn.test1.com** which is the SIP domain of Telstra.



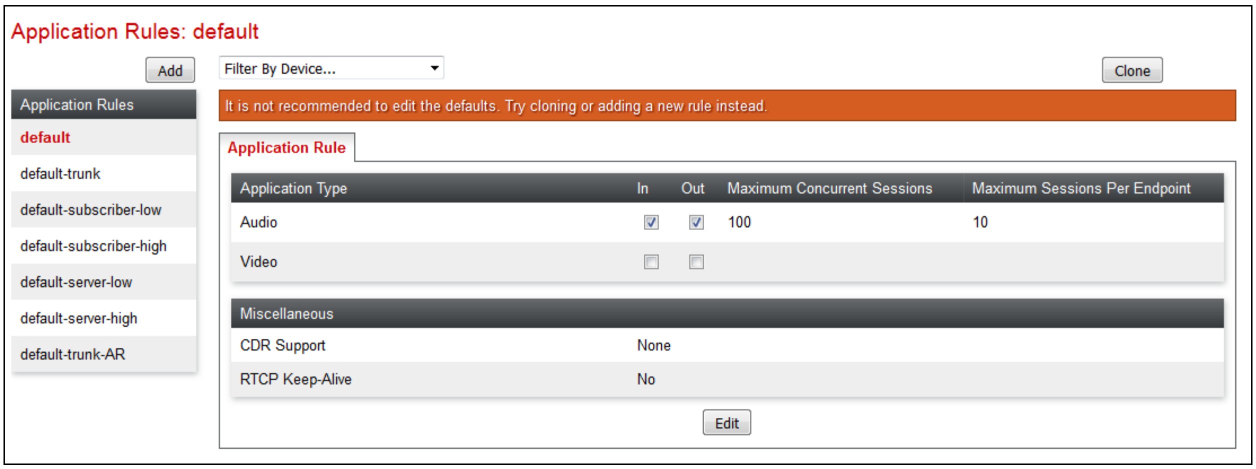
7.2.10 Domain Policies

The Domain Policies feature allows users to configure, apply and manage various rule sets (policies) to control unified communications based upon various criteria of communication sessions originating from or terminating in the enterprise.

7.2.11 Application Rules

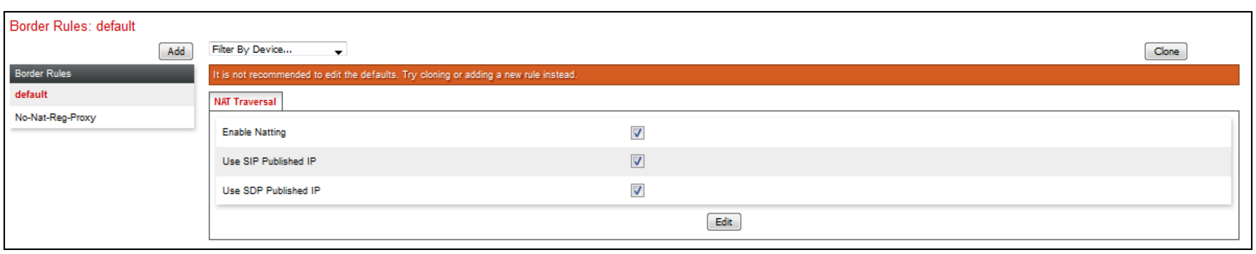
Ensure that the Application Rule used in the End Point Policy Group reflects the licensed sessions that the customer has purchased. In the lab setup, the Avaya SBCE was licensed for 100 Voice sessions, and the default rule was amended accordingly.

Note: It is not recommended to edit default rules. New rules should be added or cloned from default rules.



