Avaya Solution & Interoperability Test Lab

Application Notes for BT Wholesale Hosted SIP Trunking service with Avaya Communication Server 1000 Release 7.6 SP8, Avaya Aura® Session Manager Release 7.0.1 SP2 and Avaya Session Border Controller for Enterprise Release 7.1 SP2 - Issue 1.0

Abstract

These Application Notes illustrate a sample configuration of Avaya Communication Server 1000 Release 7.6 SP8 and Avaya Aura® Session Manager Release 7.0.1 SP2 with SIP Trunks to Avaya Session Border Controller for Enterprise (Avaya SBCE) Release 7.1 SP2 when used to connect BT Wholesale Hosted SIP Trunking Service.

BT Wholesale Hosted SIP Trunking Service provides PSTN access via a SIP trunk between the enterprise and BT Wholesale 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.

BT Wholesale 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 Avaya lab.

Table of Contents

1. Introduction

These Application Notes illustrate a sample configuration for Avaya Communication Server 1000 Release 7.6 SP8 (Avaya CS1000) and Avaya Aura® Session Manager Release 7.0.1 SP2 with SIP Trunks to Avaya Session Border Controller for Enterprise (Avaya SBCE) Release 7.1 SP2 when used to connect to the BT Wholesale Hosted SIP Trunking Service.

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 BT Wholesale Hosted SIP Trunking Service and is used to not only secure the SIP trunk, but also to make adjustments to VoIP traffic for interoperability.

The Hosted SIP Trunking Service available from BT Wholesale is the SIP-based Voice over IP (VoIP) service offered to enterprises for a variety of voice communications needs. The BT Wholesale Hosted SIP Trunking Service allows enterprises 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 BT Wholesale Hosted 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 BT Wholesale Hosted SIP Trunking Service.

The compliance testing was based on the Avaya DevConnect CS1000 Generic SIP Trunk test plan. The testing covered functionality required for compliance as a solution supported on the BT Wholesale Hosted SIP Trunking Service. Calls were made to and from the PSTN across the BT Wholesale Hosted SIP Trunking Service. The following standard features were tested as part of this effort:

- Inbound PSTN calls to 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 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 Avaya CS1000 calls from/to BT Wholesale IP Telephony.
- Dialing plan: local call.
- Calling Party Name presentation and Calling Party Name restriction.
- Codecs G.711A, G.711MU and G.729A.
- Inbound and outbound fax using T.38.
- 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 History-info.
- Avaya CS1000 MobileX feature.
- Response to incomplete call attempts and trunk errors.

2.2 Test Results

Interoperability testing of BT Wholesale Hosted 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.

- **BT Wholesale SIP Trunk Resilience –** BT Wholesale supports SIP Trunk Resilience using DNS/SRV record. The DNS/SRV record is configured with a list of two FQDNs of BT Wholesale SBC servers which are working in active-active primary-secondary model. BT Wholesale requires only one SIP trunk registration to the platform at a time, hence, only one FQDN of BT Wholesale SBC server is configured in Server Configuration of Avaya SBCE because Avaya SBCE does not support DNS/SRV in Server Configuration. As a result, Avaya SBCE is not working properly with BT Wholesale SIP Trunk Resilience.
- **SIP Options sent to BT Wholesale –** It was observed that BT Wholesale responded back with **403 Forbidden-Source Endpoint Lookup Failed** for the SIP Options sent from Avaya. This is normal treatment of BT Wholesale.
- **Avaya CS1000 MobileX** – When a PSTN phone called to an Avaya phone which had MobileX enabled, Avaya CS1000 forked the call to the twinned mobile phone. However, BT Wholesale could not route the call to the twinned mobile phone, hence, only Avaya phone ringed. This is because BT Wholesale requires either proper History-info header or Diversion header in the forking INVITE sent to BT Wholesale but Avaya CS1000 MobileX does not support those kinds of headers. Therefore, MobileX feature should not be enabled.

- **Outgoing trunk to Outgoing trunk Call Transfer -** When an Avaya phone called to a PSTN phone, then the Avaya phone performed a blinded transfer or a consultative transfer to another PSTN endpoint, the expected behavior was that the Avaya phone should transfer the call successfully. But in this case, the Avaya phone could not complete the transfer. In order to overcome this issue, plug-in 201 must be enabled on Avaya CS1000.
- **If the Avaya CS1000 phone holds/resumes an outbound call, the dialed digits were no longer displayed** - This is a known limitation on Avaya 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 Avaya CS1000 limitation.

2.3 Support

- **Avaya:** Avaya customers may obtain documentation and support for Avaya products by visiting http://support.avaya.com.
- **BT Wholesale:** Customers should contact their BT Wholesale Business representative or follow the support links available on https://www.btwholesale.com/pages/static/products-services/wholesale-SIP-trunking.htm.

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 SIP software and Avaya i2004p2 IP Telephones running Unistim software.
- Avaya 3904 digital phone.
- Avaya i2050 softphone.
- The Avaya SBCE provided Session Border Controller functionality, including, SIP header manipulation, and topology hiding between the BT Wholesale Hosted SIP Trunking Service and the enterprise network.
- BT Wholesale Hosted SIP Trunking Service provided one trunk group with a DNS/SRV record for resilience. DID range assigned by BT Wholesale for this testing is +445600653xxx (12 digits).
  Because of security reasons, real DNS A-records and SRV record of BT Wholesale Hosted SIP Trunking Service are replaced with:
  - ipcomms-sipt-core2.bt.com
  - ipcomms-sipt-metro2.bt.com
  - _sip._udp.ipcomms-sipt-metrocore2.bt.com

Avaya SBCE does not support DNS/SRV in Server Configuration so only one DNS A-record is chosen to configure in Server Configuration of Avaya SBCE (**refer to BT Wholesale SIP Trunk Resilience in section 2.2**).

- All IP addresses shown below are private IP addresses except for B1 interface of Avaya SBCE.

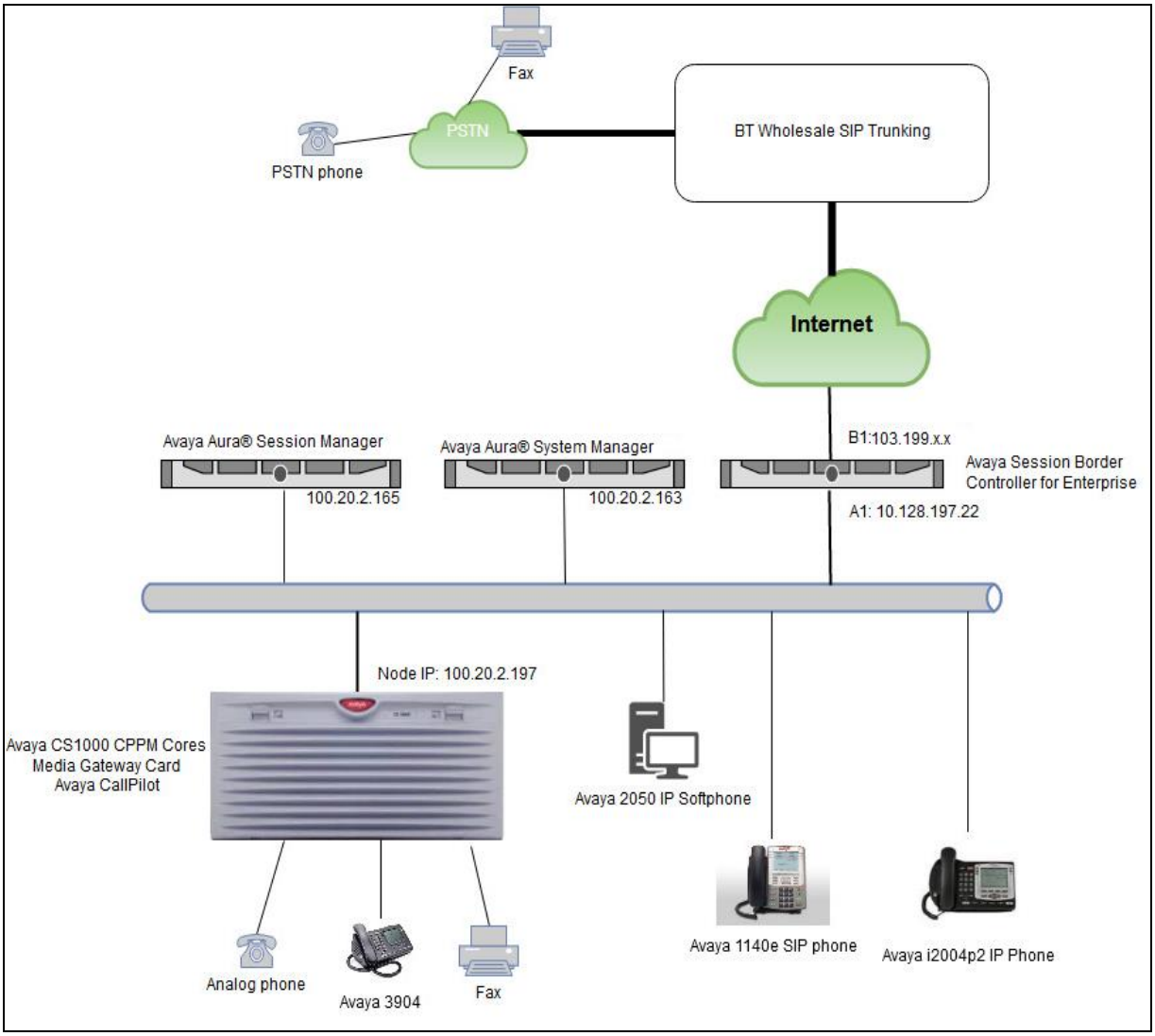


Figure 1: Network Components as Tested

4. Equipment and Software Validated

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

Component	Version
Avaya	
Avaya Aura® System Manager 7.0.1 SP2	7.0.1.2.086007
Avaya Aura® Session Manager 7.0.1 SP2	7.0.1.2.701230
Avaya Session Border Controller for Enterprise 7.1 SP2	7.1.0.2-01-13249
Avaya Communication Server 1000 7.6 SP8	Call Server 7.65 Service Pack 8 Signaling Server 7.65 Service Pack 8
Avaya CallPilot	5.1 SU4
Avaya i2004p2 Unistim phone	0604DCO
Avaya 1100 Series SIP phone	4.4.5
Avaya i2050 PC	4.4 SP7
Avaya 3904 Digital phone	9.3
Analog phone	N/A
Service Provider	
BT Wholesale Hosted SIP Trunking Service	SBC Genband Q20 9.1.13, Software Release of BroadWorks R20 SP1

Table 1: Software version

5. Configure Avaya CS1000

The configuration of the Avaya CS1000 outlined in these Application Notes uses the Incoming Digit Translation feature to receive calls, and the Trunk Steering Code (TSC) feature to route calls from the Avaya CS1000 to the PSTN via SIP trunks to the BT Wholesale Hosted SIP Trunking Service.

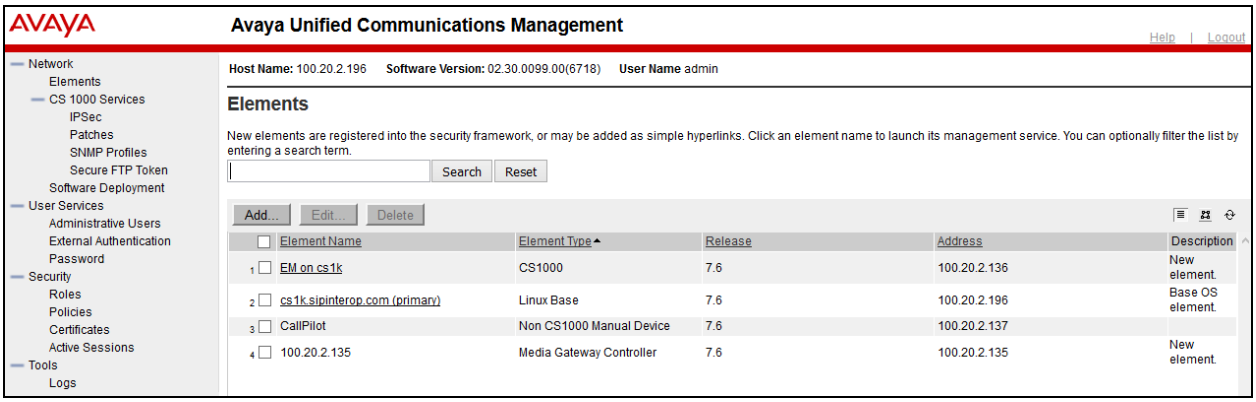
These Application Notes assume that the basic Avaya CS1000 configuration has already been administered. For further information on Avaya CS1000, please consult the references in **Section 10**. The procedures below describe the configuration details for configuring the Avaya CS1000.

5.1 Access to Avaya CS1000 System

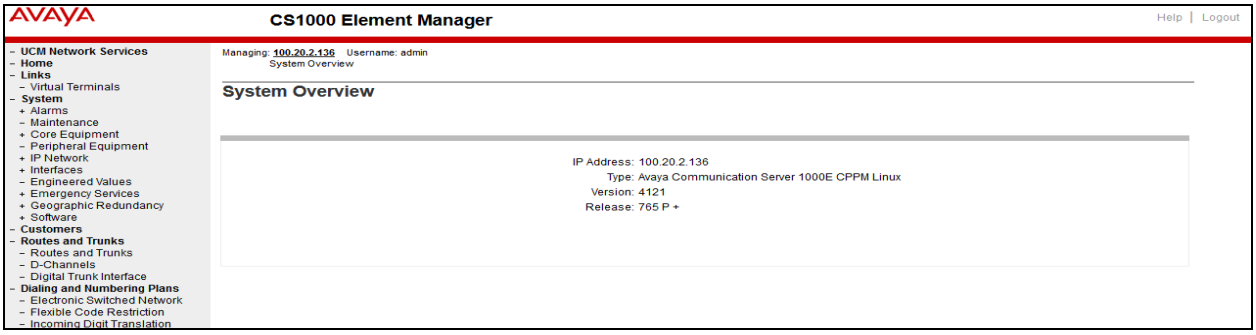
Changes to Avaya CS1000 can be made using Element Manager, which is accessible from Unified Communications Management (UCM) and offers the user a Web GUI for making changes. Changes to Avaya CS1000 can also be made using the Command Line Interface (CLI) offered using PuTTY to make an SSH connection.

5.1.1 Access to Avaya 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 Avaya CS1000 Element: "**EM on cs1k**". The Avaya CS1000 Element Manager **System Overview** page is displayed as shown below:



5.1.2 Access Avaya CS1000 Call Server by using CLI

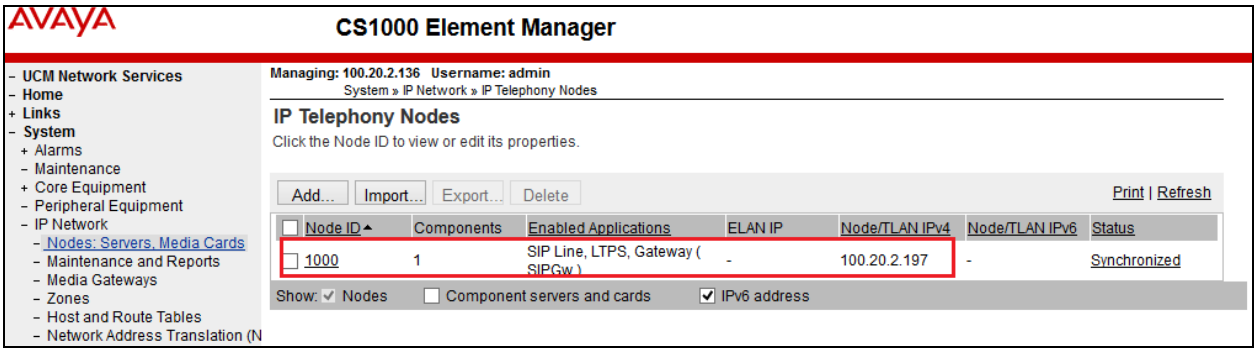
Using Putty to open an SSH session to the IP address of Avaya CS1000 Signaling Server then log in with administrator credentials. Run the command **cslogin** and log in with the appropriate user account and password. Sample output is shown below.

```
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@100.20.2.196's password:
Last login: Tue Sep 20 16:57:20 2016 from 100.20.2.189
[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
>
```

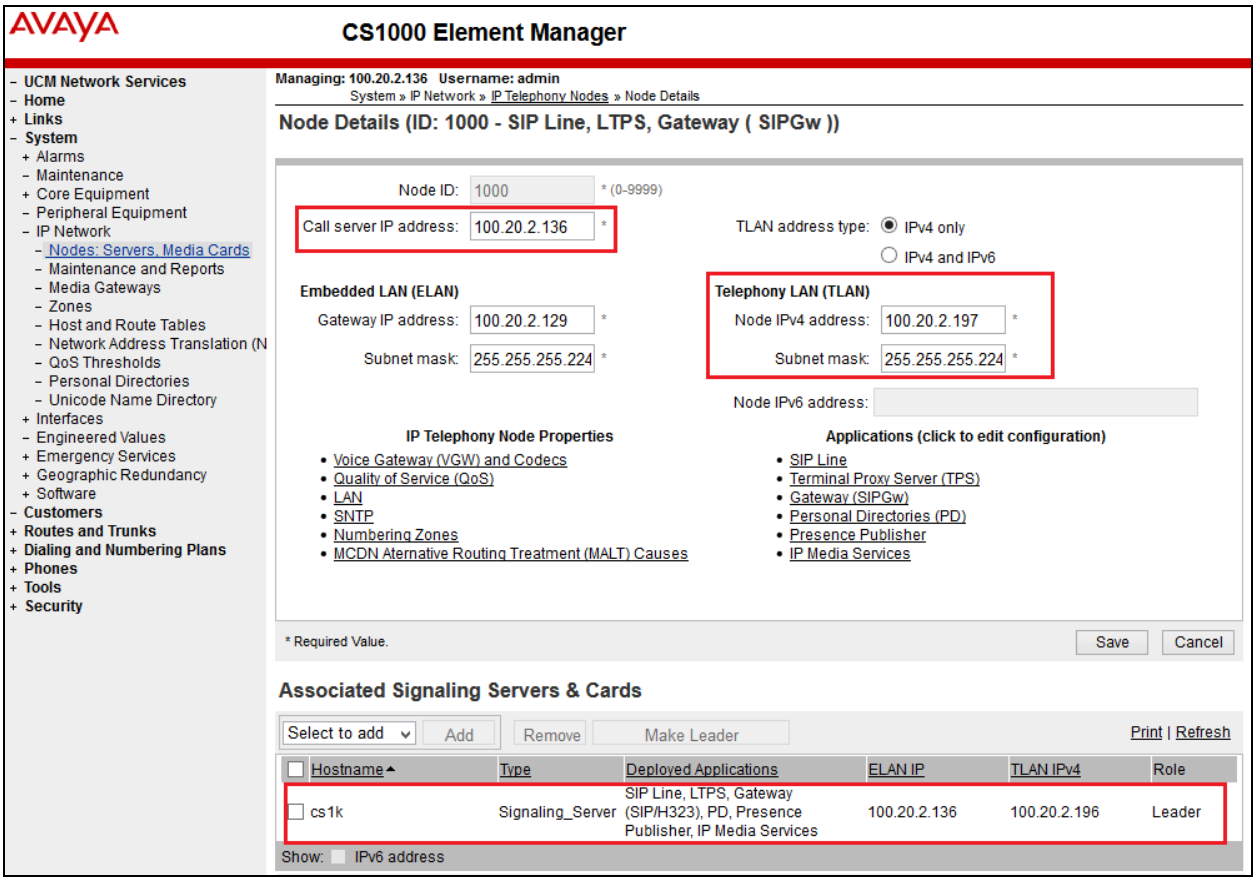
5.2 Administer IP Telephony Node

5.2.1 Obtain Node IP address

These Application Notes assume that the basic Avaya 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 Avaya CS1000 IP network to work with BT Wholesale Hosted SIP Trunking Service. 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**:**

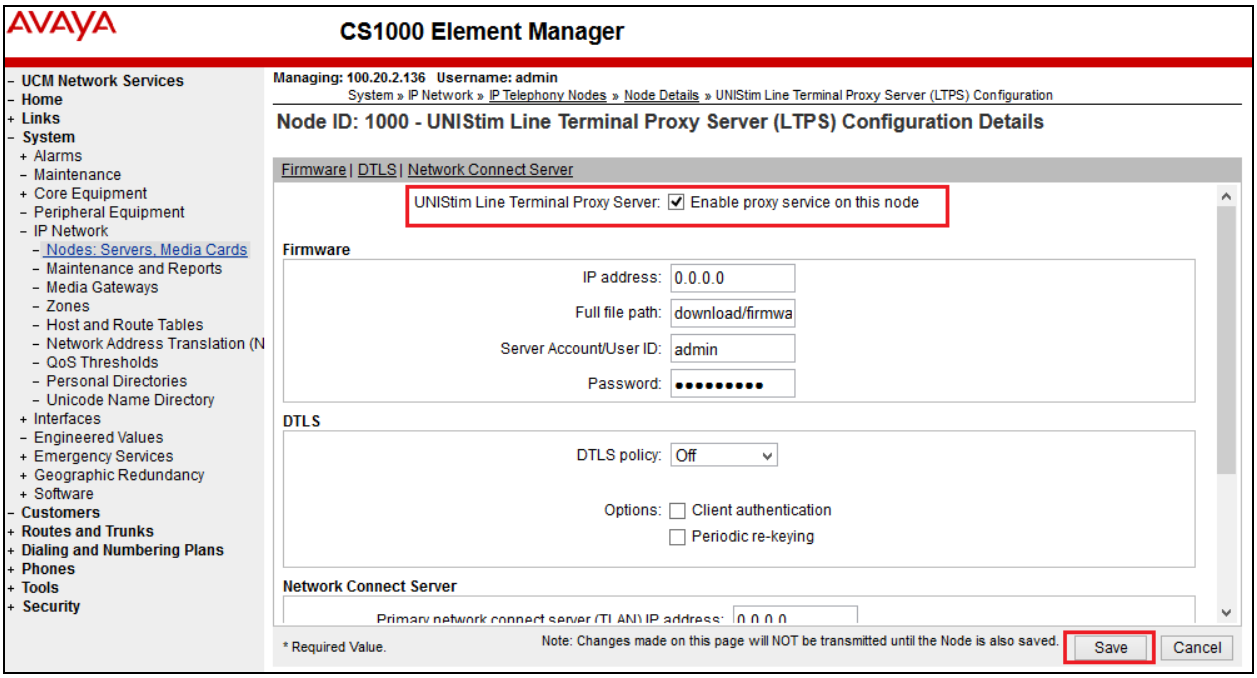


The **Node Details** screen is displayed with the IP address of the Avaya CS1000 node: **Call server IP address: 100.20.2.136**. The **Node IPv4 address 100.20.2.197** for **Telephony LAN (TLAN)** is a virtual address which corresponds to the **TLAN IPv4** address **100.20.2.196** of the Signaling Server/SIP Signaling Gateway. The SIP Signaling Gateway uses this Node IP address to communicate with other components to process SIP calls.



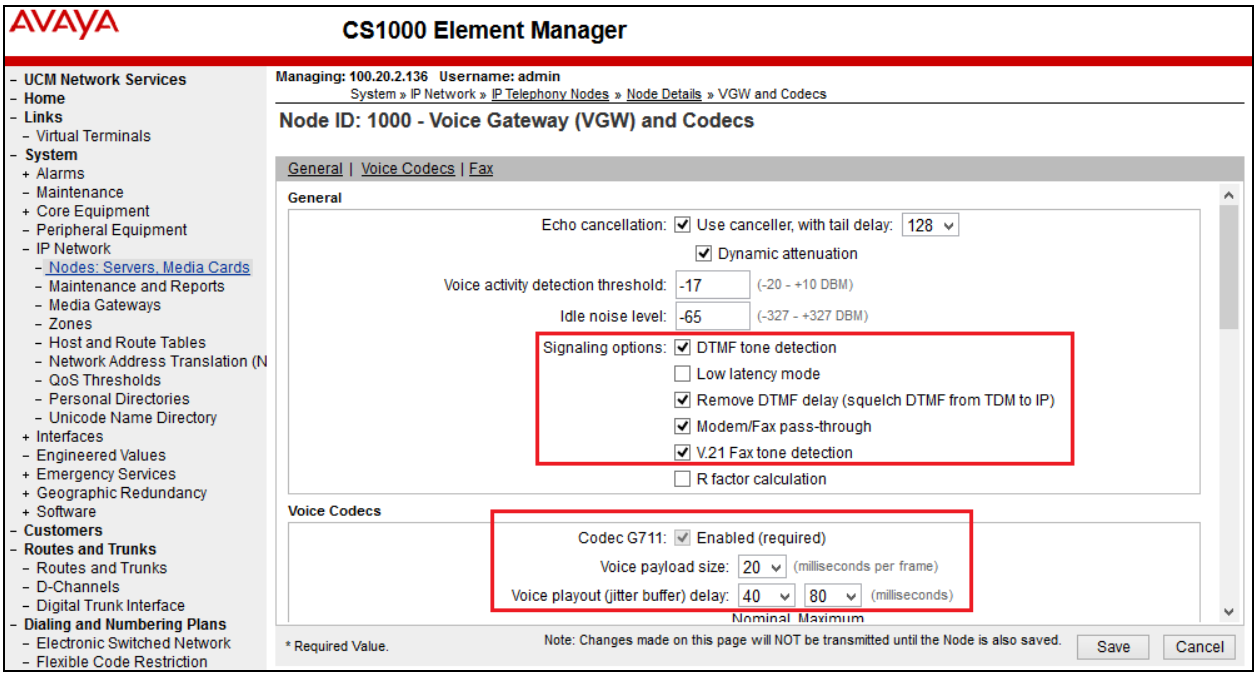
5.2.2 Administer Terminal Proxy Server (TPS)

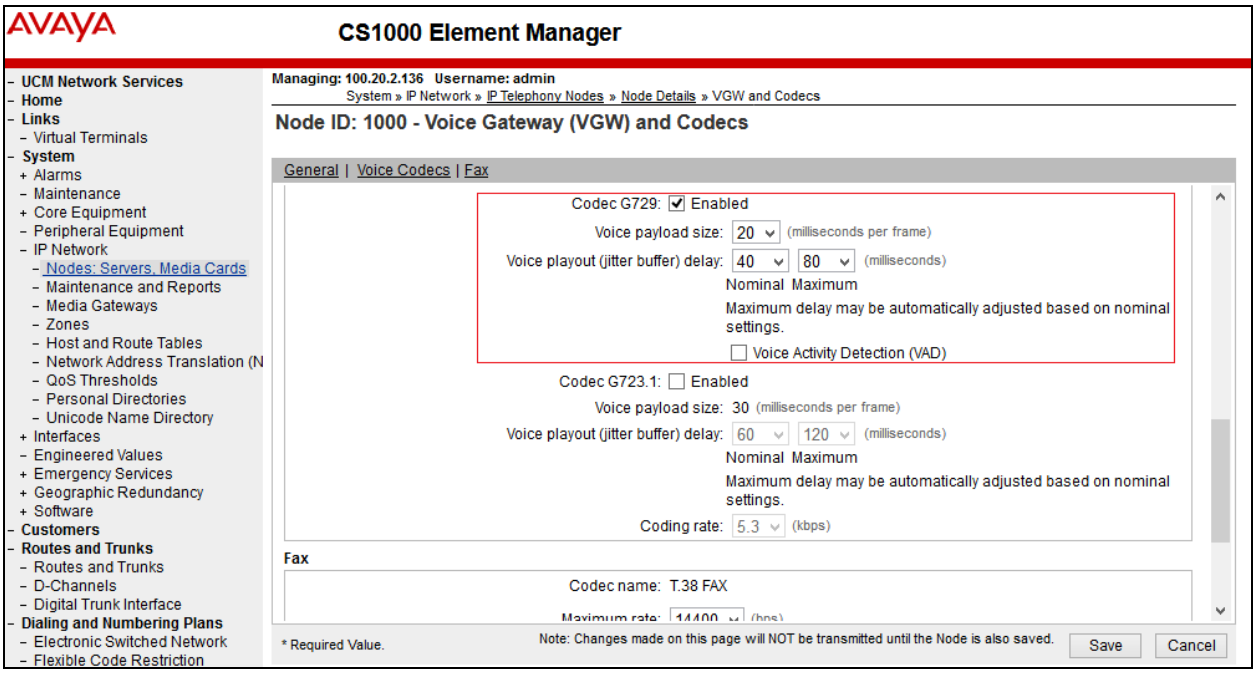
Continuing from **Section 5.2.1**, on the **Node Details** page, select the **Terminal Proxy Server** (**TPS**) link then check the **UNIStim Line Terminal Proxy Server** box to enable proxy service on this node and click on **Save** button:

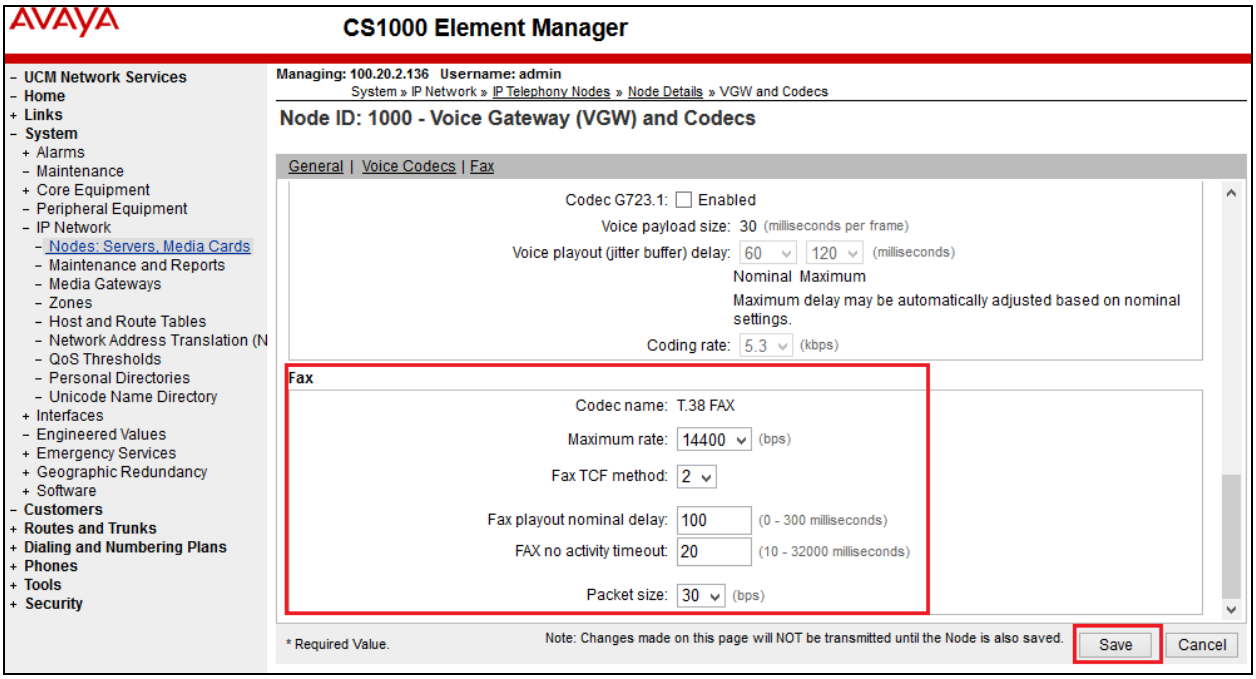


5.2.3 Administer Voice Codecs

On the **Node Details** page shown in **Section 5.2.1**, click on **Voice Gateway (VGW) and Codecs**. Make sure **T.38 FAX**, **G.711** and **G.729** are configured as shown below then click on **Save** button:







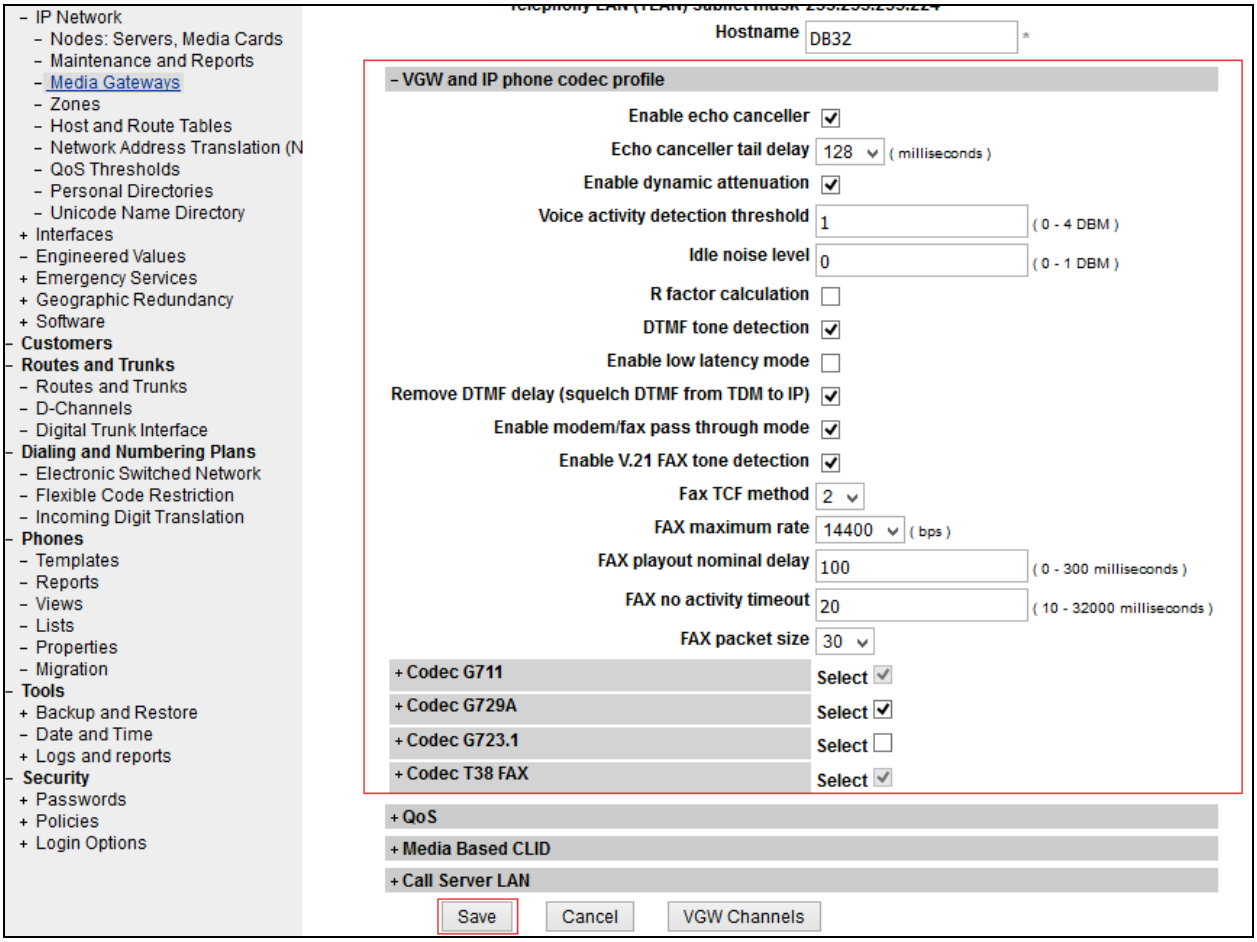
5.2.4 Synchronize New Configuration

On **Node Details** page shown in **Section 5.2.1**, click on **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, navigate to **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 modem/fax pass through mode** box then scroll down to make sure only Codec **G.711**, **G.729A** and **T.38 FAX** are selected. Scroll down to the bottom of the page and click on the **Save** button.



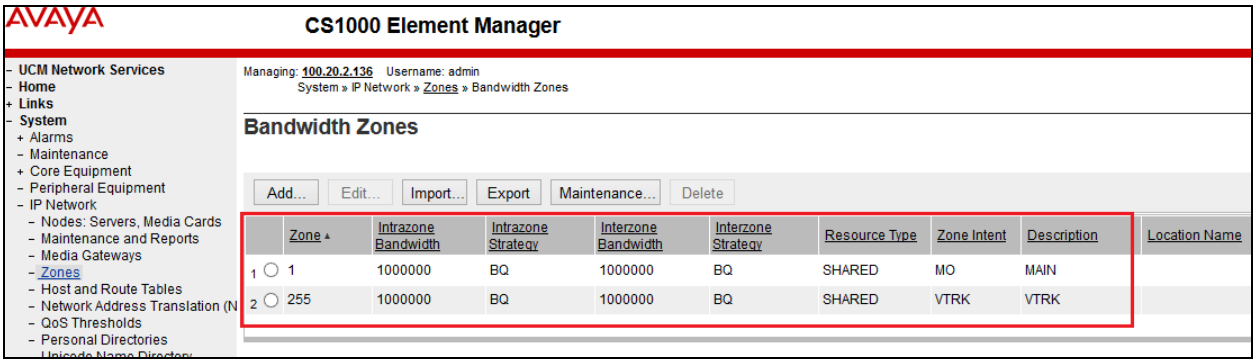
5.3 Zones and Bandwidth Management

Navigate to **System** > **IP Network** > **Zones** from the left pane (not shown), click on **Bandwidth Zones** (not shown). Click on **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.

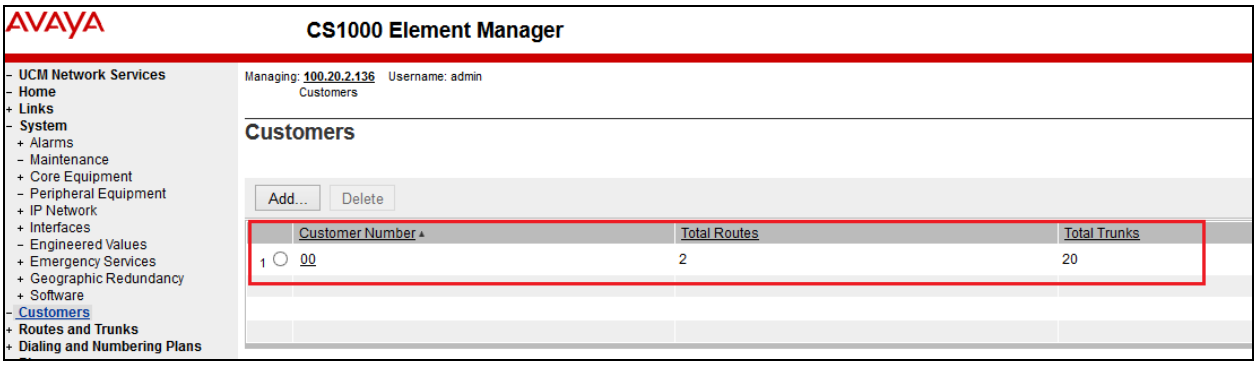


5.4 Administer SIP Trunk

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

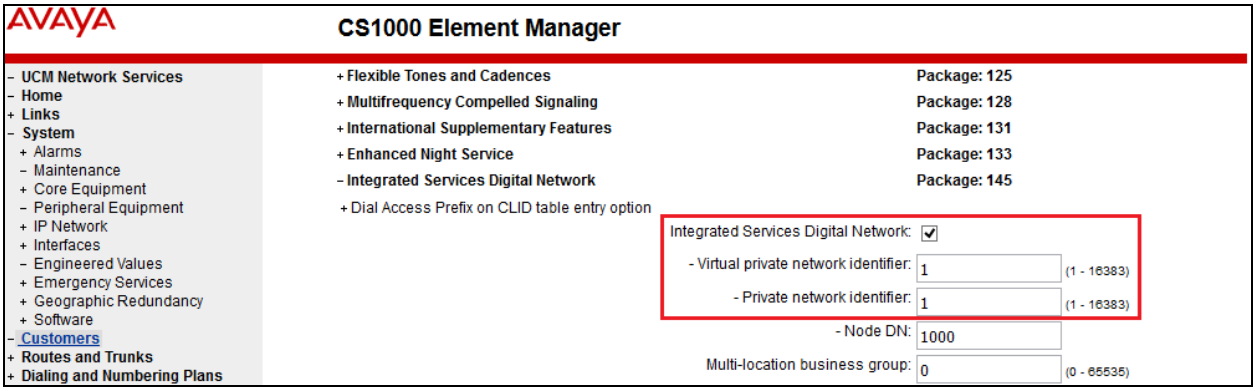
5.4.1 Integrated Services Digital Network (ISDN)

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 (not shown).

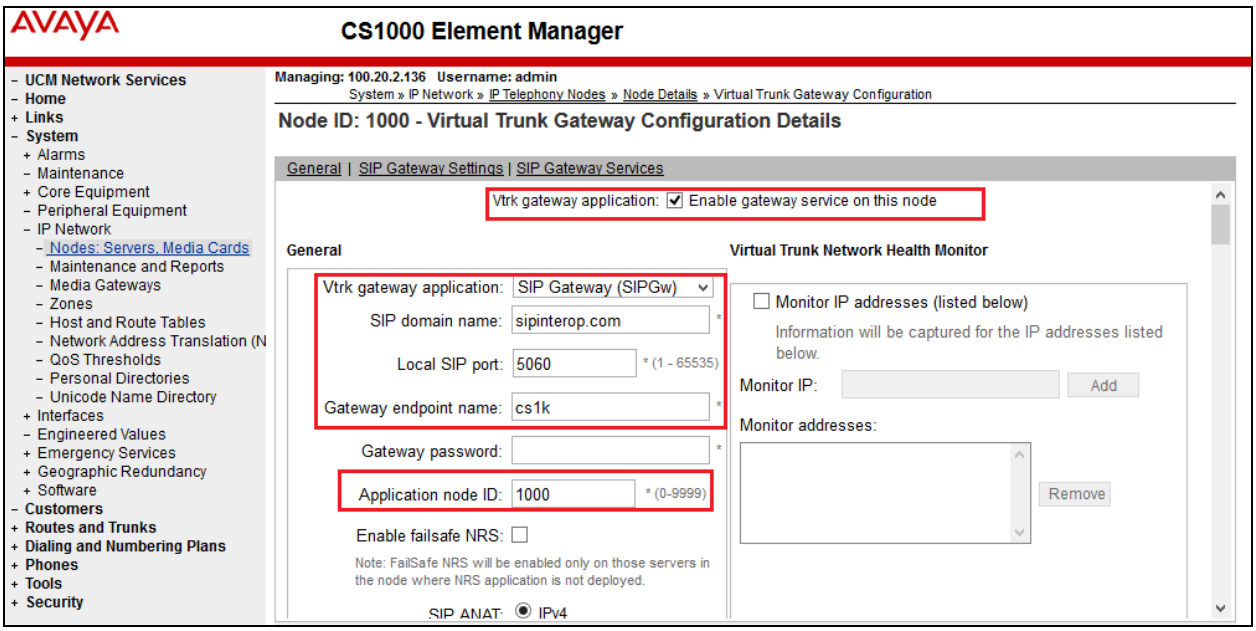
The screen is updated with a list of available **Feature Packages**. Select **Integrated Services Digital Network** to edit the parameters shown below. Check the **Integrated Services Digital Network** option, enter **1** into **Virtual private network identifier** and **Private network identifier**,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



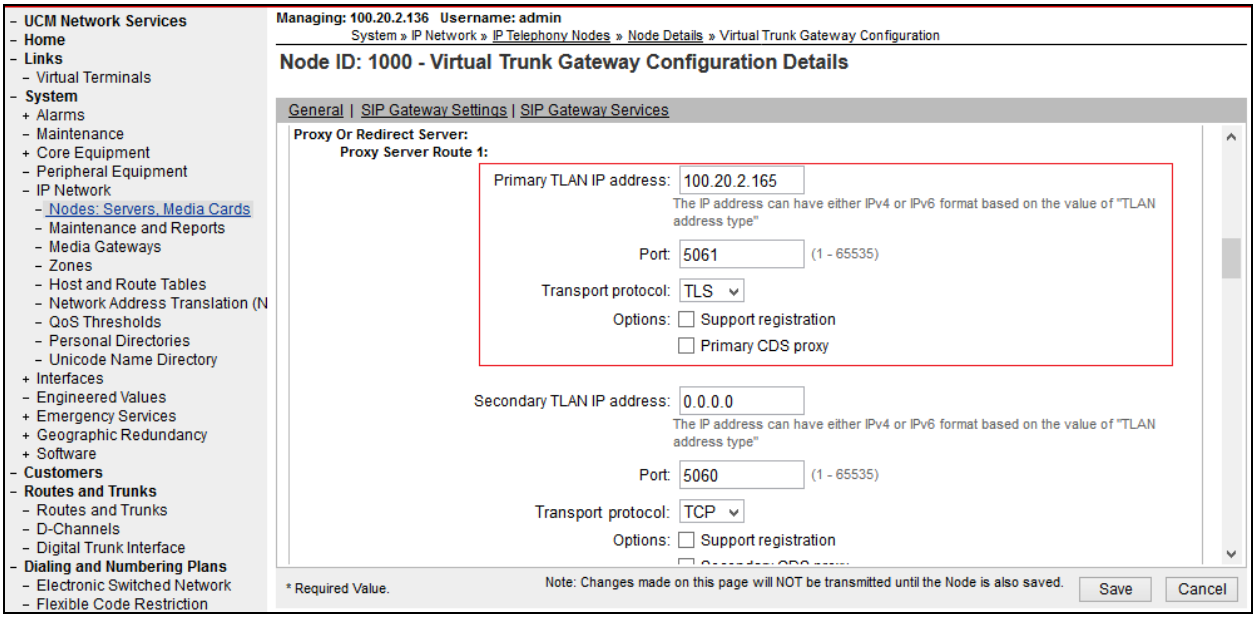
5.4.2 Administer SIP Trunk Gateway

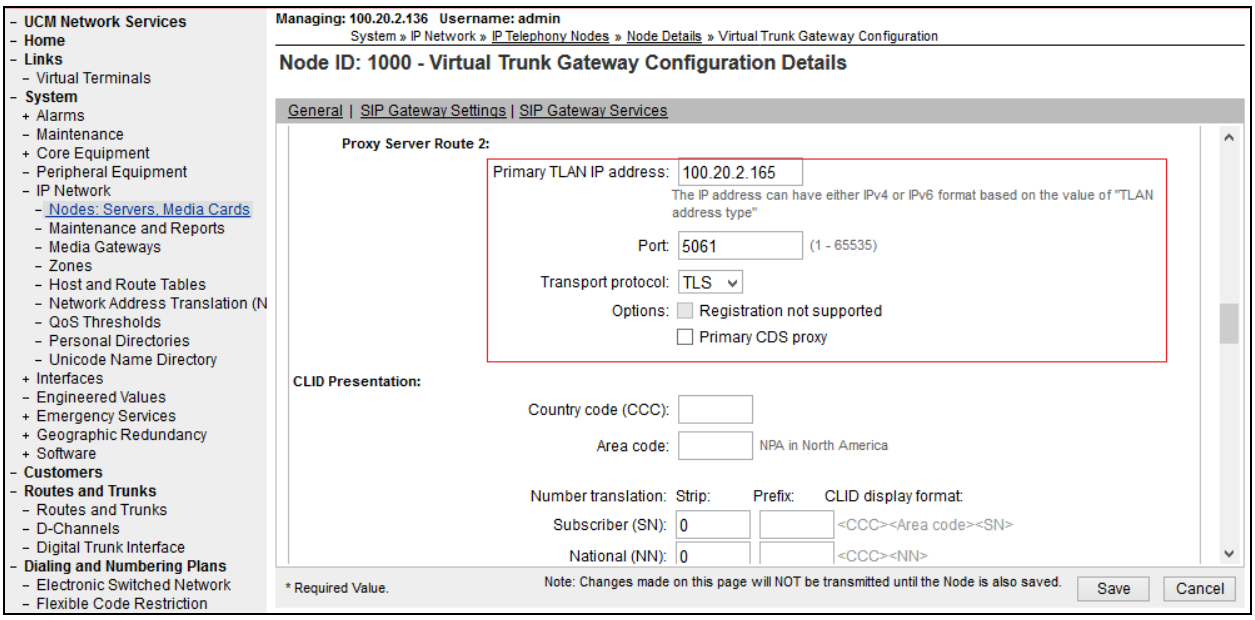
Navigate to **System > IP Network > Nodes: Servers, Media Cards** from the left pane. In the **IP Telephony Nodes** screen displayed (not shown), select the **Node ID** of the CS1000 system. The **Node Details** screen is displayed as shown in **Section 5.2.1**.

On the **Node Details** screen, select **Enable gateway service on this node** 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 Session Manager in **Section 6.2**, and **6.5**.