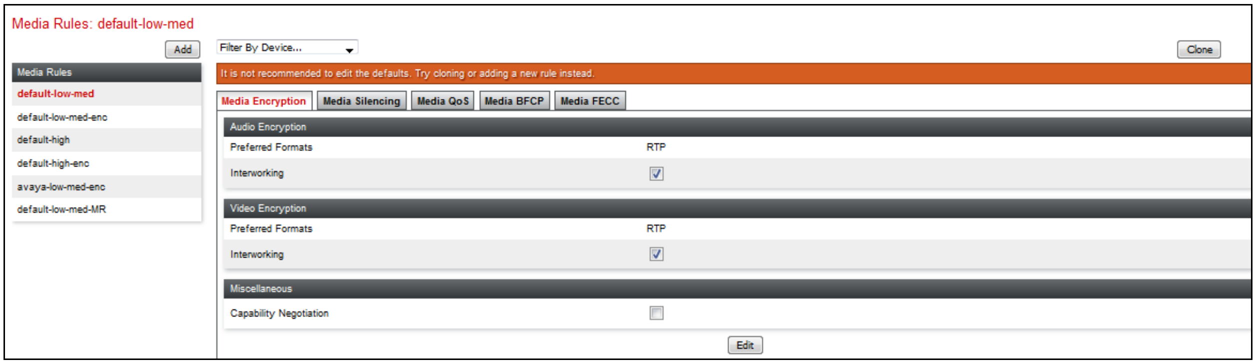
7.2.12 Border Rules

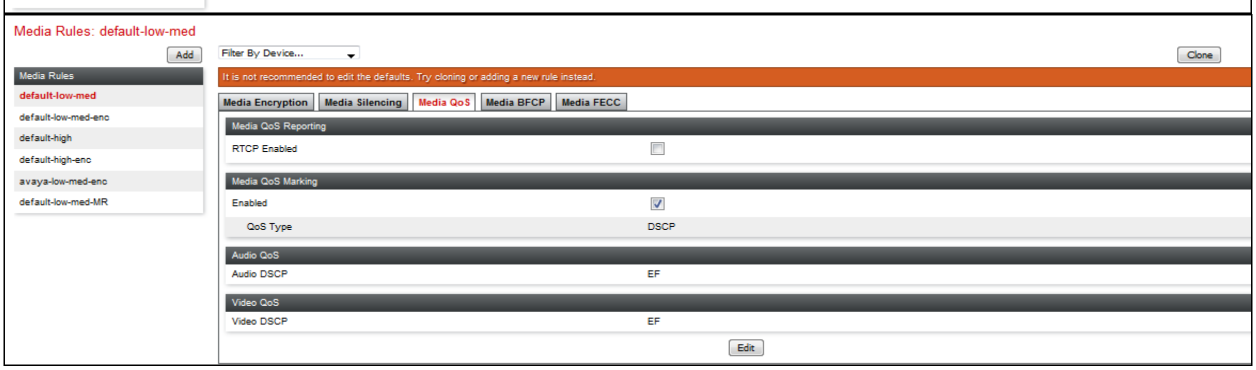
The Border Rule specifies if NAT is utilized (on by default), as well as detecting SIP and SDP Published IP addresses.



7.2.13 Media Rules

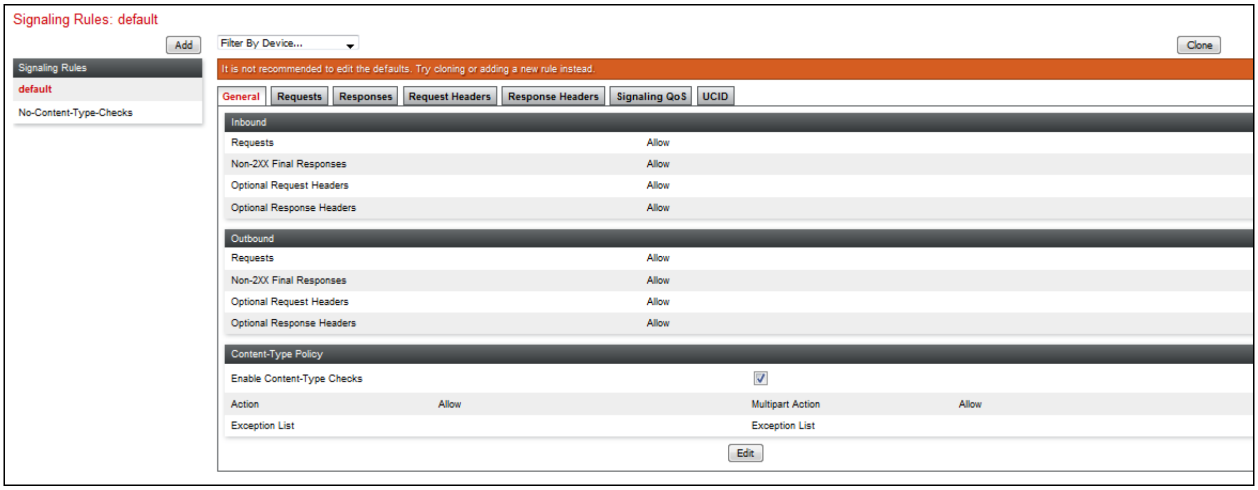
This Media Rule will be applied to both directions and therefore, only one rule is needed. In the solution as tested, the **default-low-med** rule was utilized. No customization was required.





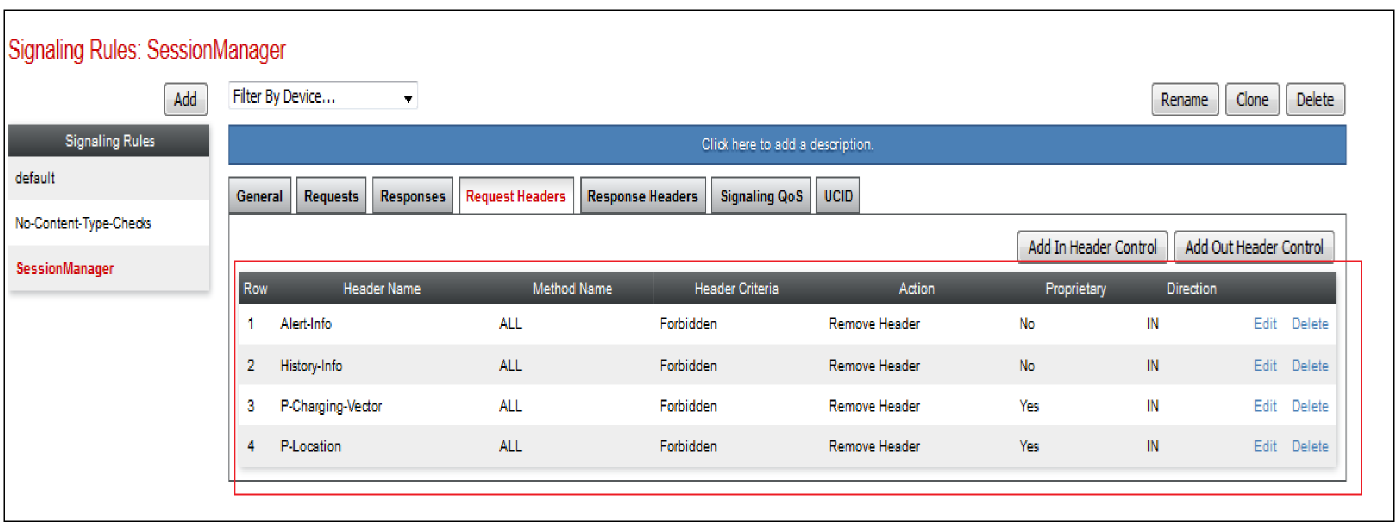
7.2.14 Signaling Rules

The default Signaling Rules was utilized for Telstra. No customization was required.