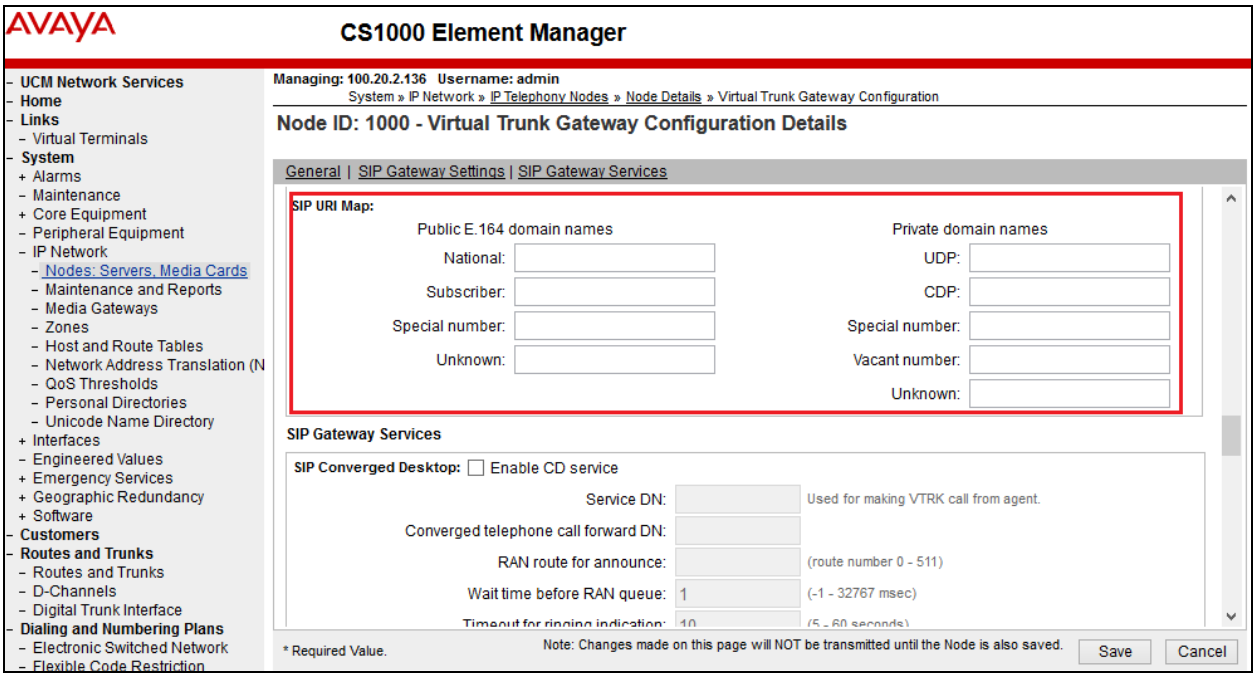
Click on the **SIP Gateway Settings** tab. Under **Proxy or Redirect Server**, enter the following values (highlighted in red boxes) for the specified fields and retain the default values for the remaining fields, as shown below. Enter the IP address of Session Manager in the **Primary TLAN IP address** field. Enter **5061** for **Port** and select **TLS** 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**.



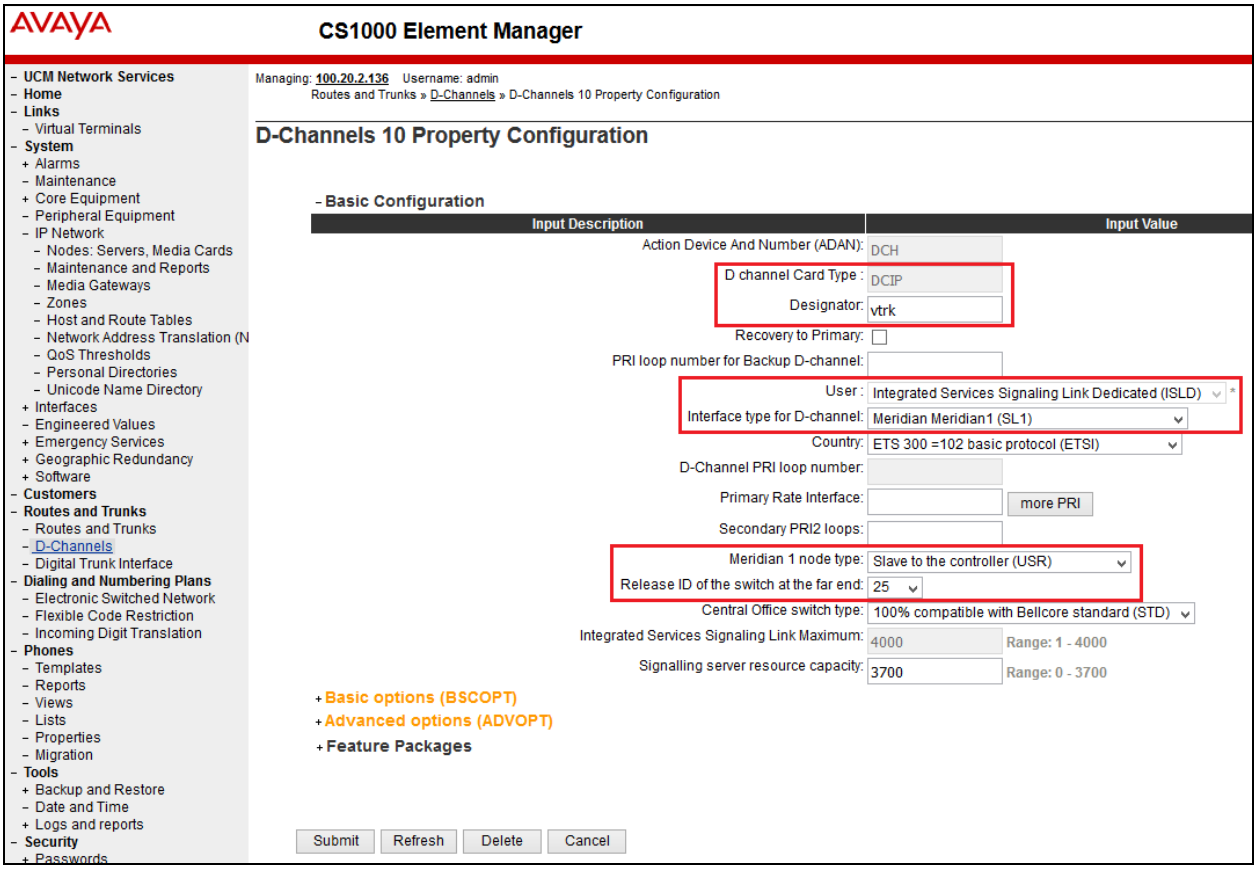
Synchronize the new configuration (please refer to **Section 5.2.4**).

5.4.3 Administer Virtual D-Channel

Navigate to **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 on **Add** button (not shown).

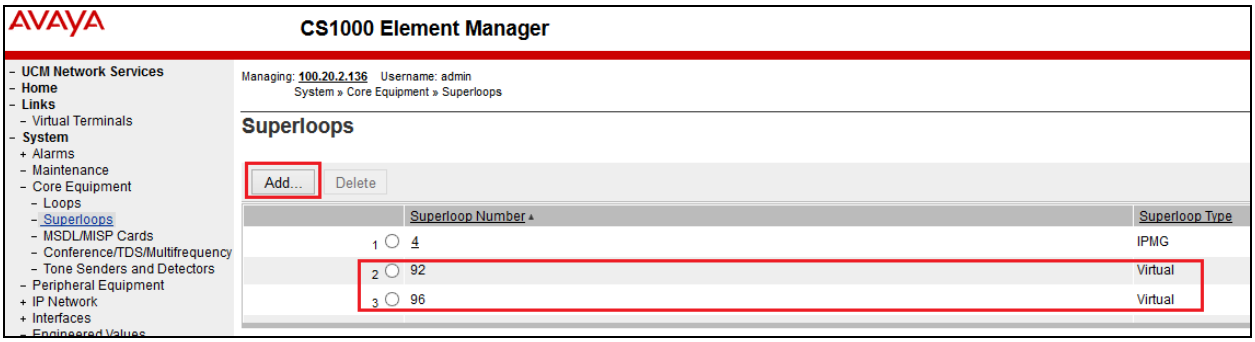
The **D-Channels 10 Property Configuration** screen is displayed next, as shown below. Enter the following values for the specified fields, and retain the default values for the remaining fields.

- **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**.



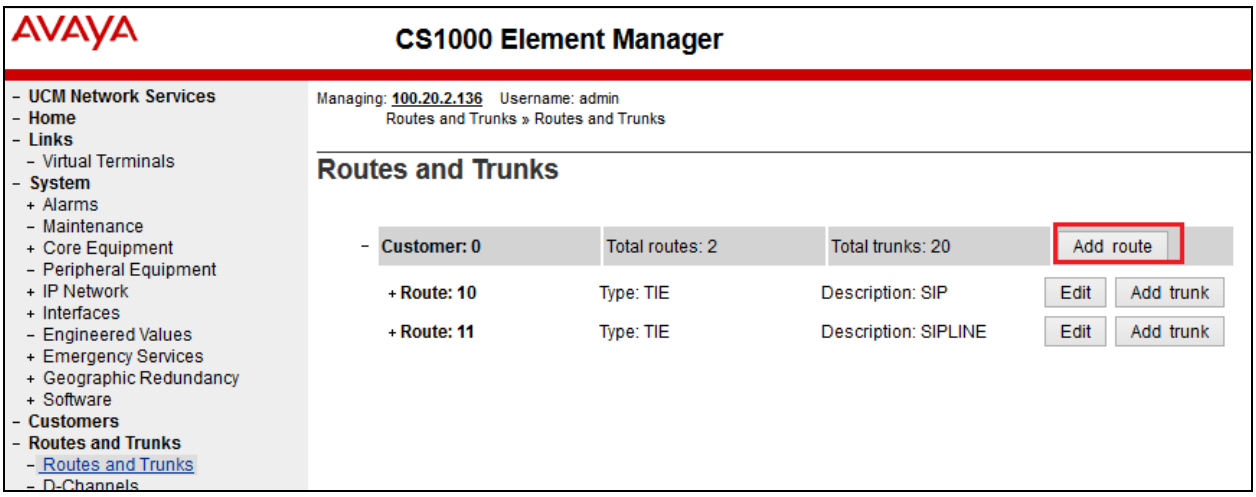
5.4.4 Administer Virtual Super-Loop

Navigate to **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 92, 96** have been added and were being used.



5.4.5 Administer Virtual SIP Routes

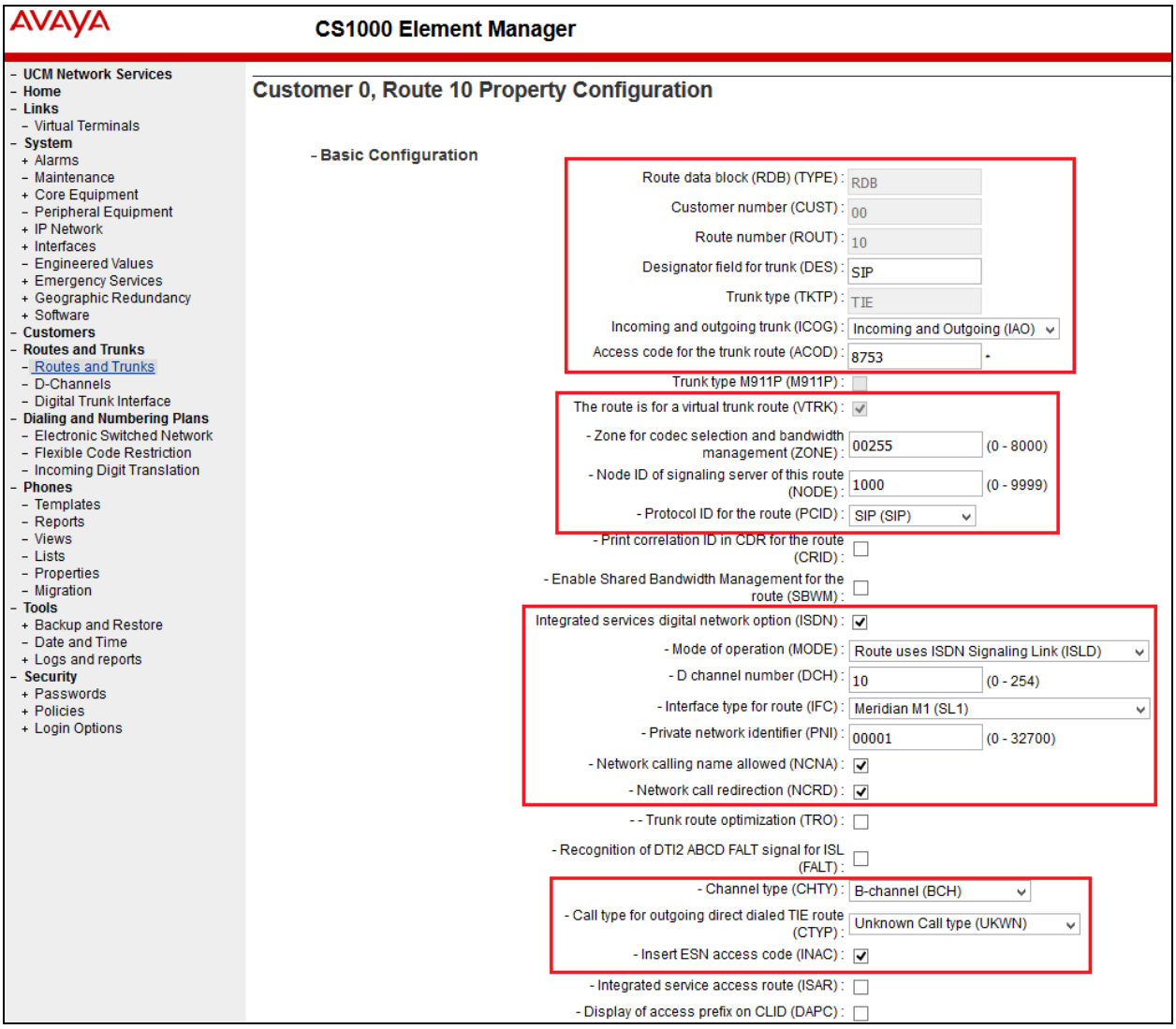
Navigate to **Routes and Trunks > Routes and Trunks** (not shown) from the left pane to display the **Routes and Trunks** screen. In this example, **Customer 0** was being used. Click on the **Add route** button as shown below.



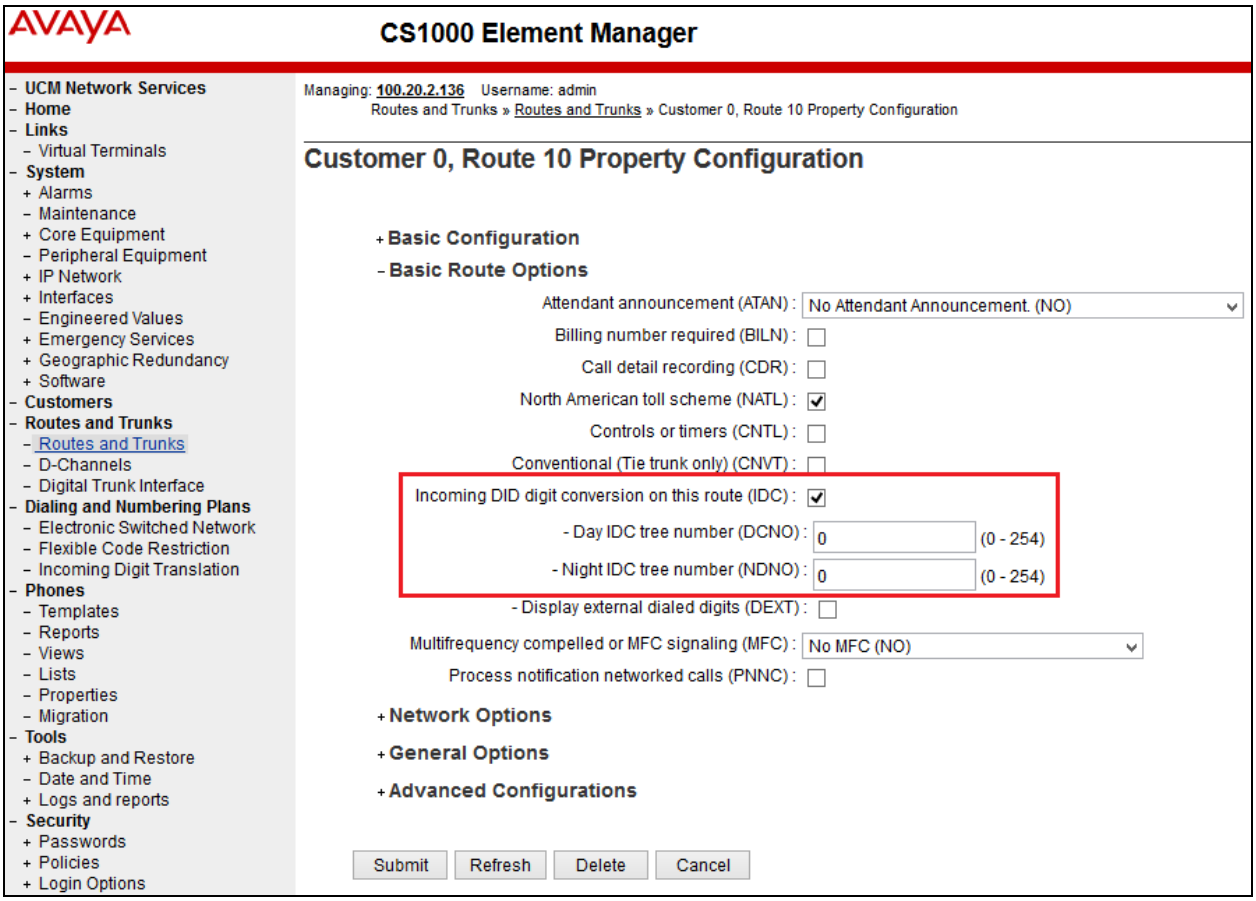
The **Customer 0**, **New Route Configuration** screen is displayed next (not shown). The **Basic Configuration** section is displayed. Enter the following values for the specific fields, and retain the default values for the remaining fields. The screenshot of **Basic Configuration** section of existing **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: **8753**)
- 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 the **Incoming DID digit conversion on this route (IDC)** box. Enter **0** for both **Day IDC tree number** and **Night IDC tree number**.



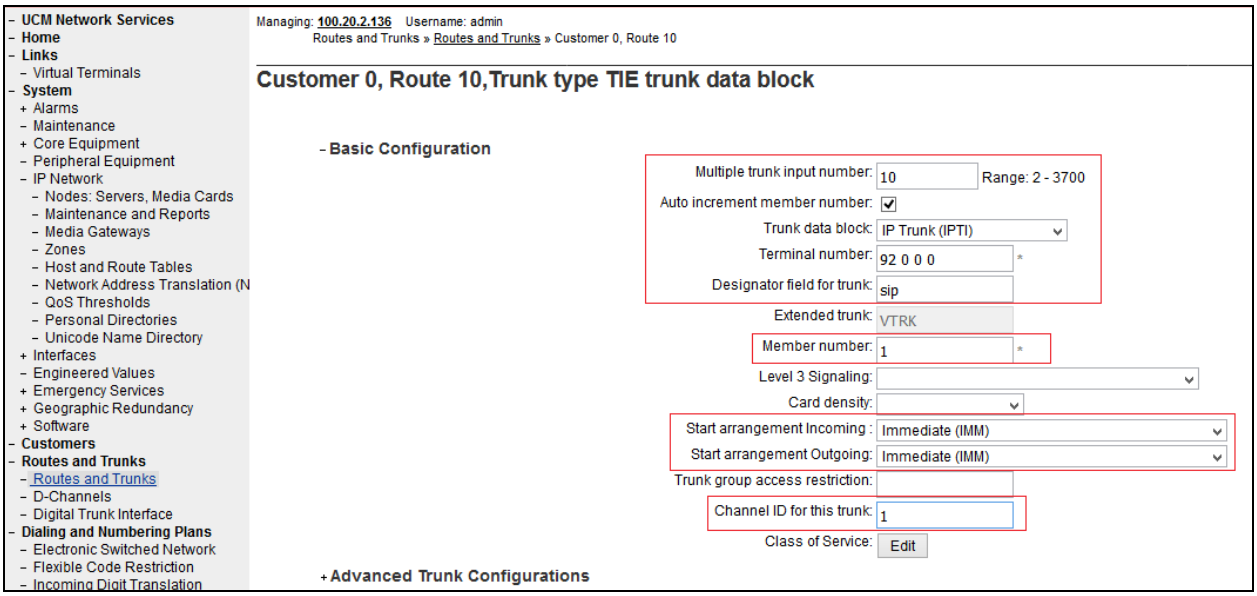
5.4.6 Administer Virtual Trunks

Navigate to **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).

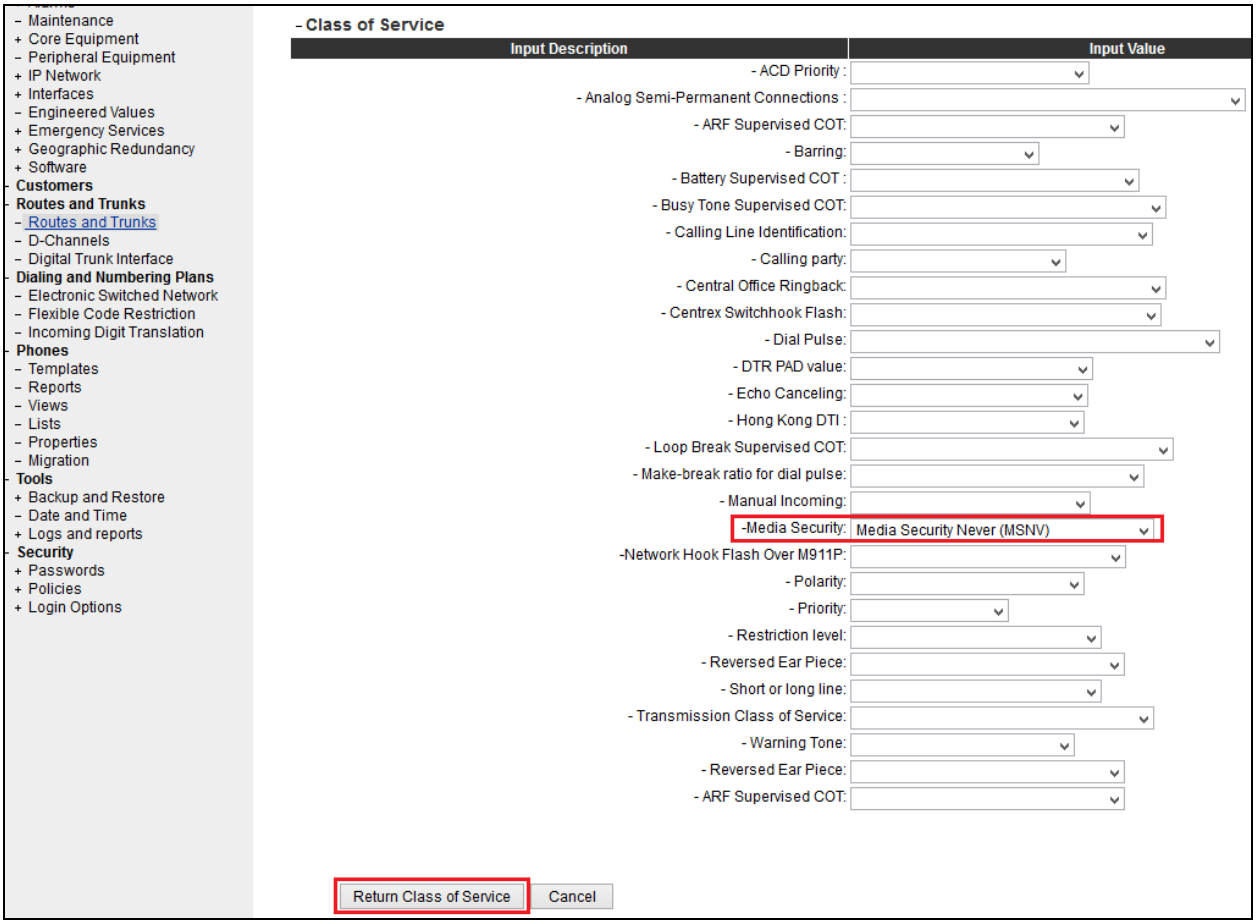
The **Customer 0, Route 10, Trunk type TIE trunk data block** screen is displayed. Enter the following values for the specified fields and retain the default values for the remaining fields. Media Security (sRTP) needs to be disabled at the trunk level by editing the **Class of Service (CLS)** at the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

In the sample configuration, 10 trunks were created.

- **Multiple trunk input number:** Enter the number of channels (in this example, there are 10 channels).
- Select **Auto increment member number**.
- **Trunk data block: IP Trunk (IPTI)**.
- **Terminal Number**: Available terminal number (**Superloop 92** created in **Section 5.4.4**).
- **Designator field for trunk**: A descriptive text (**sip**).
- **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.

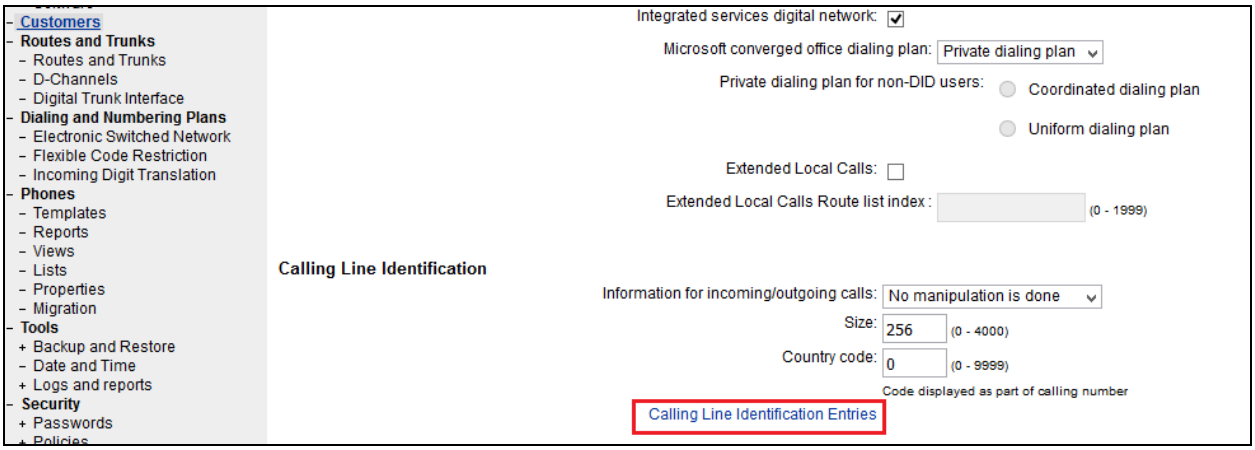


For **Media Security**, select **Media Security Never** (**MSNV)**. Enter the values for the specified fields as shown below. Scroll down to the bottom of the screen and click **Return Class of Service** and then click on the **Save** button (not shown).



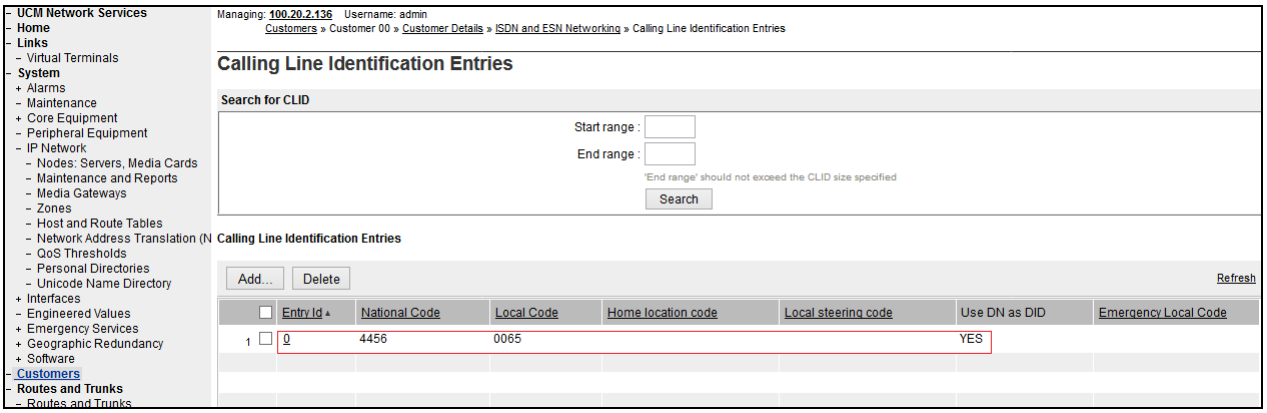
5.4.7 Administer Calling Line Identification Entries

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



Click on **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**: Enter **4456**.
- **Local Code**: Enter **0065**.
- **Home Location Code**: Leave blank
- **Local Steering Code**: Leave blank.
- **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**.

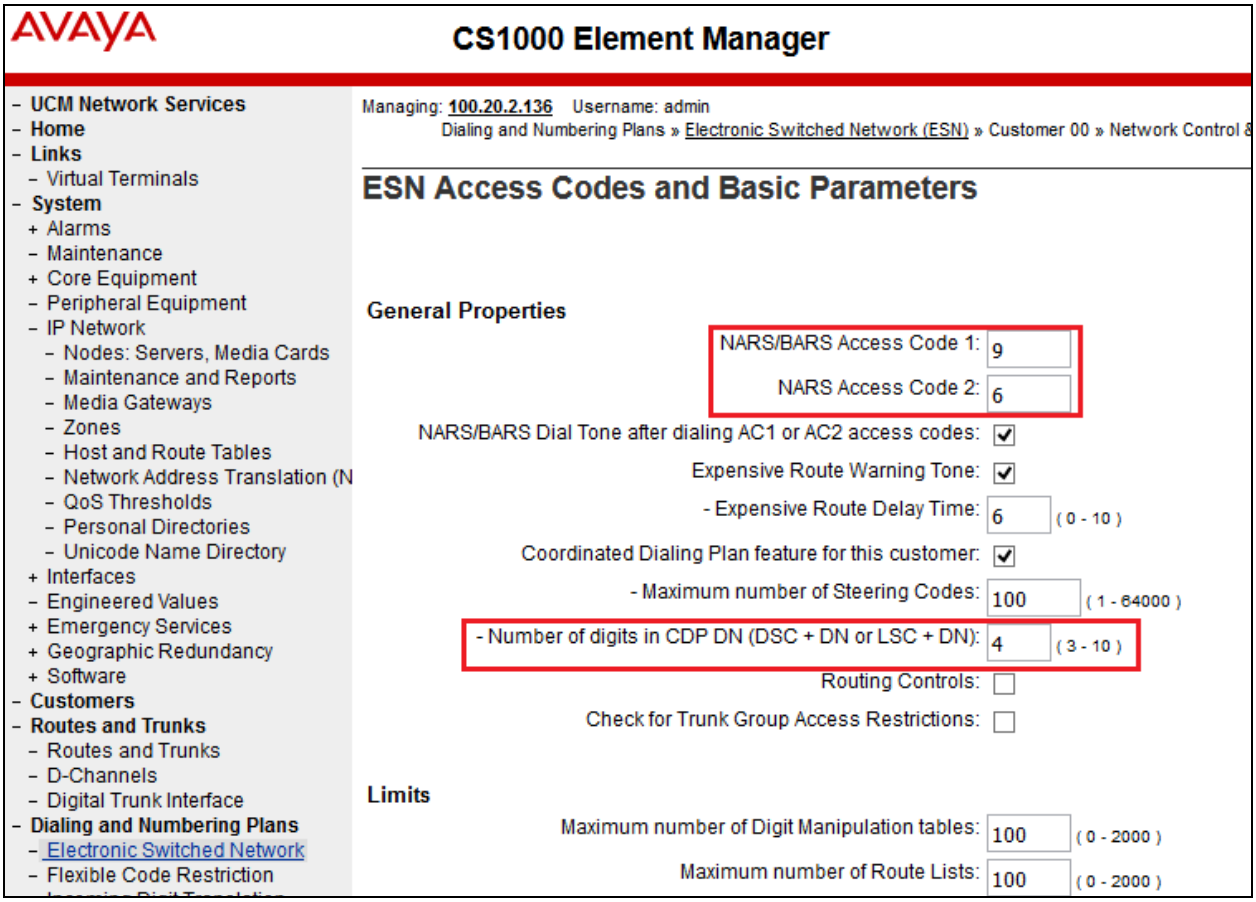
```
>ld 15
CDB000
MEM AVAIL: (U/P): 33600126 USED U P: 8345621 954062 TOT: 45579868
DISK SPACE NEEDED: 1722 KBYTES
REQ: chg
TYPE: net
TYPE NET_DATA
CUST 0
OPT
…
TRNX YES → Enable transfer feature
EXTT YES → Enable external trunk to trunk transfer
…
```

5.5 Administer Dialing Plans

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

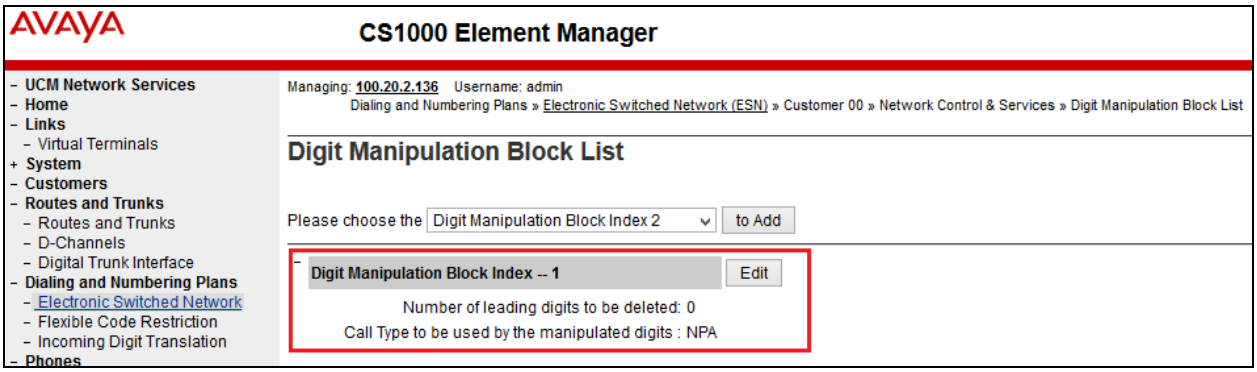
5.5.1 Define ESN Access Codes and Parameters (ESN)

Access the CS1000 Element Manager then navigate to **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**, **NARS Access Code 2** and **Number of digits in CDP DN (DSC+DN or LSC+DN)** as shown below.



5.5.2 Digit Manipulation Block Index (DMI)

In this sample configuration, **Digit Manipulation Block Index 1** was added as shown below.

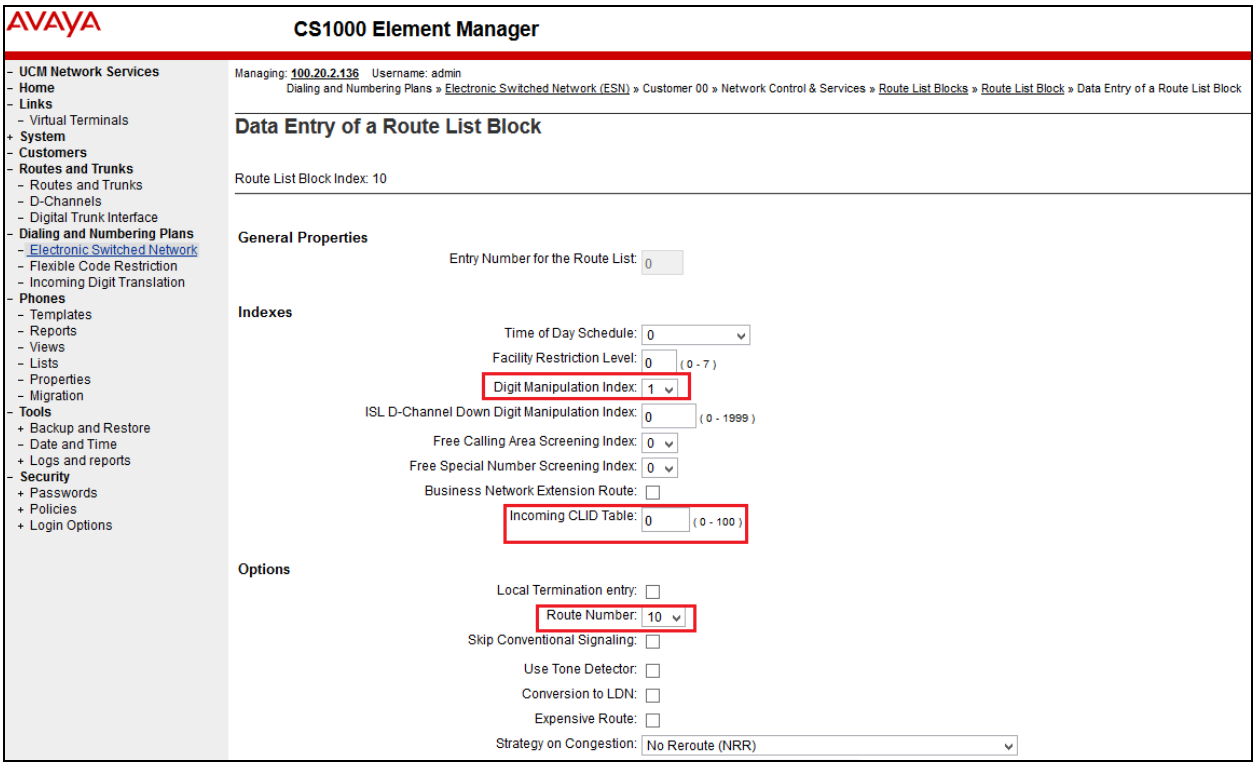


5.5.3 Route List Block Index

Navigate to **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**: **1**.
- **Incoming CLID Table**: **0** (created in **Section 5.4.7**).
- **Route number: 10** (created in **Section 5.4.5**).



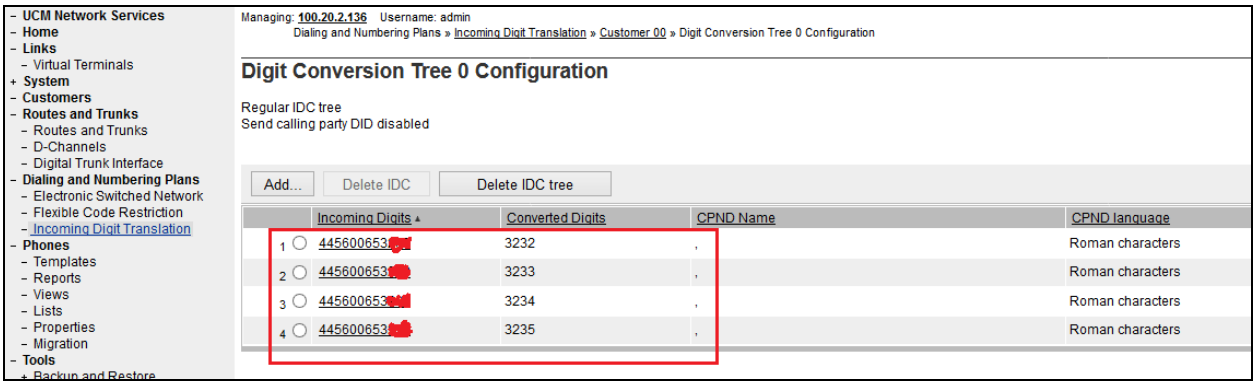
5.5.4 Incoming Digit Translation Configuration

Navigate to **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 Avaya 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 445600653xxx will be translated to the associated DN with 4 digits.

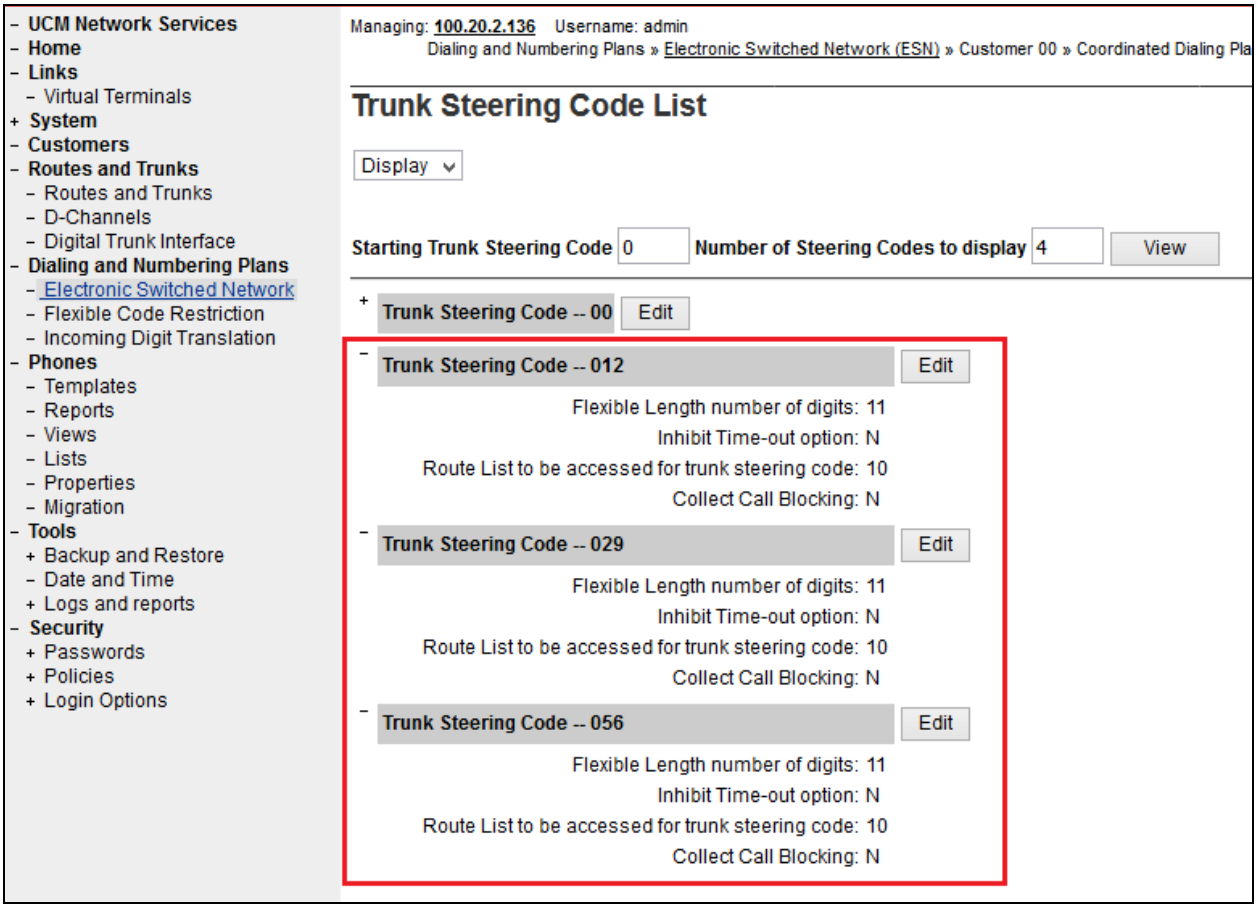
Note: For confidentiality and privacy purposes, the actual 4 remaining digits used for DID numbers in this testing have been masked.



5.5.5 Outbound Call – Trunk Steering Code Configuration

The Trunk Steering Code **012, 029** and **056** were added for making outbound call to BT Wholesale. This number was associated to **Route list index 10** created in **Section 5.5.3**.

Navigate to **Dialing and Numbering Plans > Electronic Switched Network** from the left pane to display the **Electronic Switched Network (ESN)** screen. Select **Trunk Steering Code (TSC)**. Enter a TSC number and then click on **Add** button. Below figure shows the TSC number used for this testing.

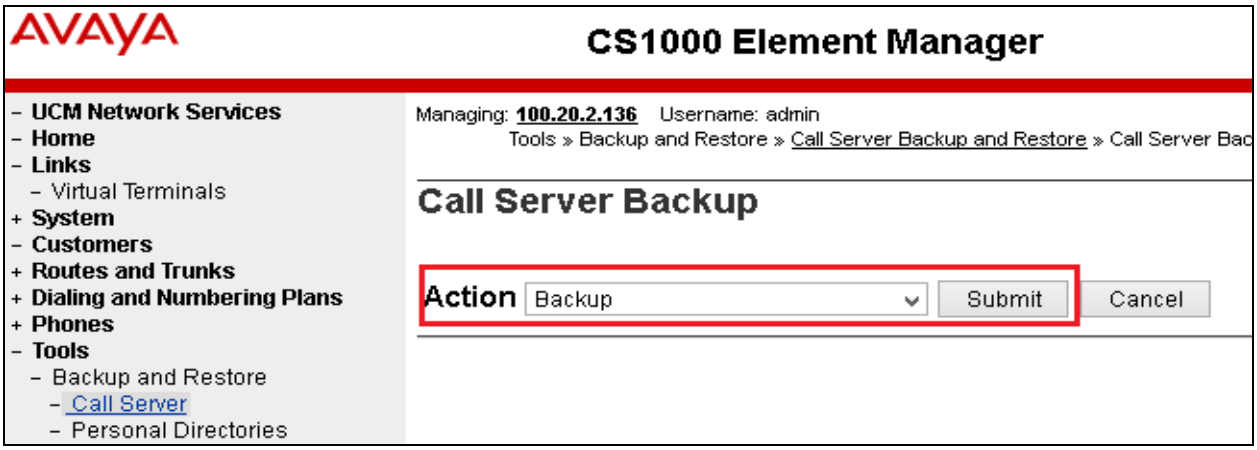


5.6 Enable Plug-ins on CS1000

In order for off-net call transfer to operate successfully, **plug-in 201** must be enabled on CS1000. Please refer to **CS 1000 Plug-in Feature** document which is available at https://downloads.avaya.com/css/P8/documents/100166144 .

5.7 Save the configuration

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



The backup process will take several minutes to complete.

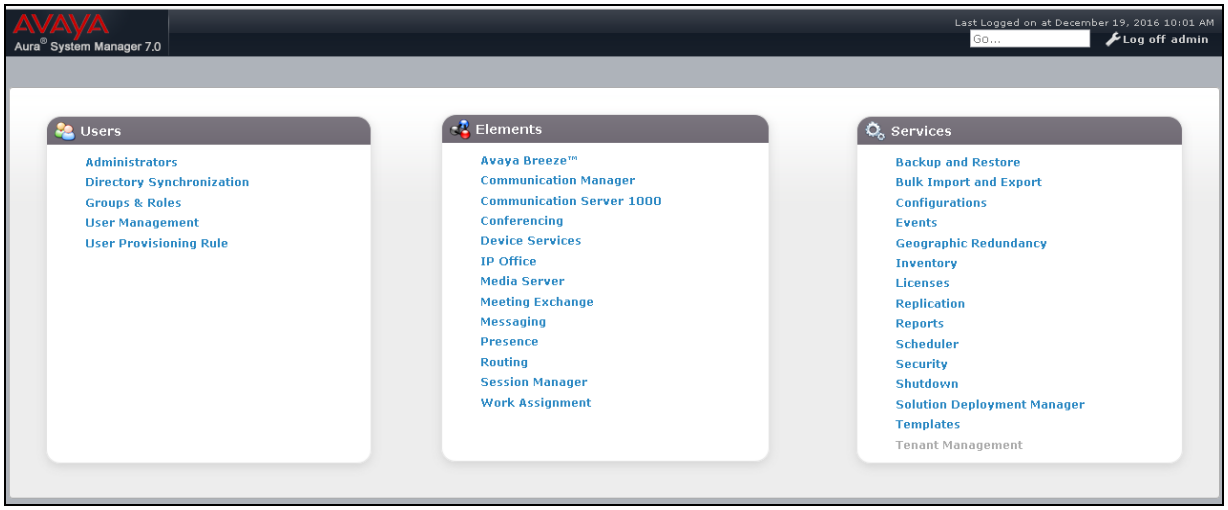
6. Configure Avaya Aura® Session Manager

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

- SIP domain.
- Logical/physical Location that can be used by SIP Entities.
- Adaptations.
- SIP Entities corresponding to Avaya 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.
-

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 click 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:

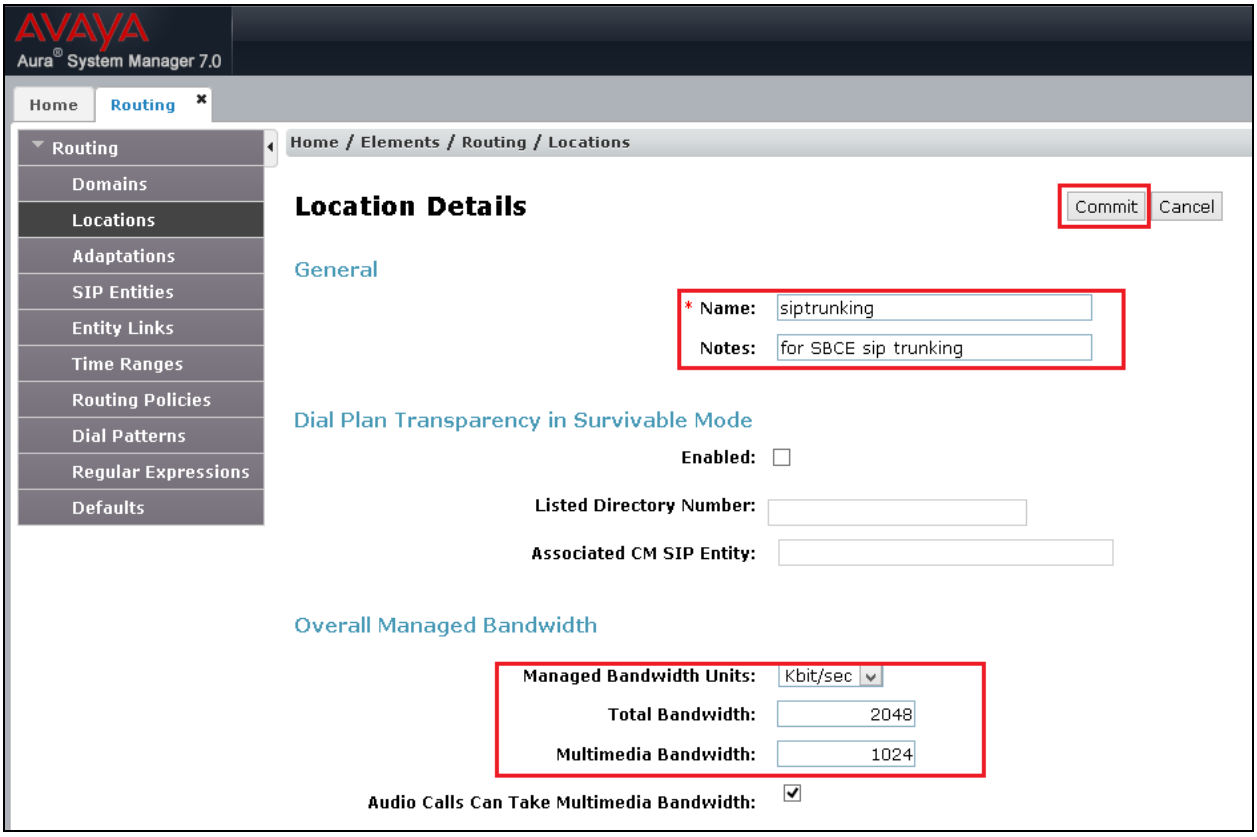
1. Select **Domains** from the left navigation menu. In the reference configuration, domain **sipinterop.com** was defined.
2. Click **New** (not shown). Enter the following values and use default values for remaining fields.
   - **Name**: Enter the enterprise SIP Domain Name. In the sample screen below, **sipinterop.com** 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 **siptrunking** was configured.