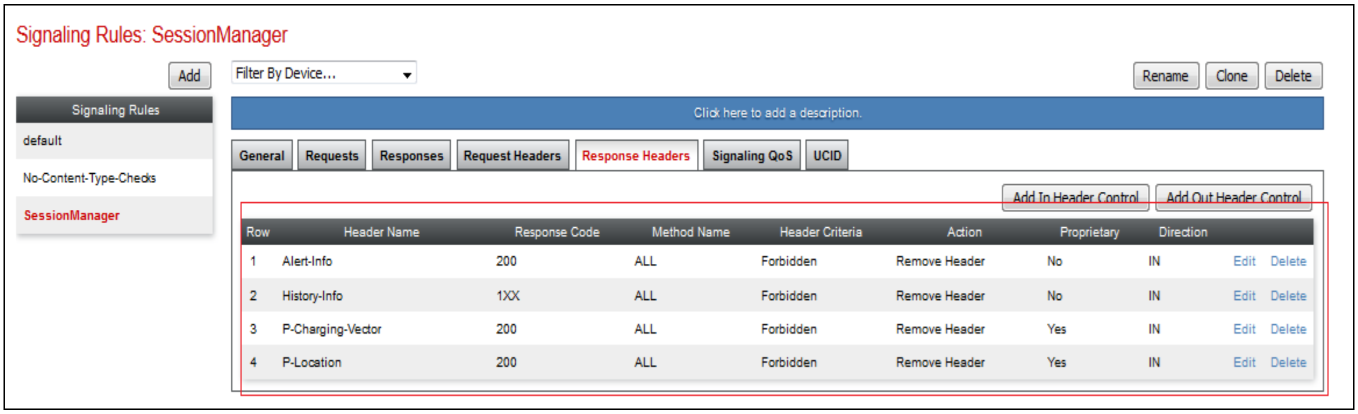


Add a new Signaling Rules for Session Manager:

1. Click on **Add** button to add a new Signaling Rules, name it as **SessionManager**.
2. Under **Request Headers**, click on **Add In Header Control** button to populate below records to remove History Info header and some unnecessary headers:

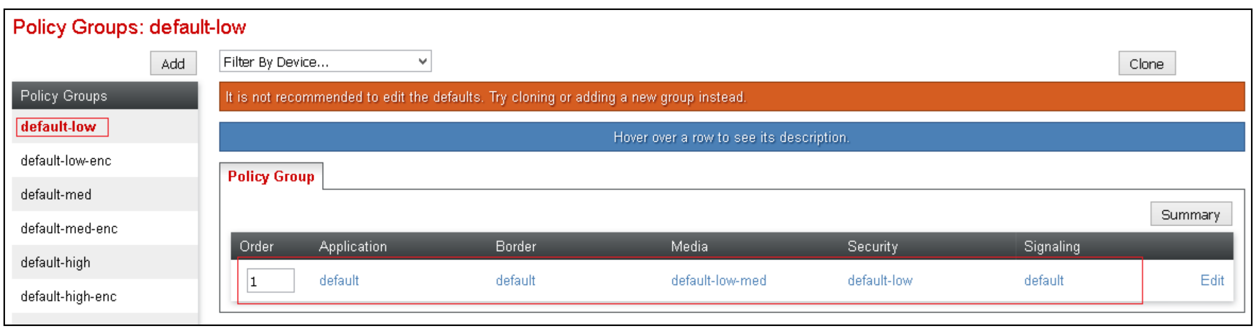


3. Under **Response Headers**, click on **Add In Header Control** button to populate the same records as in **Request Headers**:



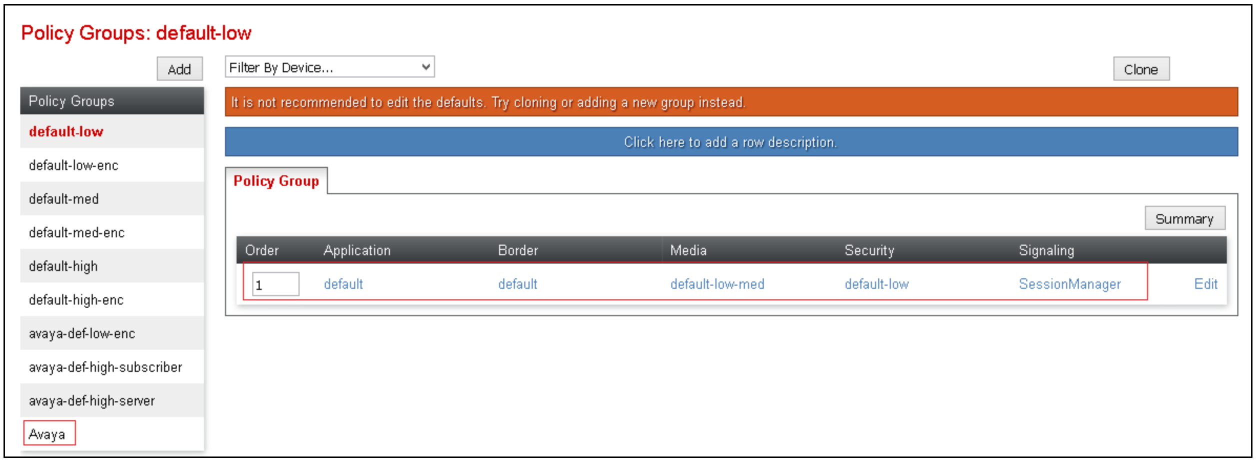
7.2.15 Endpoint Policy Groups

In the solution as tested, the **default-low** rule was utilized for Telstra. This rule incorporated the default media and Signaling Rules specified above, as well as other default policies.



Add a new Policy Groups for Session Manager:

1. Click on **Add** button to add a new Policy Groups, name it as **Avaya**.
2. Select **default** for **Application Rules**.
3. Select **default** for **Border Rules**.
4. Select **default-low-med** for **Media Rules**.
5. Select **default-low** for **Security Rules**.
6. Select **SessionManager** (created in **Section 7.2.14**) for **Signaling Rules**.



7.3 Device Specific Settings

The **Device Specific Settings** feature for SIP allows you to view aggregate system information, and manage various device-specific parameters which determine how a particular device will function when deployed in the network. Specifically, you have the ability to define and administer various device-specific protection features such as Message Sequence Analysis (MSA) functionality, end-point and session call flows.

7.3.1 Network Management

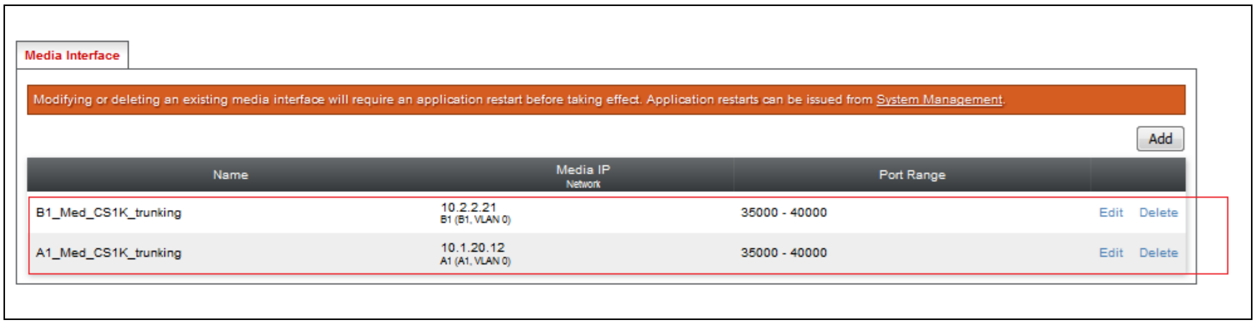
1. Select **Device Specific Settings → Network Management** from the menu on the left-hand side.
2. The **Interfaces** tab displays the enabled/disabled interfaces. In the reference configuration, interfaces A1 (private) and B1 (public) interfaces are used.
3. Select the **Networks** tab to display the IP provisioning for the A1 and B1 interfaces. These values are normally specified during installation. These can be modified by selecting **Edit**; however some of these values may not be changed if associated provisioning is in use.

7.3.2 Media Interfaces

1. Select **Device Specific Settings** from the menu on the left-hand side (not shown).
2. Select **Media Interface.**
3. Select **Add** (not shown). The **Add Media Interface** window will open. Enter the following:

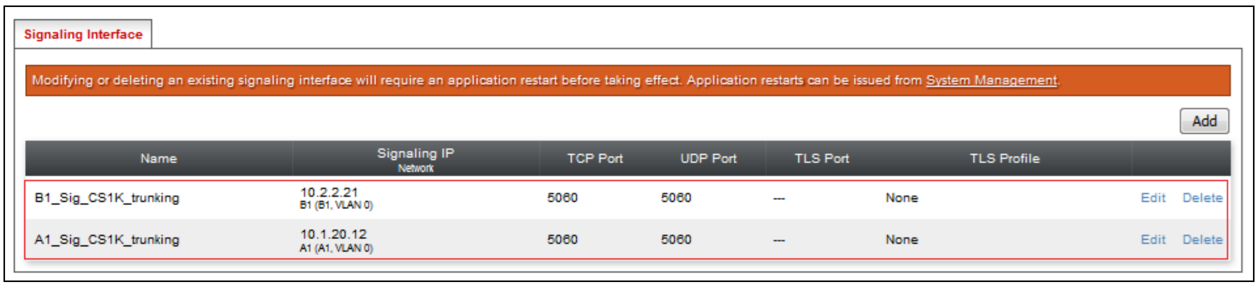
- **Name**: **A1_Med_CS1K_trunking**.
- **IP Address**: **10.1.20.12** (Avaya SBCE A1 address).
- **Port Range**: **35000-40000**.

4. Click **Finish** (not shown).
5. Select **Add** (not shown). The **Add Media Interface** window will open. Enter the following:
    - **Name**: **B1_Med_CS1K_trunking**.
    - **IP Address**: **10.2.2.21** (Avaya SBCE B1 address).
    - **Port Range**: **35000-40000**.
6. Click **Finish** (not shown). Note that changes to these values require an application restart. The completed **Media Interface** screen is shown below.