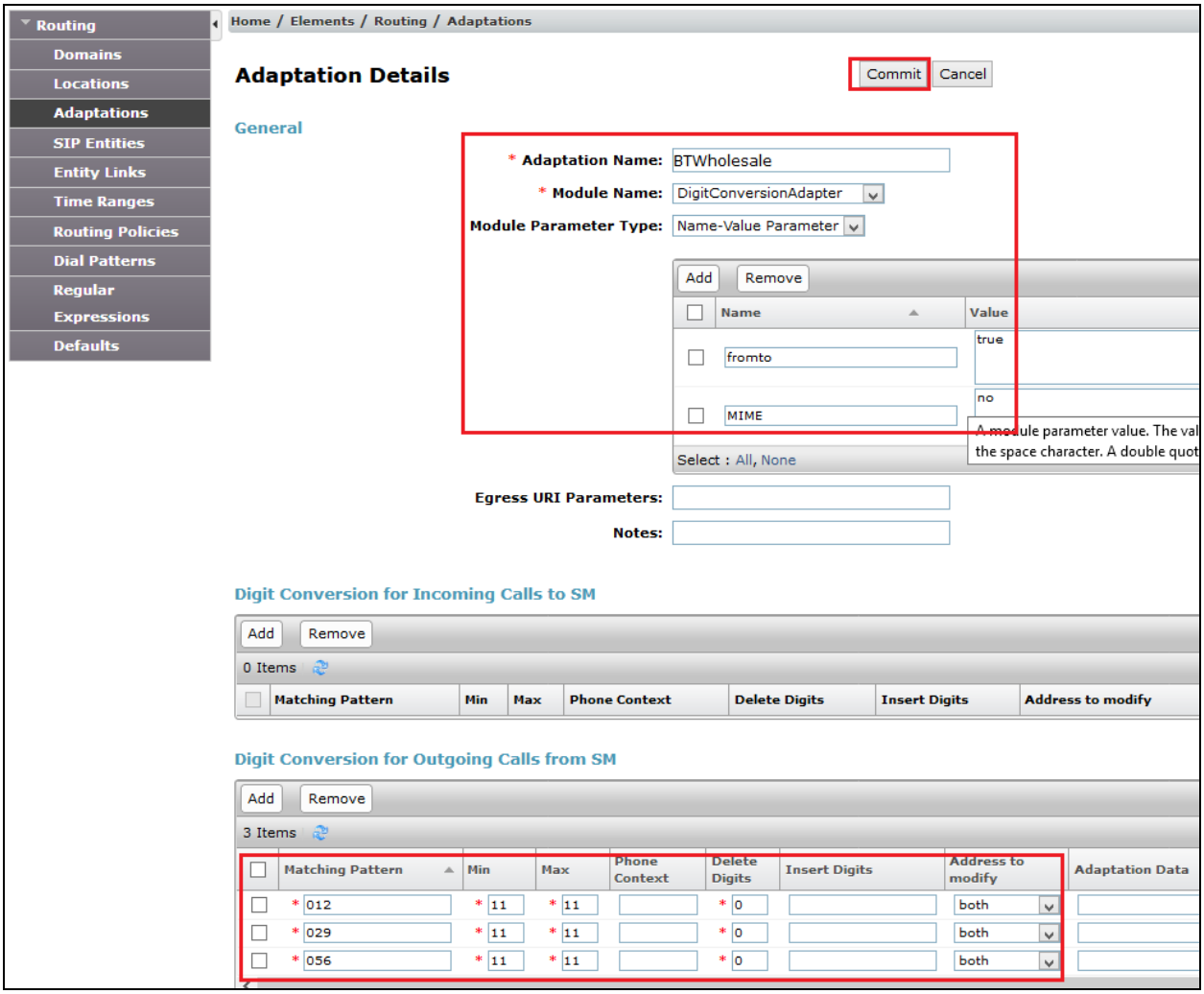
Follow the steps shown below:

1. Select **Locations** from the left navigational menu. Click on **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., **siptrunking**).
   - **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 on **Commit** to save.



6.3 Configure Adaptations

An Adaptation was configured to remove MIME part genereated by Avaya CS1000 before routing to BT Wholesale. To add a new Adaptation, navigate to **Routing > Adaptations**. Click on **New** button in the right pane (not shown). Enter an appropriate **Adaptation Name** to identify the Adaptation. Select **DigitConversionAdapter** from the **Module Name** drop-down menu. Select **Name-Value Parameter** from the **Module Parameter Type** drop-down menu. Click on **Add** button two times to add **Name** as **MIME** and **Value** as **no,** and **Name** as **Fromto** and **Value** as **true**. Scroll down to **Digit Conversion for Outgoing Calls from SM** to add records for outgoing numbers to Avaya SBCE. Click on **Commit** button after changes are completed.



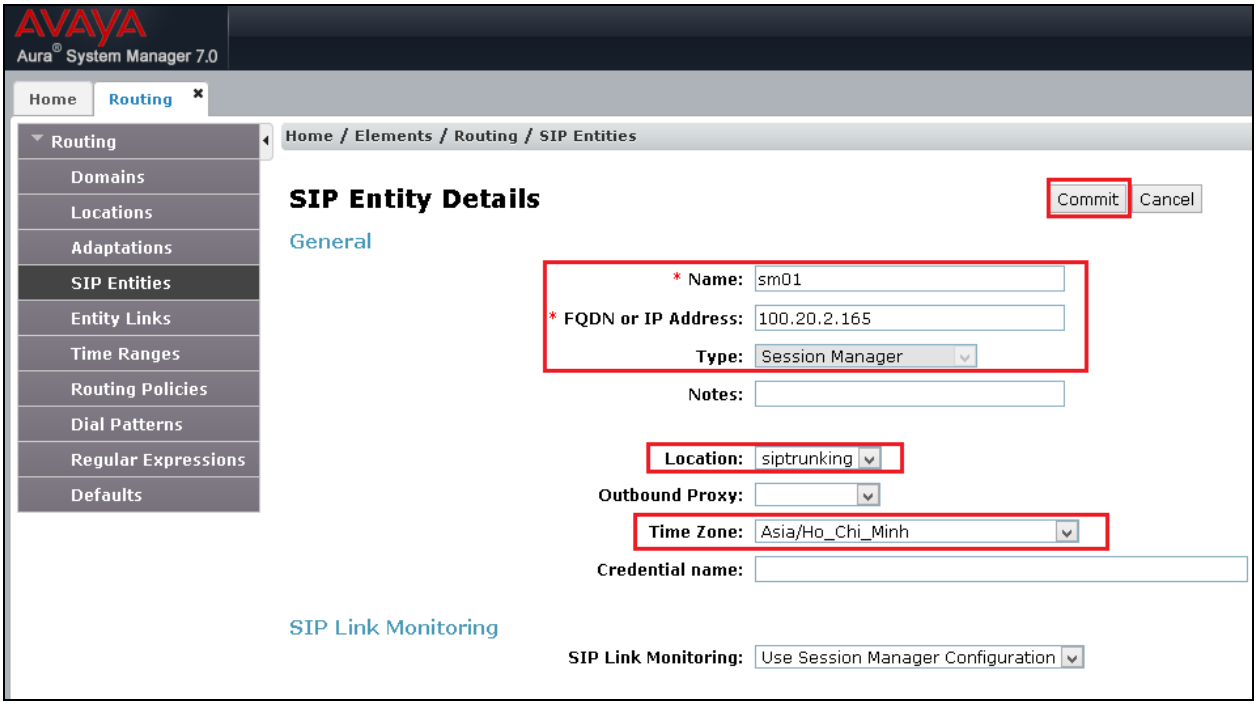
6.4 Configure SIP Entities

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

6.4.1 Configure Session Manager SIP Entity

Follow the steps shown below:

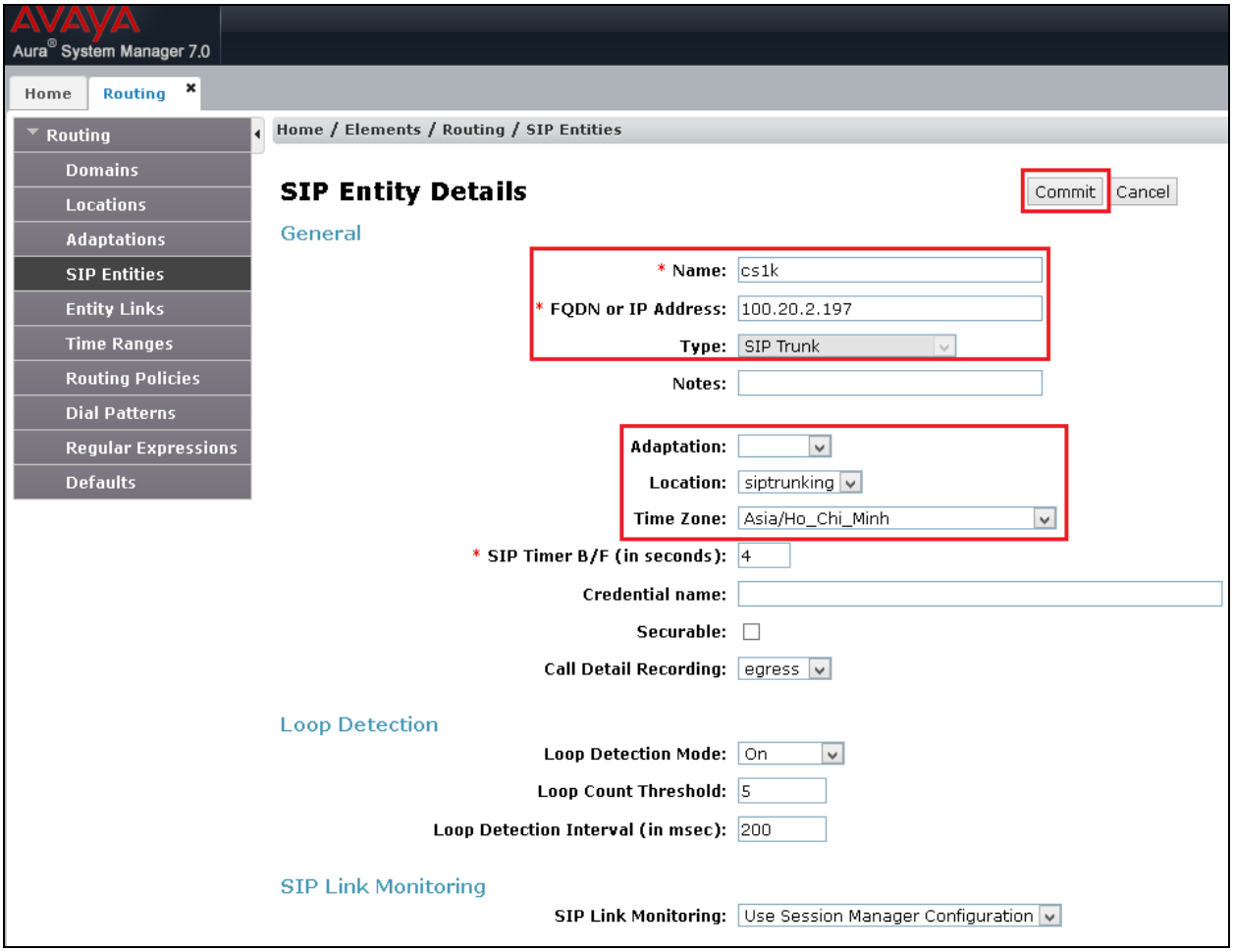
1. In the left pane under **Routing**, click on **SIP Entities**. In the **SIP Entities** page, click on **New** (not shown).
2. In the **General** section of the **SIP Entity Details** page, provision the following:
   - **Name –** Enter a descriptive name (e.g., **sm01**).
   - **FQDN or IP Address –** Enter the IP address of Session Manager signaling interface, (*not* the management interface), provisioned during installation (e.g., **100.20.2.165**).
   - **Type –** Verify **Session Manager** is selected.
   - **Location** – Select location **siptrunking**.
   - **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 Link 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. Click on **Commit**.



6.4.2 Configure Avaya CS1000 SIP Entity

Follow the steps shown below:

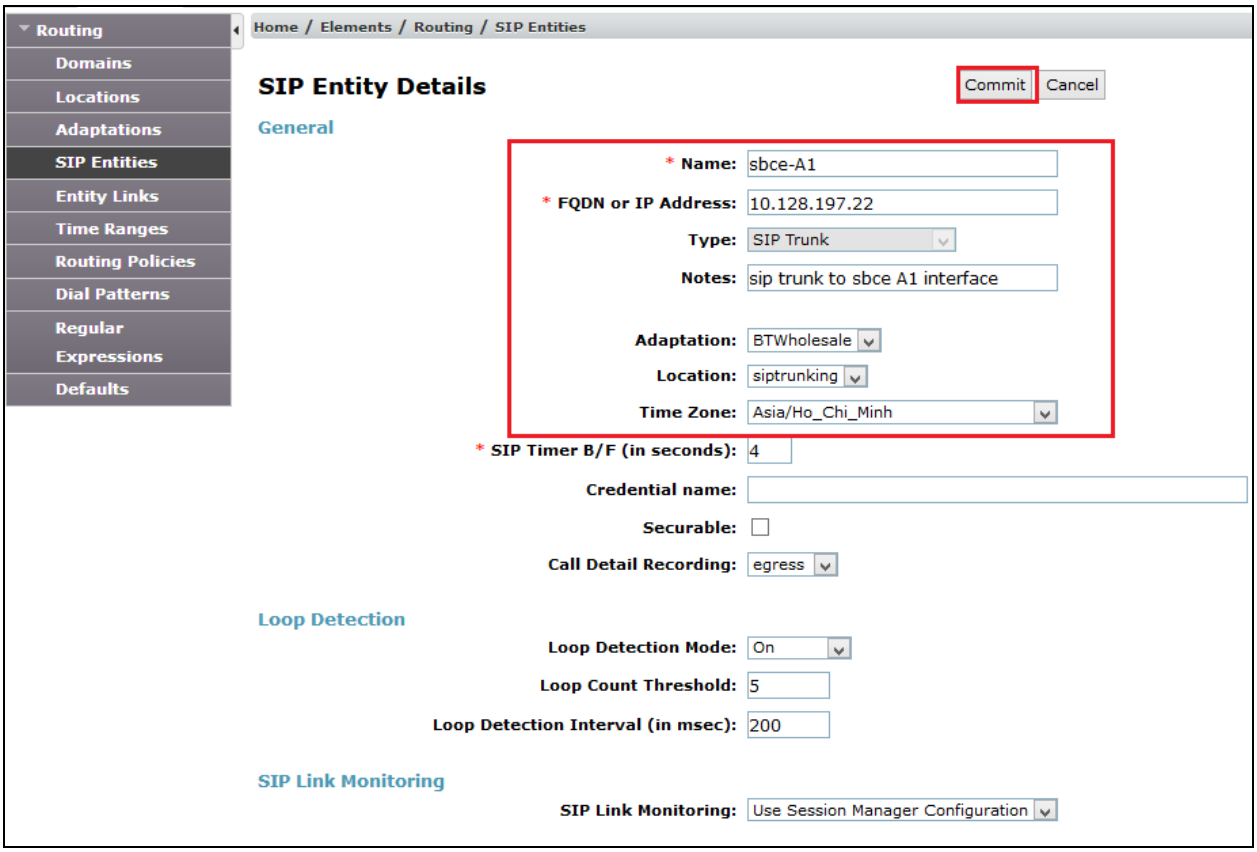
1. In the **SIP Entities** page, click on **New** (not shown).
2. In the **General** section of the **SIP Entity Details** page, provision the following:
   - **Name –** Enter a descriptive name (e.g., **cs1k**).
   - **FQDN or IP Address –** Enter the IP address of CS1000 Node IP as in **Section 5.2.1** (e.g., **100.20.2.197**).
   - **Type –** Select **SIP Trunk**.
   - **Location** – Select location **siptrunking** administered in **Section 6.2**.
   - **Time Zone** – Select the time zone in which CS1000 resides.
3. 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.
4. 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-A1**).
- **FQDN or IP Address –** Enter the IP address of the A1 (private) interface of the Avaya SBCE (e.g., **10.128.197.22**).
- **Adaptation** – Select **BTWholesale** 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 Avaya CS1000 and another one for Avaya SBCE. To add an Entity Link, navigate to **Routing → Entity Links** in the left navigation pane and click on **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, **TLS** for the Entity Link to Avaya CS1000 and 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 Avaya CS1000, select the Avaya

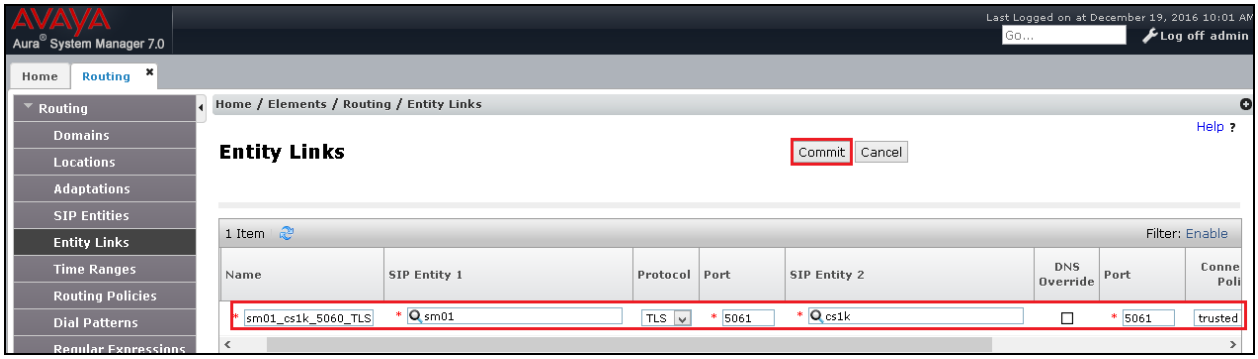
CS1000 SIP Entity defined in **Section 6.4.2**. For Avaya SBCE, select the Avaya SBCE SIP Entity defined in **Section 6.4.3**.

- **Port:** Port number on which the other system receives SIP requests from Session Manager.
- **Connection Policy:** Select **Trusted**.
- Click **Commit** to save.

6.5.1 Configure Entity Link to Avaya CS1000

Follow the steps shown below:

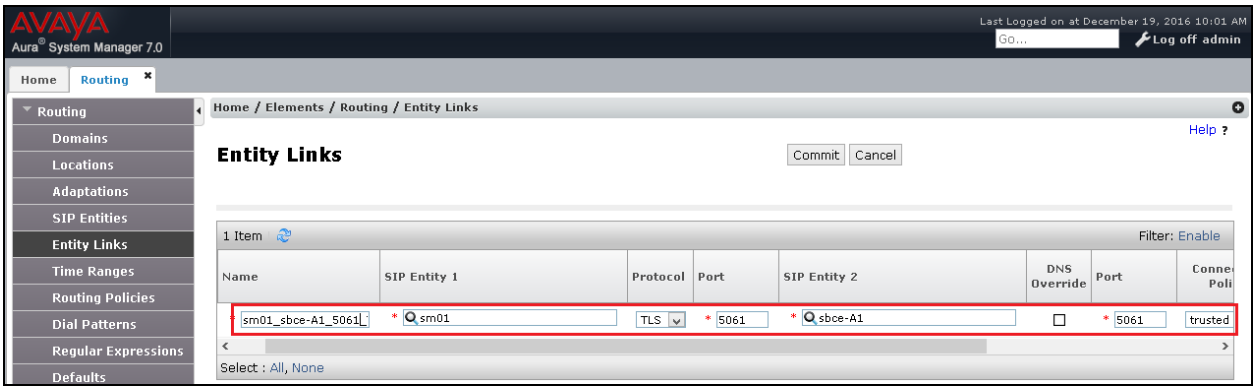
1. In the left pane under **Routing**, click on **Entity Links**, then click on **New** button (not shown).
2. Continuing in the **Entity Links** page, provision the following:
   - **Name** – Enter a descriptive name (or have it created automatically) for this link to CS1000 (e.g., **sm01_cs1k_5061_TLS**).
   - **SIP Entity 1** – Select the SIP Entity administered in **Section 6.4.1** for Session Manager (e.g., **sm01**).
   - **SIP Entity 1 Port** – Enter **5061**.
   - **Protocol –** Select **TLS.**
   - **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 **5061.**
   - **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., **sm01_sbce-A1_5061_TLS**).
- **SIP Entity 2** – Select the SIP Entity administered in **Section 6.4.3** for the Avaya SBCE entity (e.g., **sbce-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 Avaya CS1000 and another one for Avaya SBCE. To add a routing policy, navigate to **Routing → Routing Policies** in the left navigation pane and click on **New** button in the right pane (not shown).