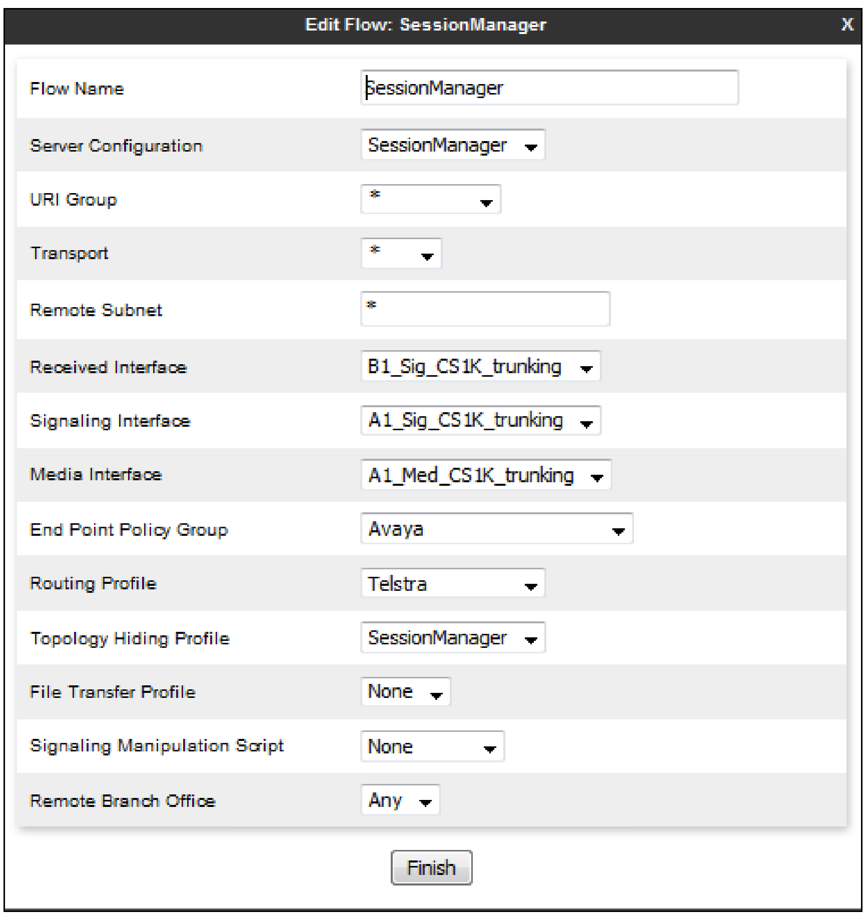
7.3.3 Signaling Interface

1. Select **Device Specific Settings** from the menu on the left-hand side (not shown).
2. Select **Signaling Interface**.
3. Select **Add** (not shown) and enter the following:
   - **Name**: **A1_Sig_CS1K_trunking**.
   - **IP Address**: **10.1.20.12** (Avaya SBCE A1 address).
   - **TCP Port: 5060.**
   - **UDP Port: 5060.**
4. Click **Finish** (not shown).
5. Select **Add** again, and enter the following:
   - **Name**: **B1_Sig_CS1K_trunking**.
   - **IP Address**: **10.2.2.21** (Avaya SBCE B1 address).
   - **TCP Port: 5060**.
   - **UDP Port: 5060.**
6. Click **Finish** (not shown). Note that changes to these values require an application restart.



7.3.4 Endpoint Flows – For Session Manager

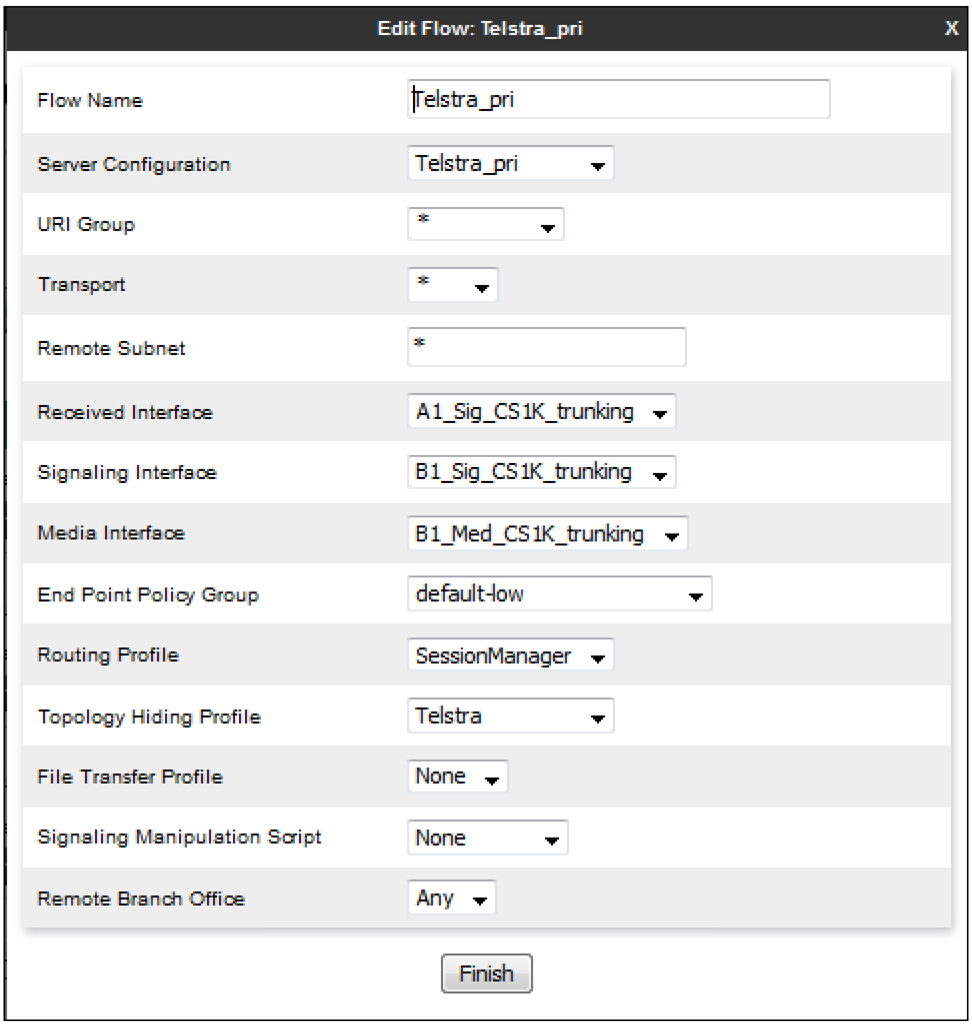
1. Select **Device Specific Settings → Endpoint Flows** from the menu on the left-hand side (not shown).
2. Select the **Server Flows** tab (not shown).
3. Select **Add**, (not shown) and enter the following:
    - **Name**: **SessionManager**.
    - **Server Configuration**: **SessionManager**.
    - **URI Group**: *
    - **Transport**: *
    - **Remote Subnet**: *
    - **Received Interface**: **B1_Sig_CS1K_trunking.**
    - **Signaling Interface**: **A1_Sig_CS1K_trunking**.
    - **Media Interface**: **A1_Med_CS1K_trunking**.
    - **End Point Policy Group**: **Avaya**.
    - **Routing Profile**: **Telstra**.
    - **Topology Hiding Profile**: **SessionManager**.
    - Let other values default.
4. Click **Finish**.



7.3.5 Endpoint Flows – For Telstra

Repeat step **1** through **4** from **Section 7.3.4**, with the following changes:

- **Name**: **Telstra**.
- **Server Configuration**: **Telstra**.
- **Received Interface**: **A1_Sig_CS1K_trunking**.
- **Signaling Interface**: **B1_Sig_CS1K_trunking**.
- **Media Interface**: **B1_Med_CS1K_trunking**.
- **End Point Policy Group**: **default_low**.
- **Routing Profile**: **SessionManager**.
- **Topology Hiding Profile**: **Telstra**.



8. Verification Steps

The following steps may be used to verify the configuration.

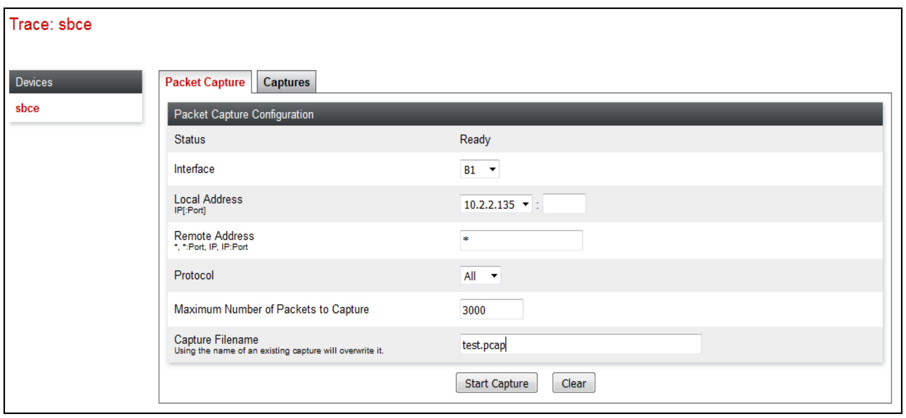
8.1 Avaya Session Border Controller for Enterprise

Log into the Avaya SBCE as shown in **Section 7**. Across the top of the display are options to display **Alarms**, **Incidents**, **Logs**, and **Diagnostics**. In addition, the most recent Incidents are listed in the lower right of the screen.

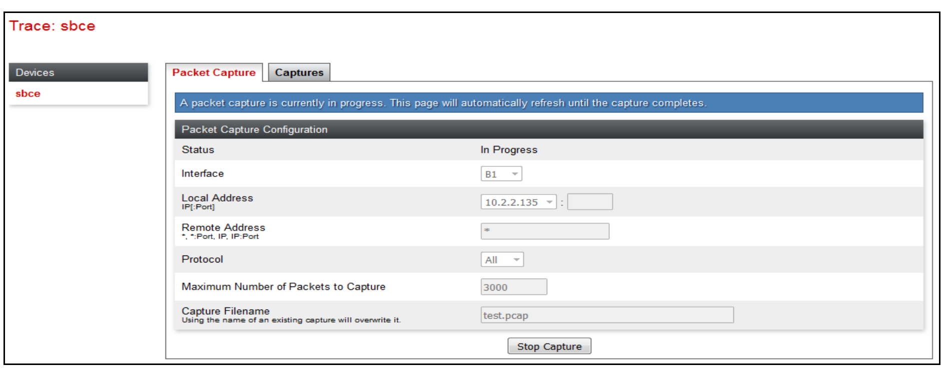
Protocol Traces

The Avaya SBCE can take internal traces of specified interfaces.

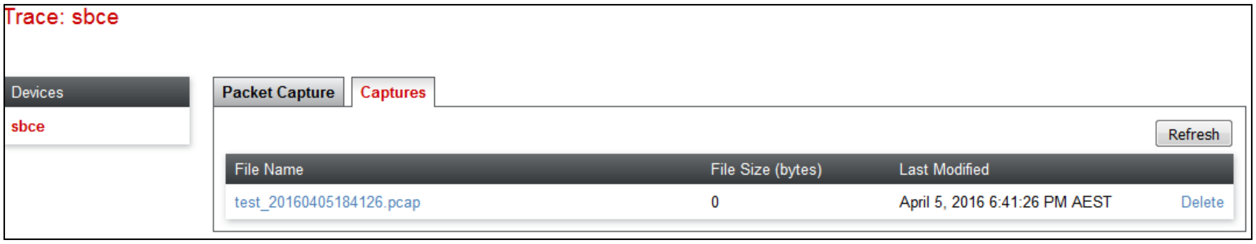
1. Navigate to **Device Specific Settings → Troubleshooting → Trace**.
2. Select the **Packet Capture** tab and select the following:
   - Select the desired **Interface** from the drop down menu (e.g., **All**).
   - Specify the **Maximum Number of Packets to Capture** (e.g., **5000**).
   - Specify a **Capture Filename** (e.g., **TEST.pcap**).
   - Unless specific values are required, the default values may be used for the **Local Address**, **Remote Address**, and **Protocol** fields.
   - Click **Start Capture** to begin the trace.