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

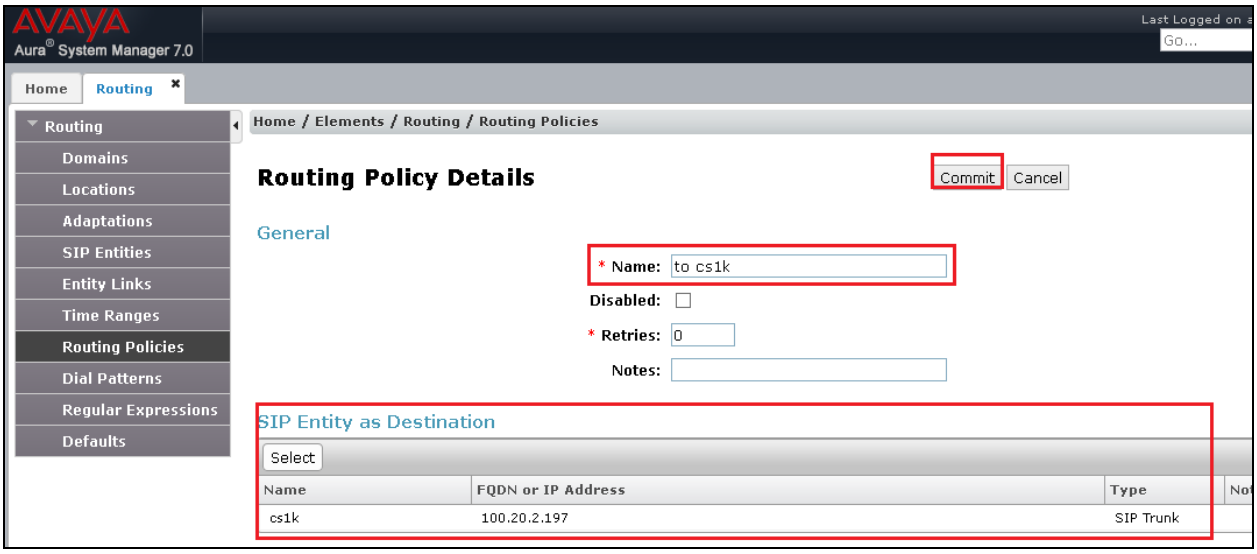
- **Name:** Enter a descriptive name.
- **Notes:** Add a brief description (optional).

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

6.6.1 Configure Routing Policy for Avaya CS1000

This Routing Policy was used for inbound calls from BT Wholesale.

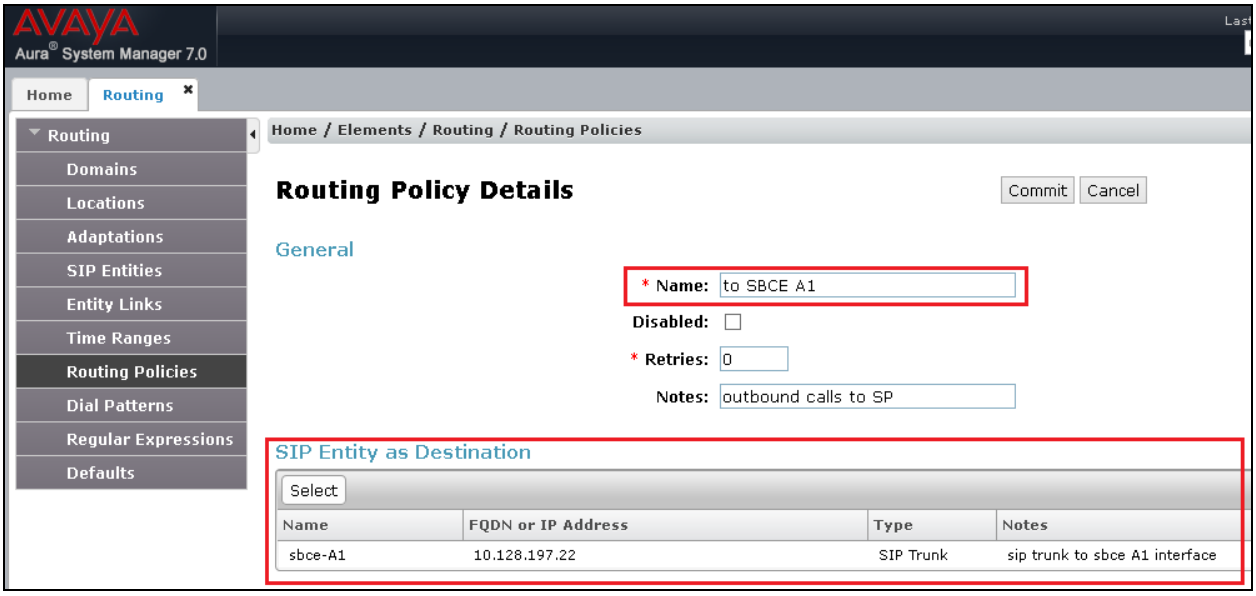
1. In the left pane under **Routing**, click on **Routing Policies**. In the **Routing Policies** page click on **New** button (not shown).
2. In the **General** section of the **Routing Policy Details** page, enter a descriptive **Name** for routing calls from BT Wholesale to Avaya CS1000 (e.g., **to 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 6.4.2** 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., **to SBCE A1**).
- **SIP Entity List** –Select the SIP Entity administered in **Section 6.4.3** for the Avaya SBCE entity (e.g., **sbce-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 Avaya CS1000 to BT Wholesale 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 on **New** button in the right pane (not shown).

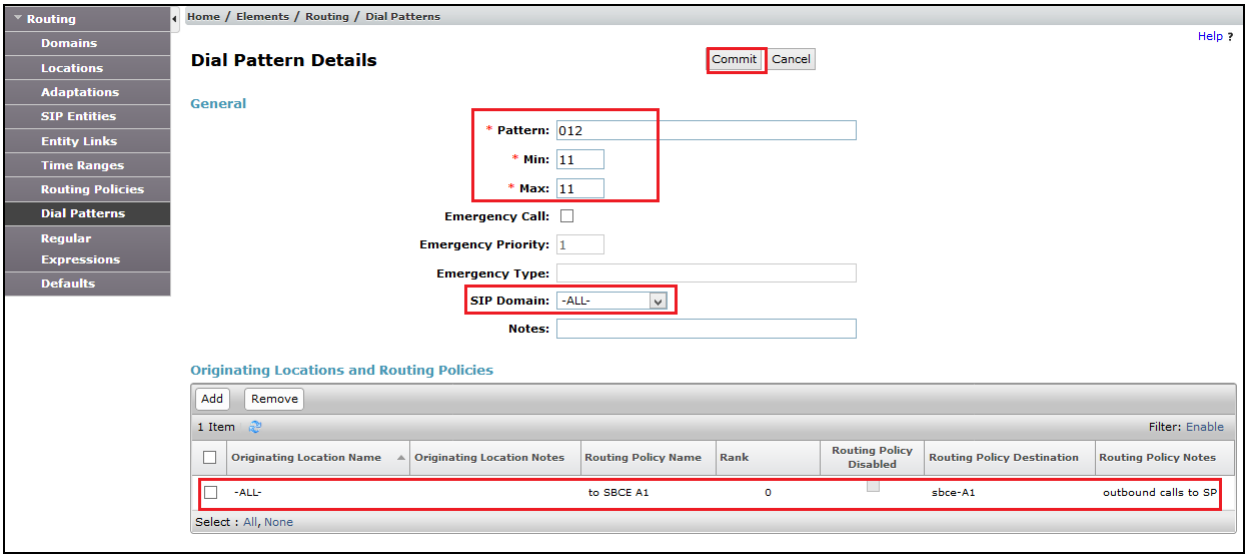
In the **General** section, enter the following values:

- **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).

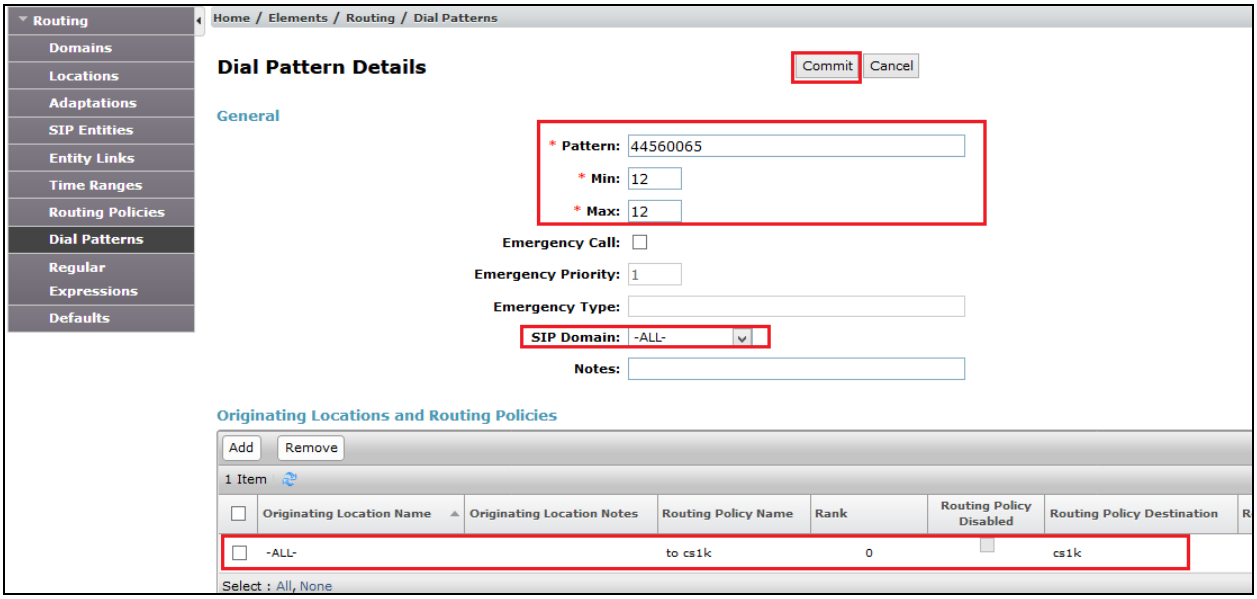
In the **Originating Locations and Routing Policies** section, click on **Add**. From the **Originating Locations and Routing Policy List** that appears (not shown), select the appropriate originating location for use in the match criteria. Lastly, select the routing policy from the list that will be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

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

The first example shows that 11-digit dialed numbers that begin with **012** and have a destination domain of "**ALL**" uses route policy to Avaya SBCE as defined in **Section 6.6.2.** Do the same for 11-digit dialed numbers that begin with **029** and **056**.



The second example shows that 12-digit pattern that starts with 44560065 is used for inbound calls from BT Wholesale to DID numbers on Avaya CS1000.



7. Configure Avaya Session Border Controller for Enterprise

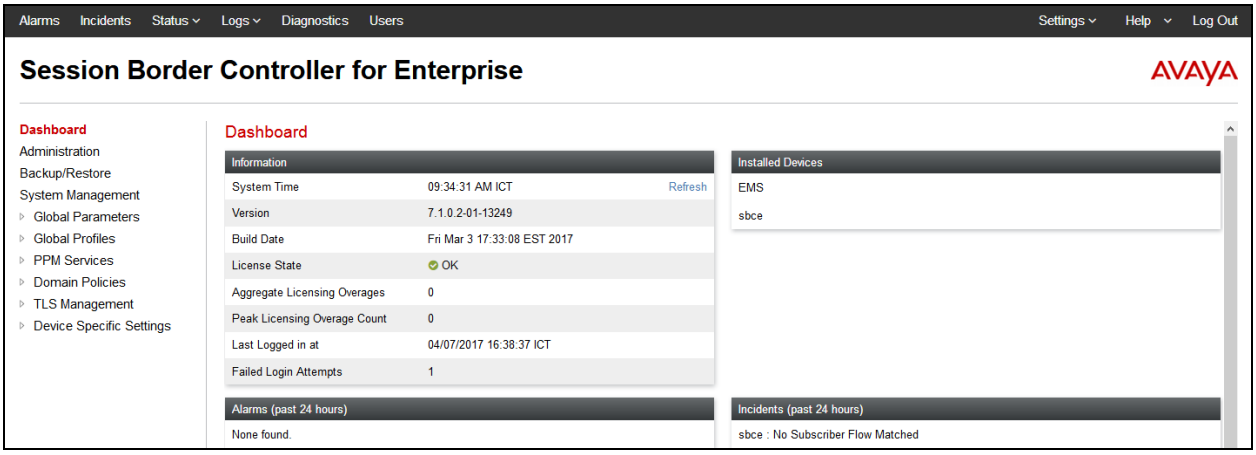
Note: The installation and initial provisioning of the Avaya SBCE is beyond the scope of this document.

As described in **Section 3**, the reference configuration places the private interface (A1) of the Avaya SBCE in the enterprise site (10.128.197.21). The connection to BT Wholesale uses the Avaya SBCE public interface B1 (192.168.5.48). 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**.

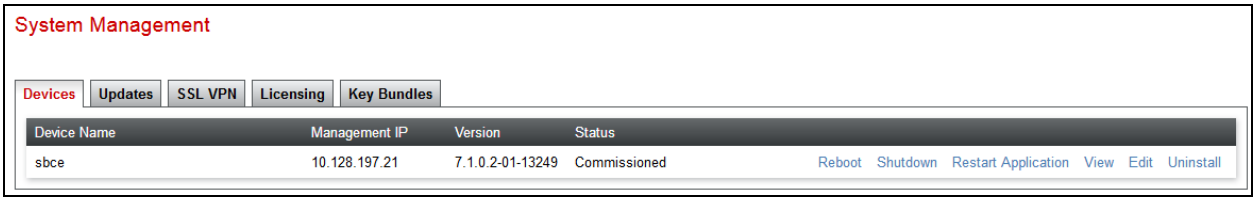
3. Enter the password and click on **Log In**.

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.

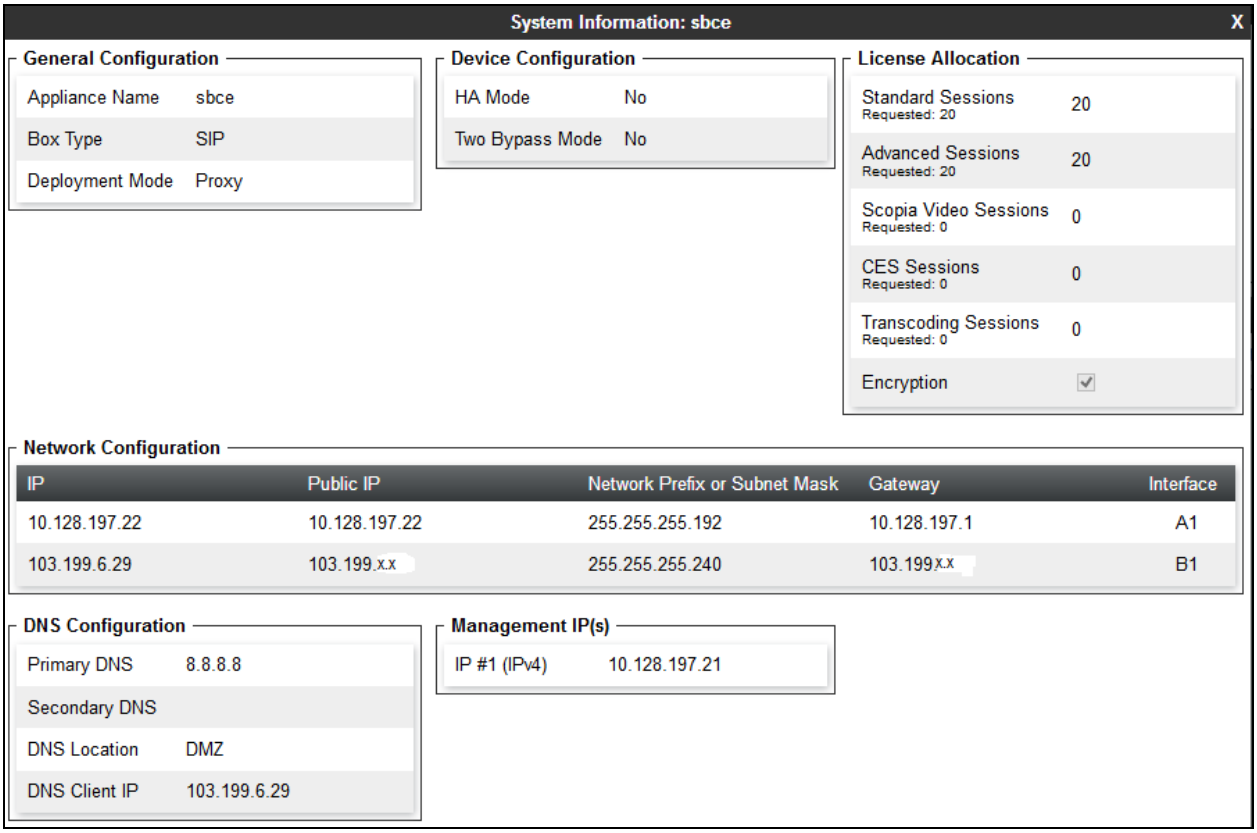


7.1 System Management – Status

1. Select **System Management** and verify that the **Status** column says **Commissioned**.



2. Click on **View** (shown above) to display the **System Information** screen.



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

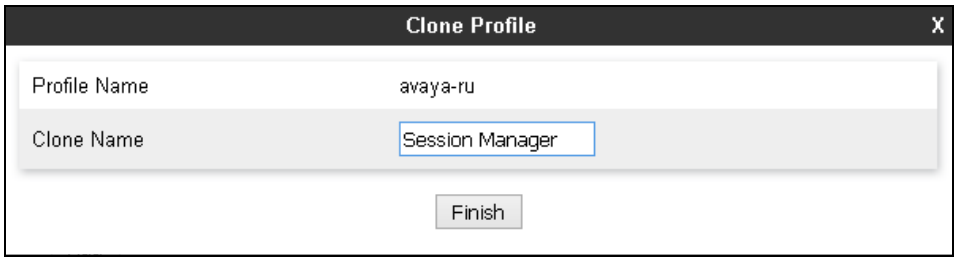
URI Group feature allows a user to create any number of logical URI Groups that are comprised of individual SIP subscribers located in that particular domain or group. These groups are used by the various domain policies to determine which actions (Allow, Block, or Apply Policy) should be used for a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

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

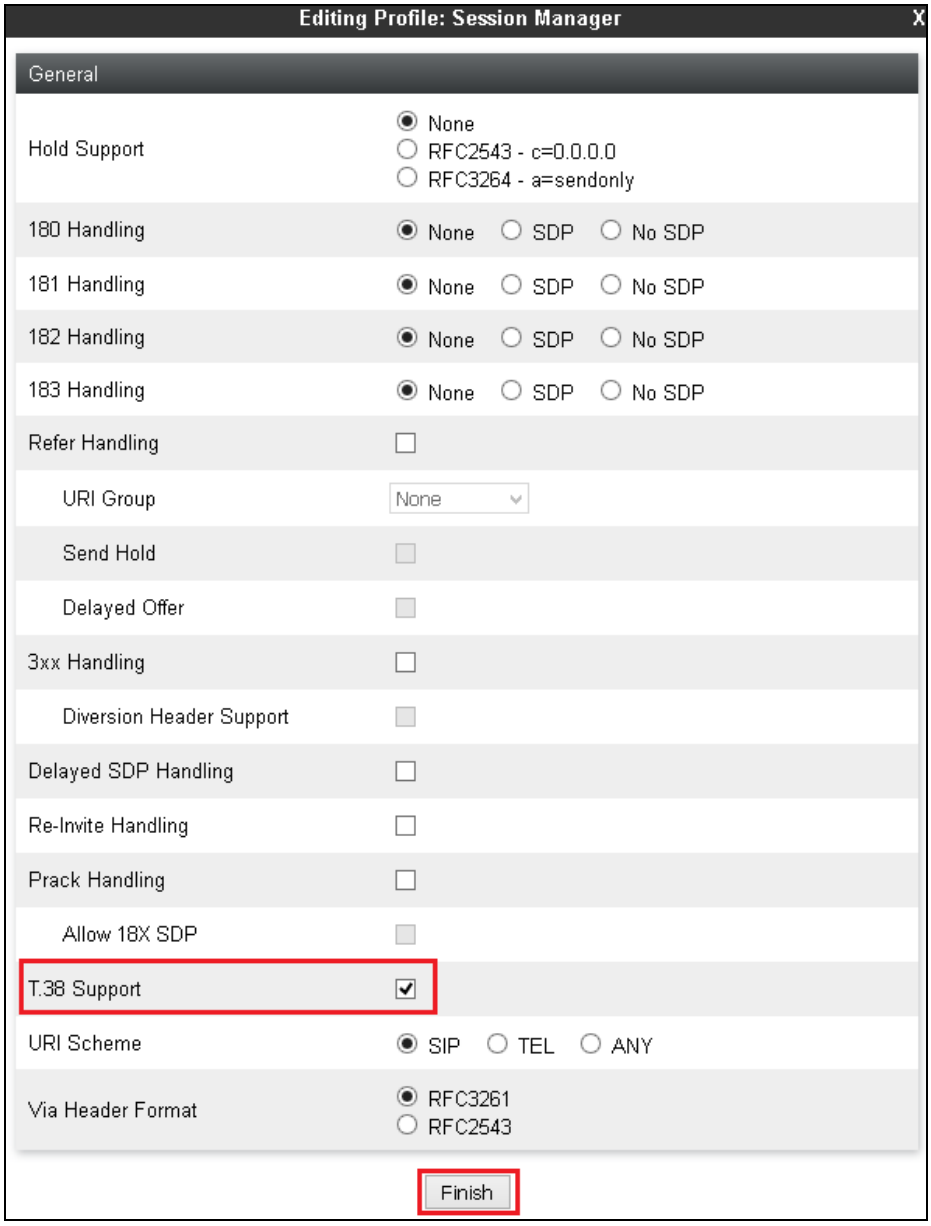
7.2.2 Server Interworking – Session Manager

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. Navigate to **Global Profiles > Server Interworking** from the left-hand menu.
2. Select **avaya-ru** then click on **Clone** button.
3. Enter profile name: (e.g., **Session Manager**), and click on **Finish**.



4. Click on **Edit** in **General** tab (not shown).
   - Check **T38 Support** box.
   - Click on **Finish**.

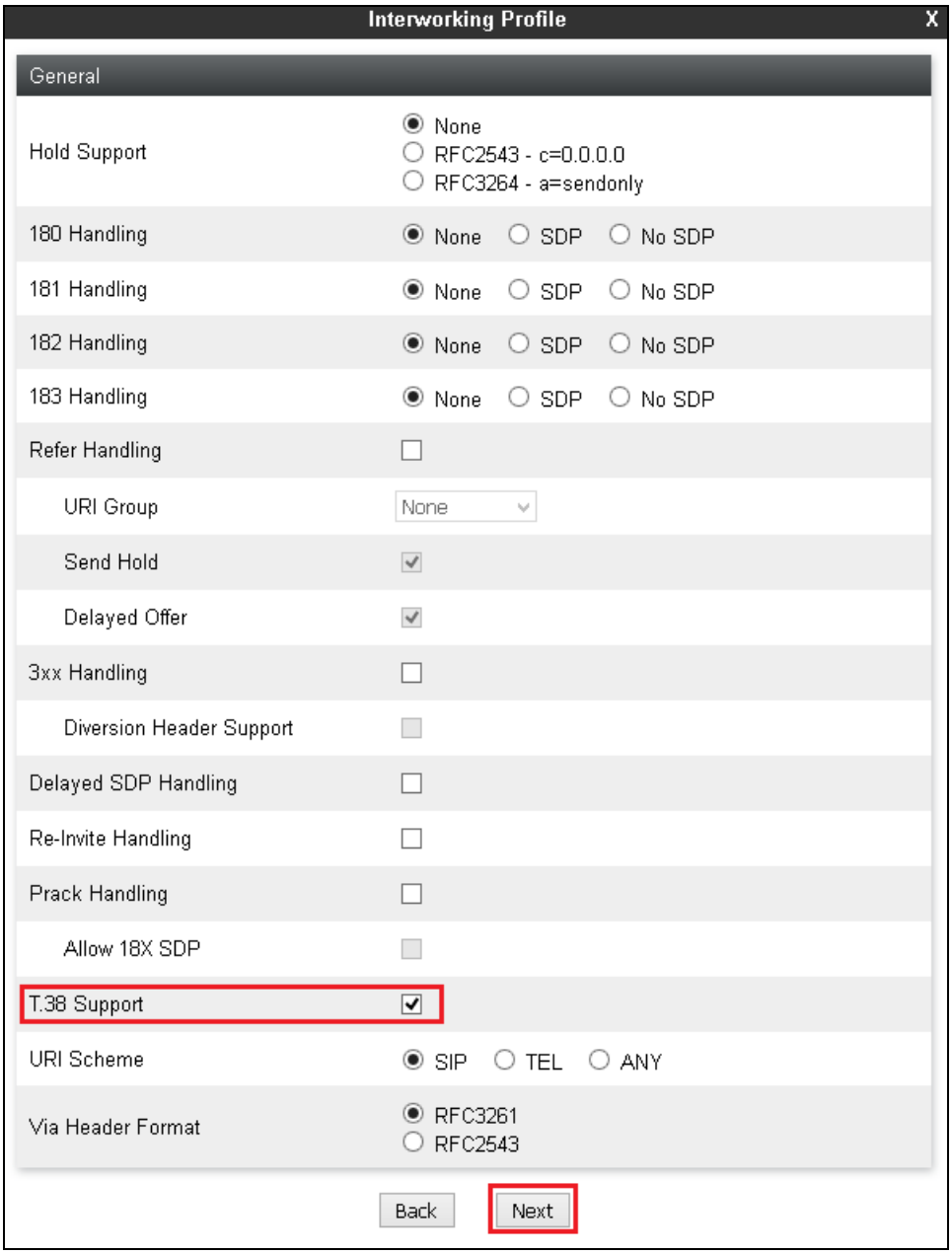


5. Click on **Edit** in the **Advanced** tab (not shown).
   - **Record Routes**: Choose **None**.
   - Click on **Finish**.