The capture process will initialize and then display the following **In Progress** status window:



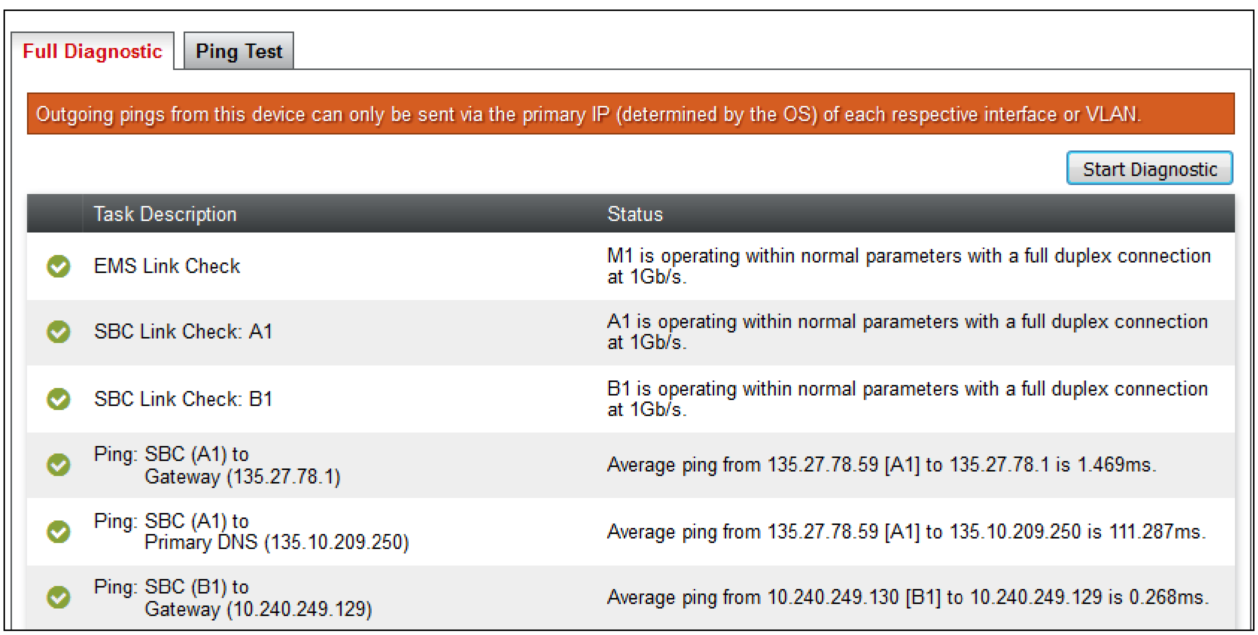
3. Run the test.
4. When the test is completed, select the **Stop Capture** button shown above.
5. Click on the **Captures** tab and the packet capture is listed as a *.pcap* file with the date and time added to filename specified in **Step 2**.
6. Click on the **File Name** link to download the file and use Wireshark to open the trace.

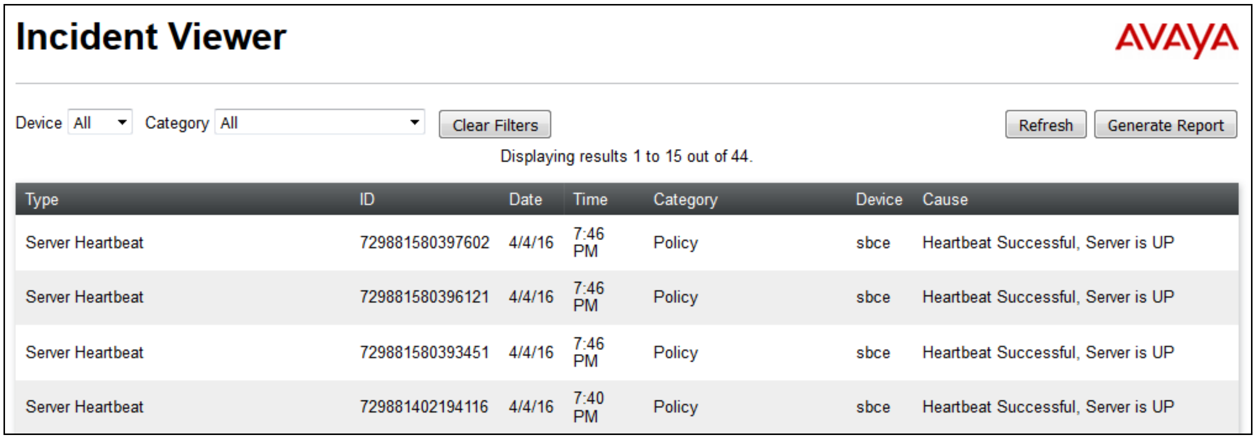


The following section details various methods and procedures to help diagnose call failure or service interruptions. As detailed in previous sections, the demarcation point between the Telstra Enterprise SIP Trunking service and the customer SIP PABX is the customer SBC.

On either side of the SBC, various diagnostic commands and tools may be used to determine the cause of the service interruption. These diagnostics can include:

- Ping from the SBC to the Telstra network gateway.
- Ping from the SBC to the Session Manager.
- Ping from the Telstra network towards the customer SBC.
- Note any Incidents or Alarms on the Dashboard screen of the SBC.





Type	ID	Date	Time	Category	Device	Cause
Server Heartbeat	729881580397602	4/4/16	7:46 PM	Policy	sbce	Heartbeat Successful, Server is UP
Server Heartbeat	729881580396121	4/4/16	7:46 PM	Policy	sbce	Heartbeat Successful, Server is UP
Server Heartbeat	729881580393451	4/4/16	7:46 PM	Policy	sbce	Heartbeat Successful, Server is UP
Server Heartbeat	729881402194116	4/4/16	7:40 PM	Policy	sbce	Heartbeat Successful, Server is UP

8.2 Avaya CS1000

SIP Trunk monitoring (ld 32): Place an inbound call from PSTN to an Avaya CS1000 phone. Then check the SIP trunk status by using ld 32, and verify one trunk is BUSY.

```
>ld 32
NPR000
.stat 100 0
009 UNIT(S) IDLE
001 UNIT(S) BUSY
000 UNIT(S) DSBL
000 UNIT(S) MBSY
```