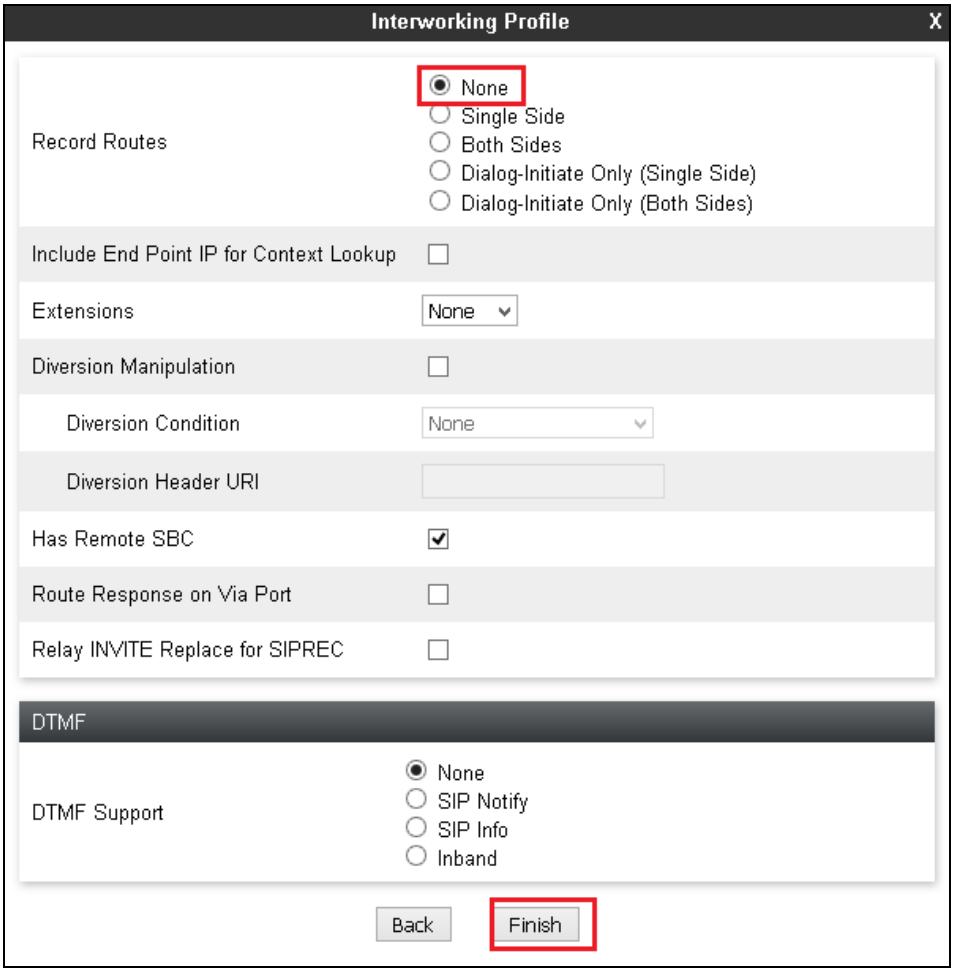
7.2.3 Server Interworking – BT Wholesale

Navigate to **Global Profiles** > **Server Interworking** from the left-hand menu to add an Interworking Profile for the connection to BT Wholesale network.

1. Click on **Add** (not shown) then enter **BT** as the **profile name** and click on **Next** (not shown).
2. In **General** window: Check **T.38 Support** then click on **Next**.



3. Leave default values in **SIP Timers** window and **Privacy** window (not shown).
4. In **Advance** window: Select **None** for **Record Routes** then click on **Finish**.



7.2.4 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 calls from the Avaya CS1000, BT Wholesale requires the P-Asserted-Identity (PAI) header should contain either trunk Pilot number or any number in the assigned DID numbers. In this solution test, trunk Pilot number was used.

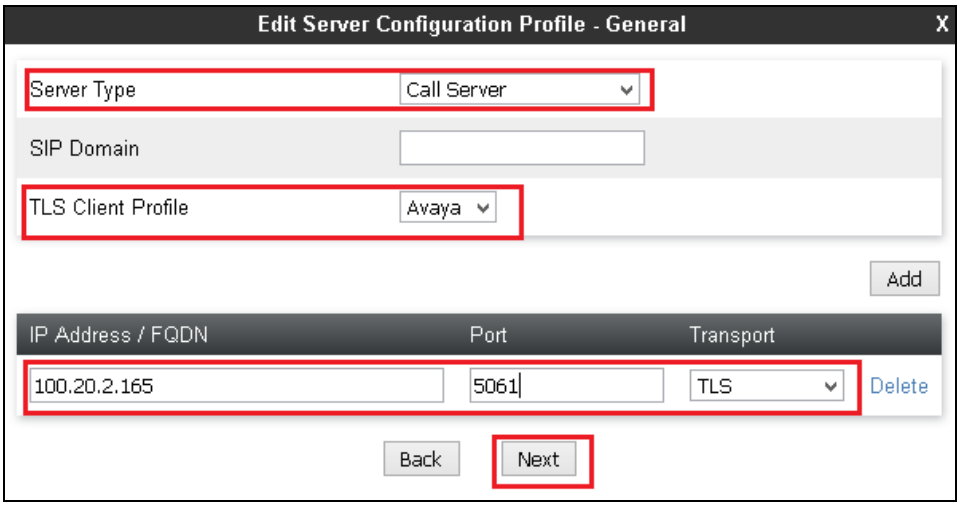
To define the signaling manipulation, navigate to **Global Profiles > Signaling Manipulation** in the main menu on the left hand side (not shown). Click on **Add** and enter **BT** for the **Title** in the script editor (not shown). The script text is displayed below. Note that the real trunk Pilot number was masked for security reason.

```
within session "INVITE"
{
act on request where %DIRECTION="OUTBOUND" and %ENTRY_POINT="POST_ROUTING"
{
%HEADERS["P-Asserted-Identity"][1].URI.USER = "445600653xxx";
}
}
```

7.2.5 Server Configuration – Session Manager

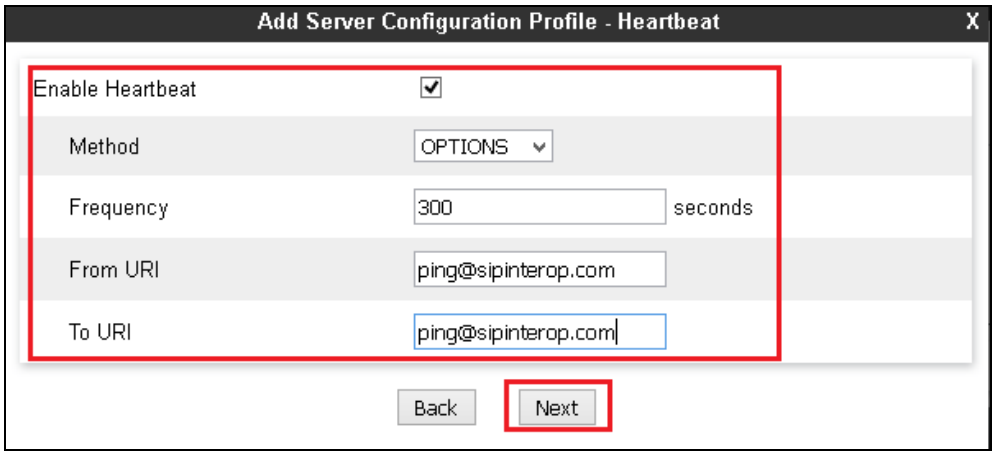
This section defines the Server Configuration for the Avaya SBCE connection to Session Manager.

1. Navigate to **Global Profiles** > **Server Configuration** from the left-hand menu.
2. Select **Add** and the **Profile Name** window will open. Enter a Profile Name (e.g., **Session Manager**) and click on **Next** (not shown).
3. The **Edit Server Configuration Profile - General** window will open.
   - Select **Server Type**: **Call Server**.
   - **IP Address / FQDN**: **100.20.2.165** (Session Manager signaling IP Address as configured in **Section 6.4.1**).
   - **Transport**: Select **TLS**.
   - **Port**: **5061**.
   - **TLS Client Profile**: Select **Avaya**.
   - Click on **Next**.

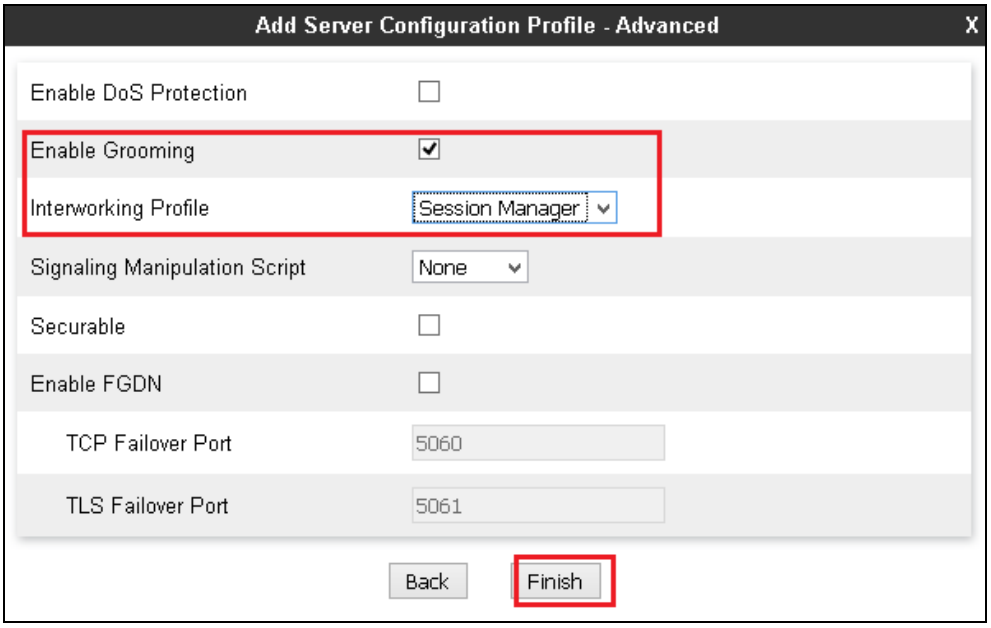


4. The **Add Server Configuration Profile - Authentication** window will open (not shown).
   - Click on **Next** to accept default values.

5. The **Add Server Configuration Profile - Heartbeat** window will open.
   - Check **Enable Heartbeat** box.
   - **Method**: Select **OPTIONS**.
   - **Frequency**: Enter **300** (or desired number of seconds in the range of 30 - 7200).
   - **From URI** and **To URI**: Enter **ping@sipinterop.com**
   - Click on **Next** button.



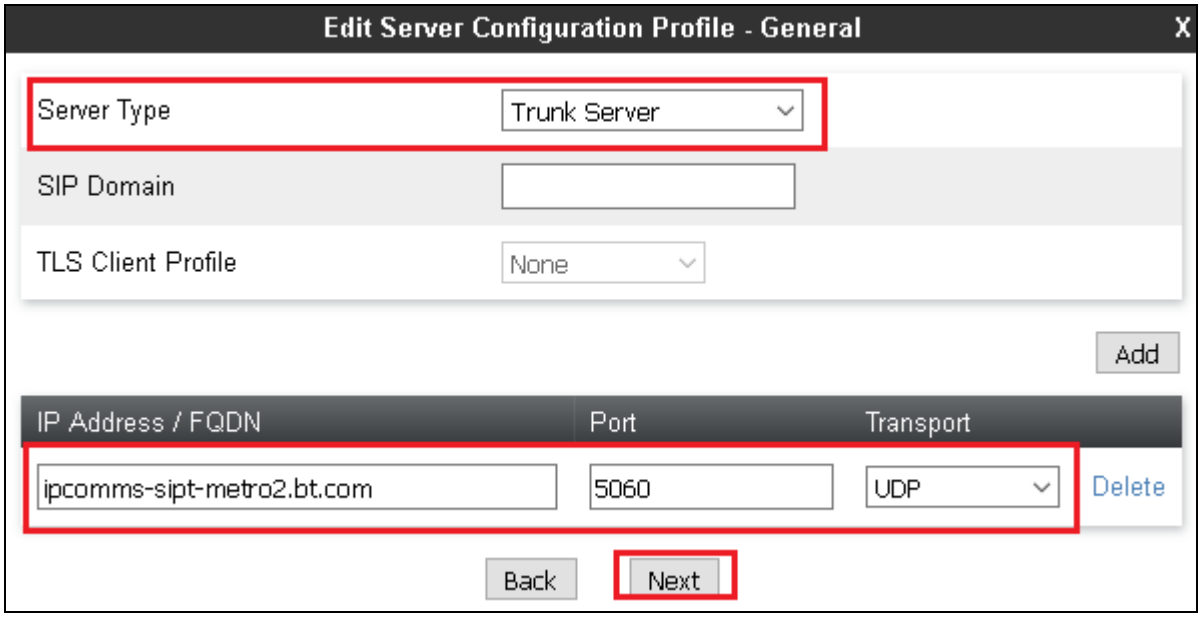
6. The **Add Server Configuration Profile - Advanced** window will open.
   - Check **Enable Grooming** box.
   - For **Interworking Profile**, select the profile created for Session Manager in **Section 7.2.2**.
   - Click on **Finish**.



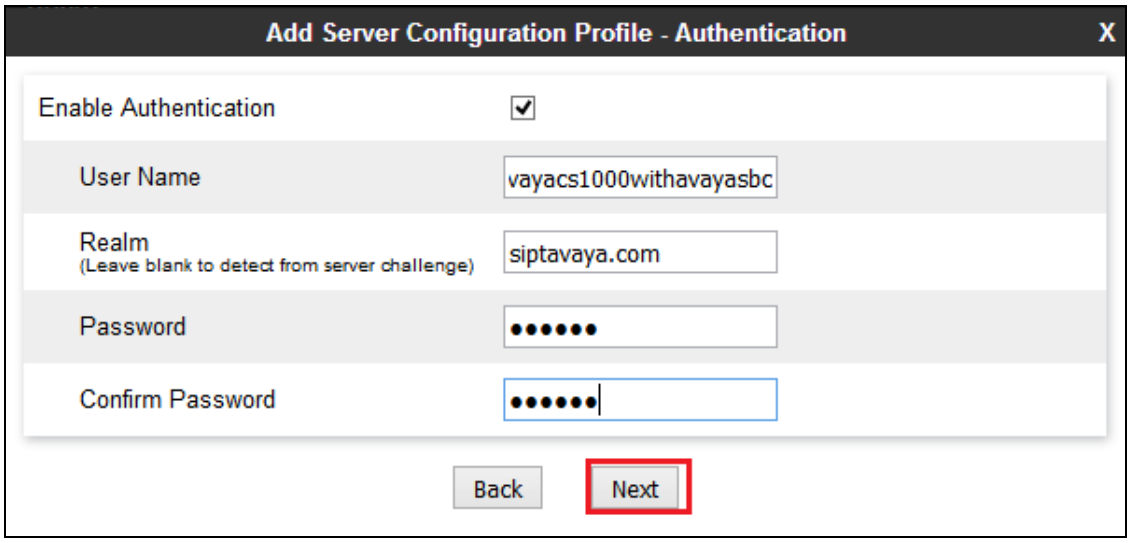
7.2.6 Server Configuration – BT Wholesale

Repeat the steps in **Section 7.2.5**, with the following changes, to create a Server Configuration for the Avaya SBCE connection to BT Wholesale.

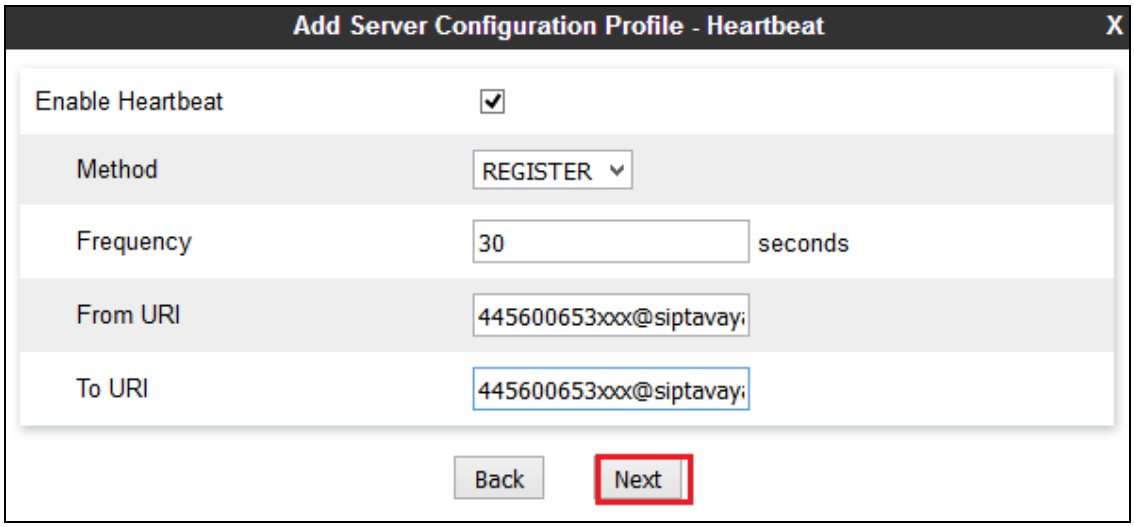
1. Select **Add Profile** and enter a Profile Name (e.g., **BT**) and click on **Next** (not shown).
2. On the **Edit Server Configuration Profile - General** window, enter the following.
   - Select **Server Type: Trunk Server**.
   - **IP Address / FQDN:** add one FQDN of BT Wholesale SBC server (e.g., **ipcomms-sipt-metro2.bt.com)**.
   - **Transport**: Select **UDP**.
   - **Port: 5060**.
   - Click on **Next**.



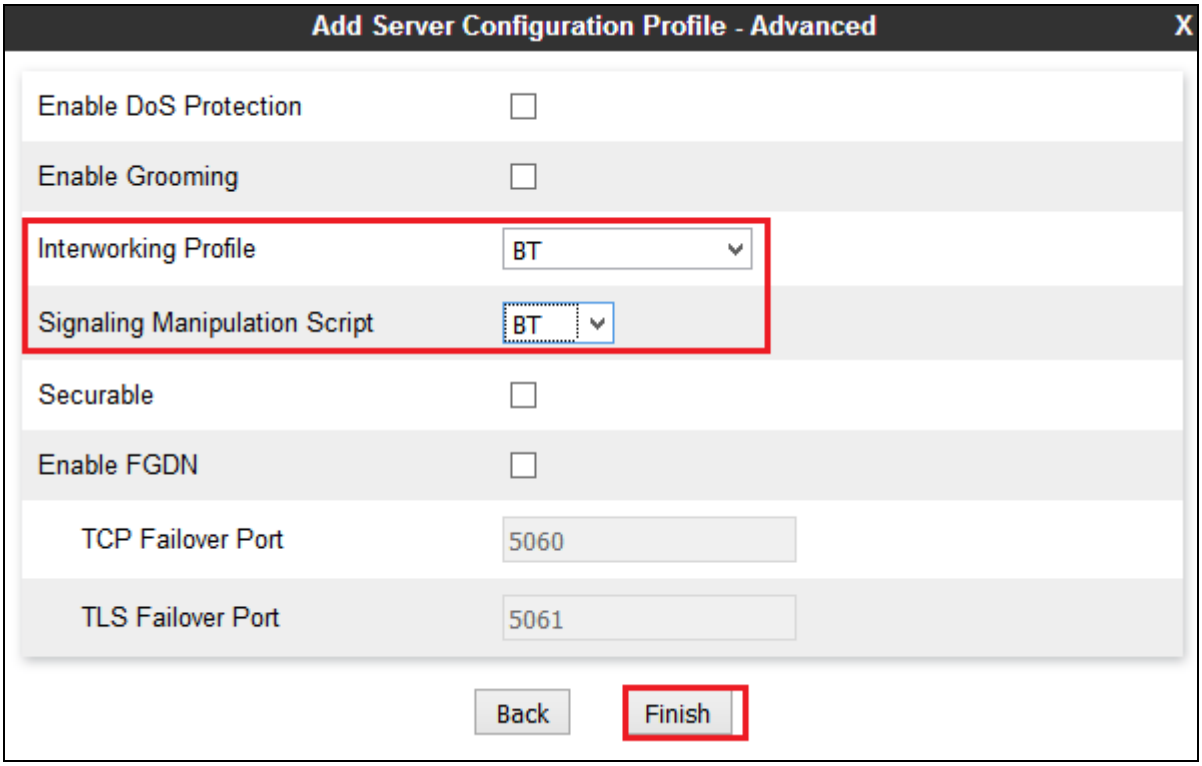
3. Under **Add Server Configuration Profile – Authentication**:
   - Select **Enable Authentication**.
   - **User Name**: Enter authentication name provided by BT Wholesale.
   - **Realm**: Enter domain name provided by BT Wholesale.
   - **Password** and **Confirm Password**: Enter authentication password provided by BT Wholesale.



4. Under **Add Server Configuration Profile - Heartbeat**:
   - Select **Enable Heartbeat**.
   - **Method**: Select **REGISTER**.
   - **Frequency**: Enter **30** (or desired number of seconds in the range of 30-7200).
   - **From URI** and **To URI**: Enter trunk Pilot number 445600653xxx@siptavaya.com.
   - Click on **Next** button.



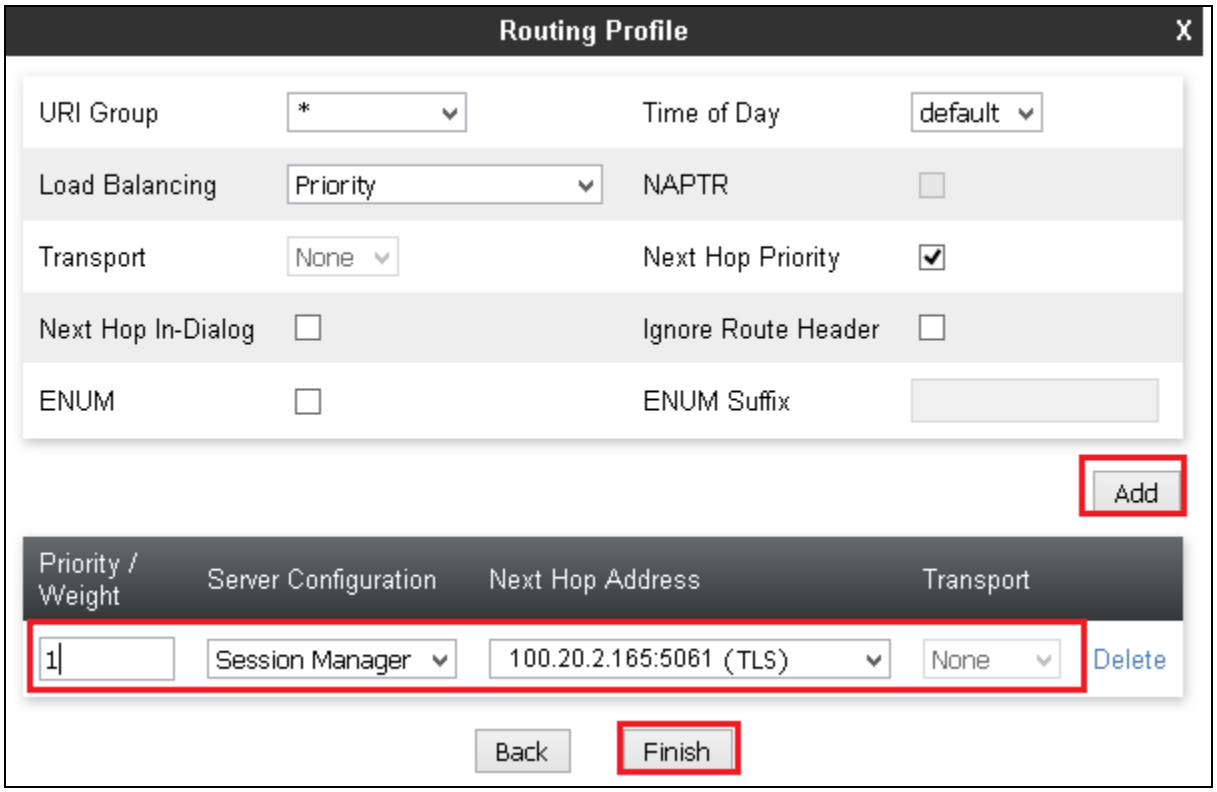
5. Under **Add Server Configuration Profile - Advanced** window:
    - Select **BT** for **Interworking Profile**.
    - Select **BT** for **Signaling Manipulation Script** as configured in **Section 7.2.4**.