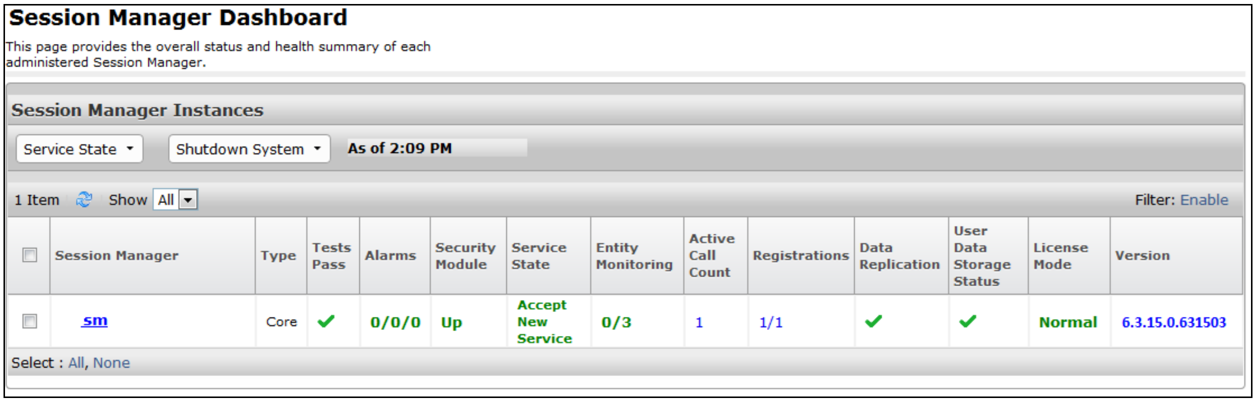
After the call is released, check that SIP trunk status. It should change to the IDLE state.

```
>ld 32
NPR000
.stat 100 0
010 UNIT(S) IDLE
000 UNIT(S) BUSY
000 UNIT(S) DSBL
000 UNIT(S) MBSY
```

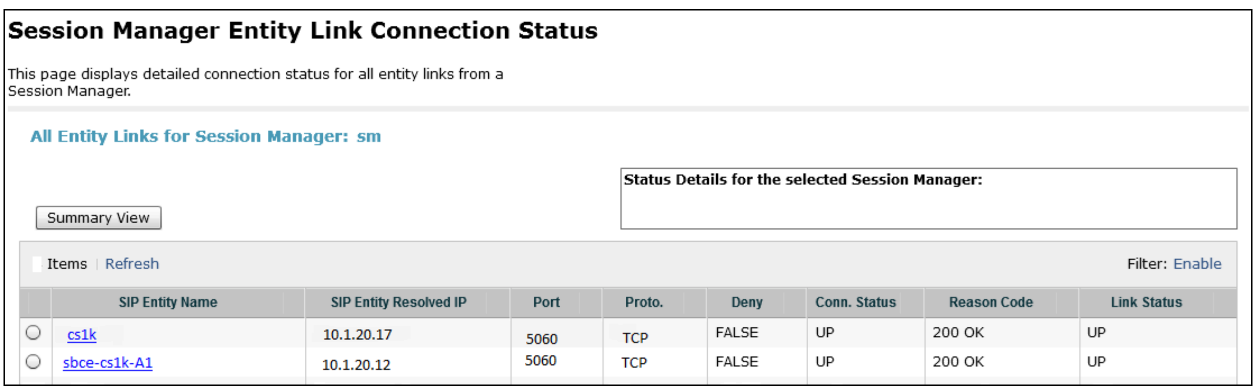
8.3 Avaya Aura® Session Manager Status

The Session Manager configuration may be verified via System Manager.

1. Using the procedures described in **Section 6**, access the System Manager GUI. From the **Home** screen, under the **Elements** heading, select **Session Manager**.



2. The Session Manager Dashboard is displayed. Note that the **Test Passed**, **Alarms**, **Service State**, and **Data Replication** columns, all show good status. In the **Entity Monitoring Column**, Session Manager shows that there are **0** (zero) alarms out of the **3** Entities defined.
3. Clicking on the **0/3** entry in the **Entity Monitoring** column, results in the following display:



8.4 Telephony Services

1. Place inbound/outbound calls, answer the calls, and verify that two-way talk path exists. Verify that the call remains stable for several minutes and disconnects properly.
2. Verify basic call functions such as hold, transfer, and conference.
3. Verify the use of DTMF signaling.

9. Conclusion

As illustrated in these Application Notes, Avaya Communication Server 1000 Release 7.6, Avaya Aura® Session Manager 6.3.15, and Avaya Session Border Control for Enterprise 6.3.6 can be configured to interoperate successfully with Telstra Enterprise SIP Trunking service. This solution allows enterprise users access to the PSTN using the Telstra Enterprise SIP Trunking service connection. Please refer to **Section 2.2** for exceptions.

10. Additional References

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

[1] *Deploying Avaya Aura® System Manager on VMware® in Virtualized Environment*, 13 Apr 2015.
[2] *Administering Avaya Aura® System Manager for Release 6.3.10*, 19 Feb 2015.
[3] *Administering Avaya Aura® Session Manager*, *22* May 2015.
[4] *Deploying Avaya Aura Session Manager using VMware in the Virtualized Environment*, 20 Nov 2014.
[5] *Deploying Avaya SBCE on VMware in Virtualized Environment*, 29 Aug 2015.
[6] *Administering Avaya Session Border Controller*, 12 Feb 2016.
[7] *Document Collection - Communication Server 1000 Release 7.6,* 18 Jul 2016.
[8] *RFC 3261 SIP: Session Initiation Protocol,* http://www.ietf.org/
[9] *RFC 3515, The Session Initiation Protocol (SIP) Refer Method*, http://www.ietf.org/
[10] *RFC 2833 RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals,* http://www.ietf.org/

Product documentation for Telstra Enterprise SIP Trunking service is available from Telstra.

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.