7.2.7 Routing – To Session Manager

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

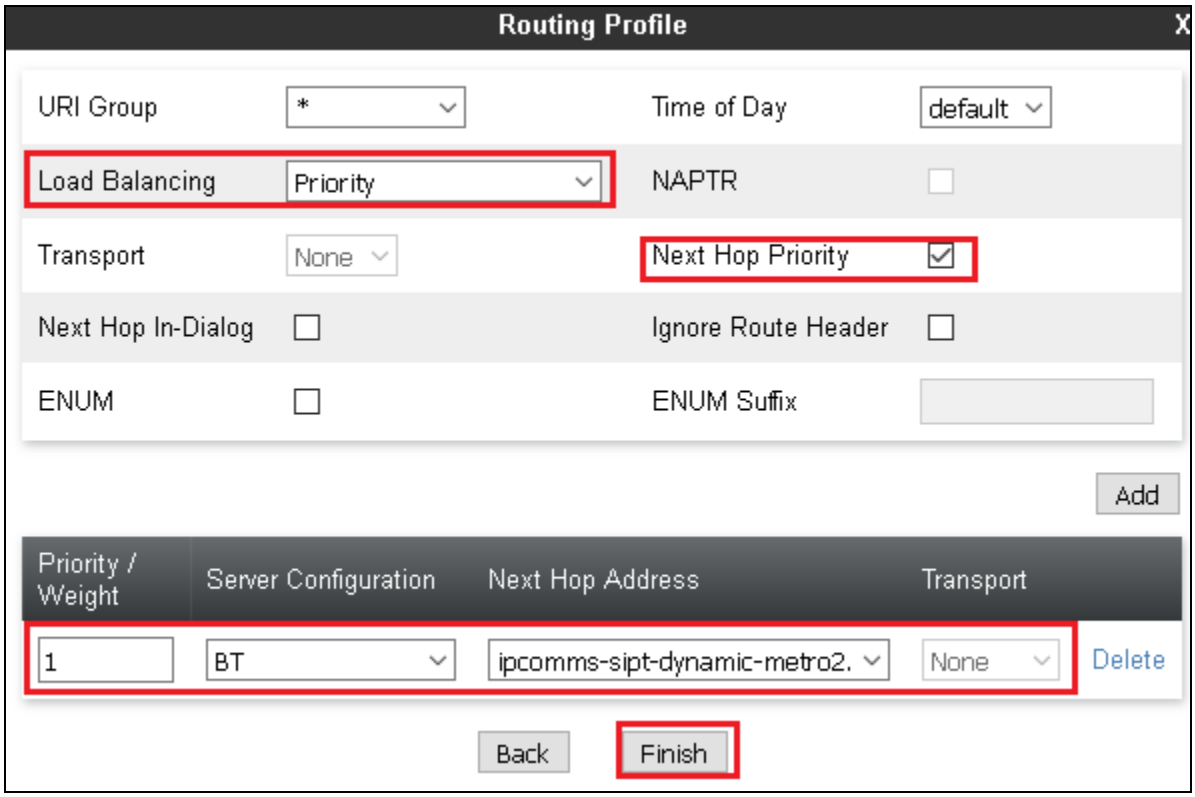
1. Navigate to **Global Profiles** > **Routing** from the left-hand menu, and click on **Add** (not shown).
2. Enter a **Profile Name**: (e.g., **Session Manager)** and click **Next** (not shown).
3. The **Routing Profile** window will open. Using the default values shown, click on **Add**.
4. Populate the following fields:
   - **Priority/Weight** = **1**.
   - **Server Configuration** = **Session Manager**.
   - **Next Hop Address:** Verify that the **100.20.2.165:5061 (TLS)** entry from the drop down menu is selected (Session Manager IP address). Also note that the **Transport** field is grayed out.
5. Click on **Finish**.



7.2.8 Routing – To BT

Repeat the steps in **Section 7.2.7**, with the following changes, to add a Routing Profile for the Avaya SBCE connection to BT Wholesale.

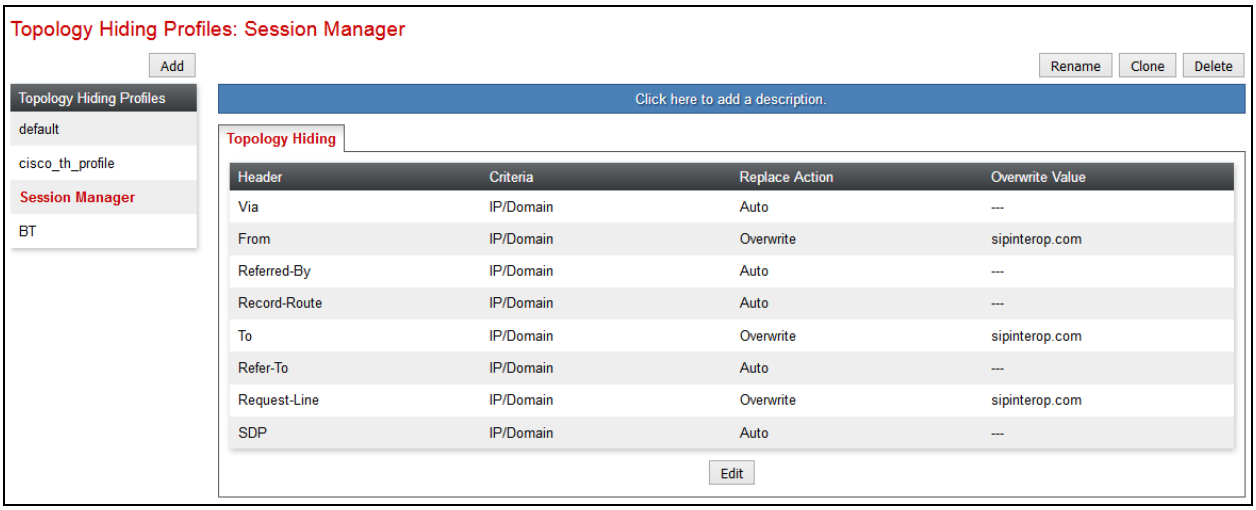
1. On the **Global Profiles → Routing** window (not shown), enter a **Profile Name**: (e.g., **BT**).
2. **Load Balancing**: Select **Priority**.
3. Check to **Next Hop Priority**.
4. On the **Routing Profile** window, populate the following fields:
   - **Priority / Weight**: Enter 1.
   - **Server Configuration:** Select **BT**.
   - Click on **Finish**.



7.2.9 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. Navigate to **Global Profiles** > **Topology Hiding** from the left-hand side menu.
2. Click on **Add** button, enter **Profile Name**: (e.g., **Session Manager**), and click **Next** (not shown).
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 on **Finish** (not shown). Note that the **Overwrite Value** is **sipinterop.com**.

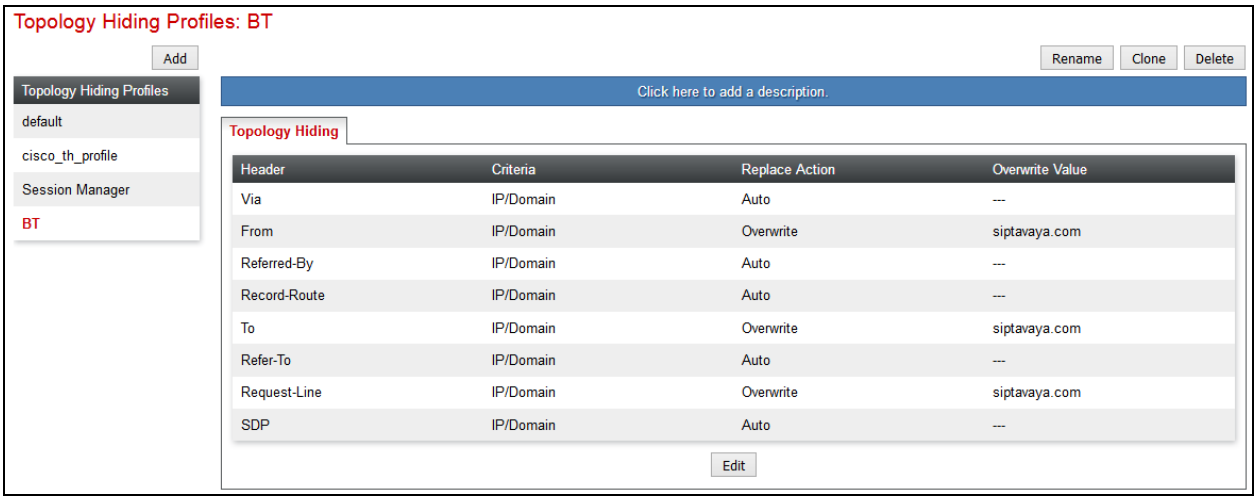


Header	Criteria	Replace Action	Overwrite Value
Via	IP/Domain	Auto	---
From	IP/Domain	Overwrite	sipinterop.com
Referred-By	IP/Domain	Auto	---
Record-Route	IP/Domain	Auto	---
To	IP/Domain	Overwrite	sipinterop.com
Refer-To	IP/Domain	Auto	---
Request-Line	IP/Domain	Overwrite	sipinterop.com
SDP	IP/Domain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

7.2.10 Topology Hiding – BT

Repeat the steps in **Section 7.2.9,** with the following changes, to create a Topology Hiding Profile for the Avaya SBCE connection to BT Wholesale.

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



7.3 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.

7.3.1 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 default rule was used.

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

7.3.2 Border Rules

The Border rules specifies if NAT is utilized (on by default), as well as detecting SIP and SDP published IP addresses. In the solution as tested, the **default** rule was utilized. No customization was required.

7.3.3 Media Rules

The Media rules will be applied to both directions. In the solution as tested, the **default-low-med** rule was utilized. No customization was required.

7.3.4 Security Rules

The Security rule will be applied to both directions. In the solution as tested, the **default-low** rule was utilized. No customization was required.

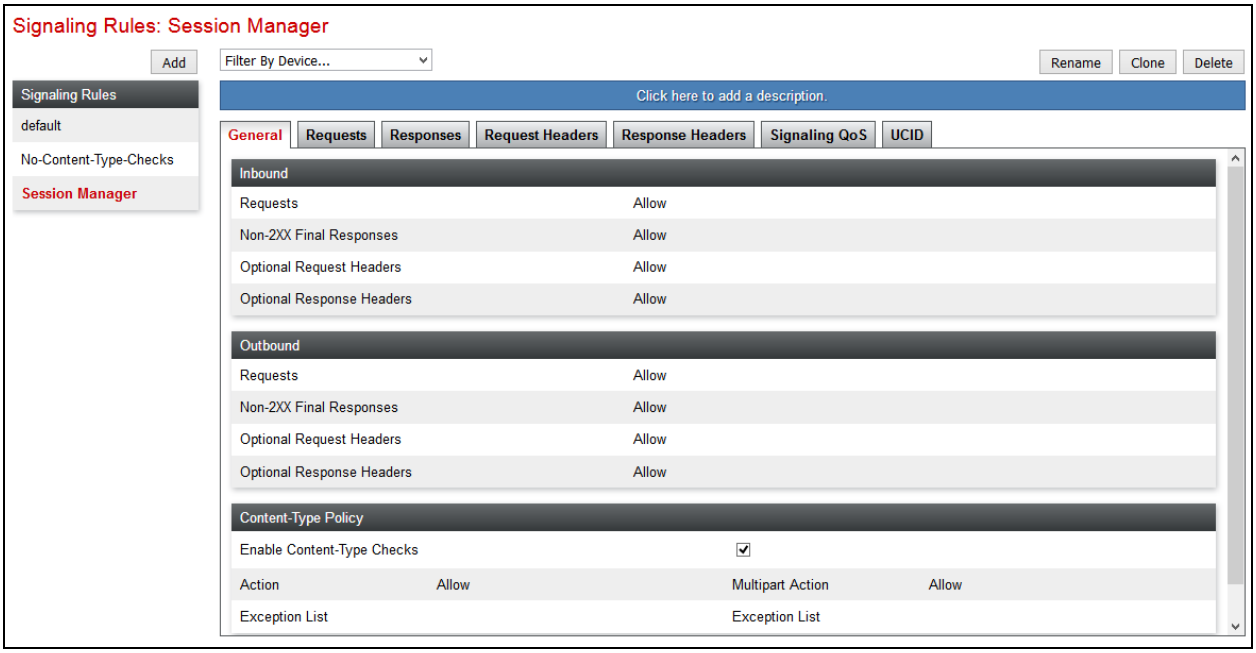
7.3.5 Signaling Rules

Signaling rules are a mechanism on the Avaya SBCE to manipulate the signaling 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 flow to BT Wholesale, 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 signaling rule, navigate to **Domain Policies > Signaling Rules** in the main menu on the left hand side.

1. Click on **Add** and enter details in the **Signaling Rule** pop-up box. In the **Rule Name** field enter a descriptive name such as **Session Manager** for the signaling rule to remove Avaya proprietary and unnecessary headers.
2. Click on **Next** and **Next** again, then **Finish** (not shown).

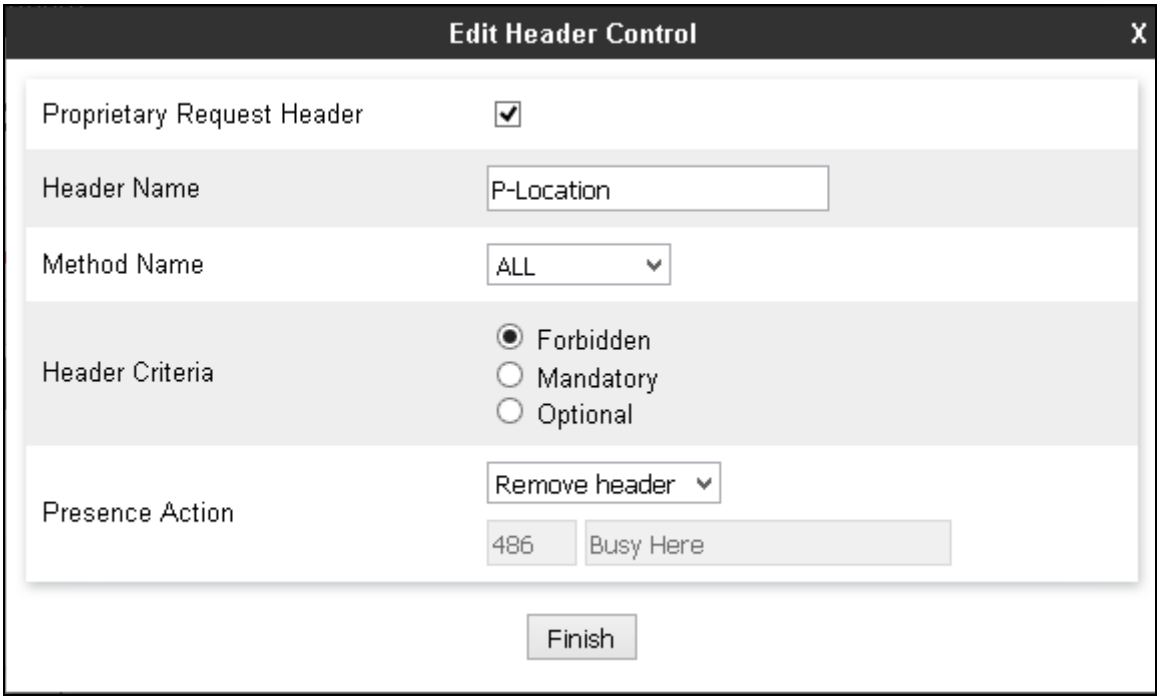


Select the **Request Headers** tab (not shown) and define the rules to remove Avaya proprietary headers and unnecessary headers as follows:

- Click on **Add In Header Control** (not shown).

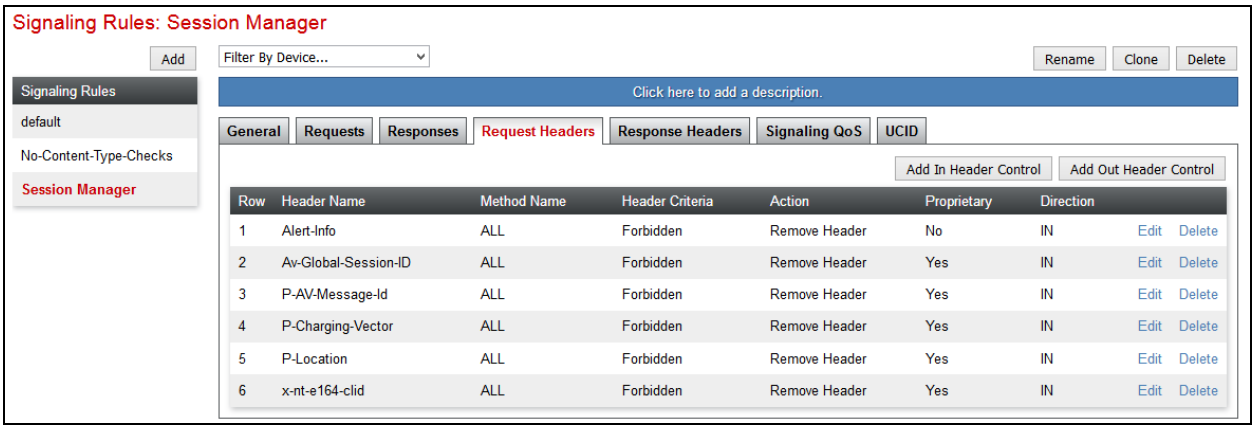
- Check the **Proprietary Request Header** box to remove Avaya proprietary headers or uncheck it to remove unnecessary headers.
- Enter the name of the header to be removed in the **Header Name** field.
- Select **ALL** in the **Method Name** field.
- Check **Forbidden** in the **Header Criteria** options.
- In the **Presence Action** drop down menu, select **Remove Header**.
- Click on **Finish**.

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



Note: During the test, the same was done for **Alert-Info**, **Av-Global-Session-ID**, **P-AV-Message-Id**, **P-Charging-Vector**, **x-nt-e164-clid** and **P-Location** headers.

When finished, all the Request Headers defined will be displayed under the Request Headers tab as shown below.

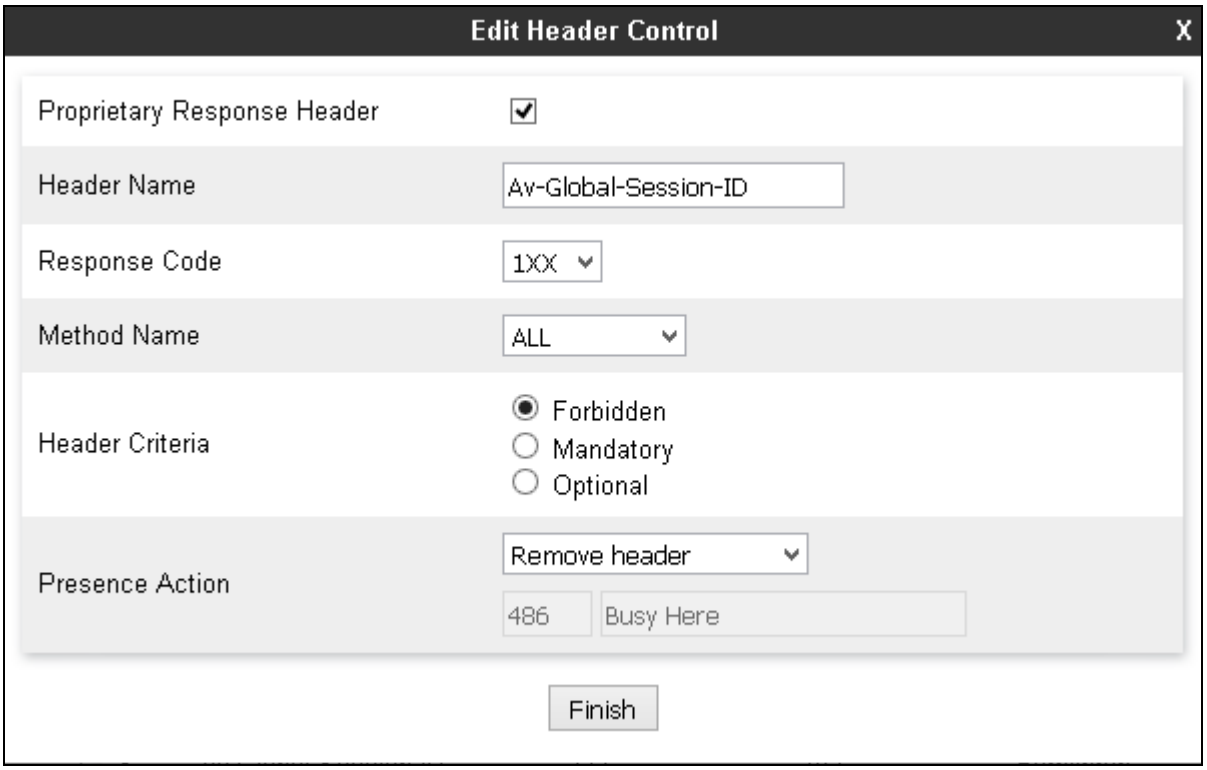


The same is required for **Response Headers**. Select the **Response Headers** tab (not shown) and define the rules to remove Avaya proprietary headers as follows:

- Click on **Add In Header Control** (not shown).
- Check the **Proprietary Request Header** box to remove Avaya proprietary headers or uncheck it to remove unnecessary headers.
- 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 on **Finish**.

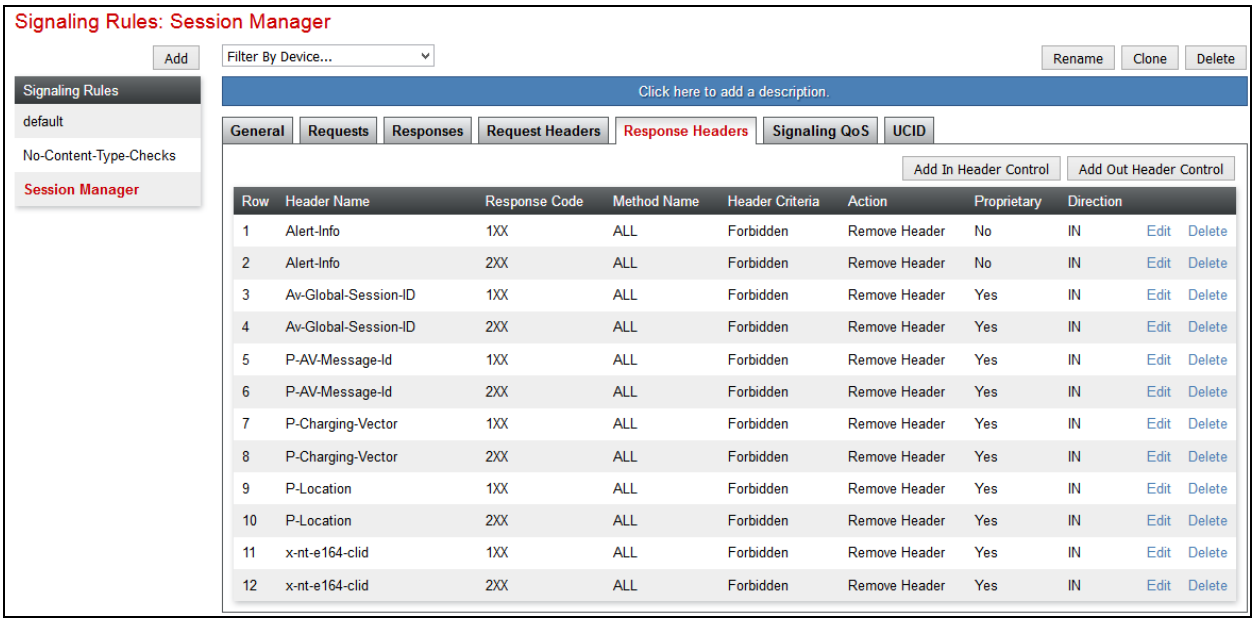
Repeat above process and select **2XX** in the **Response Code** so that the header is removed from 200 OK messages.

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



Note: During the 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 **Response Headers** defined will be shown under the **Response Headers** tab as shown below.



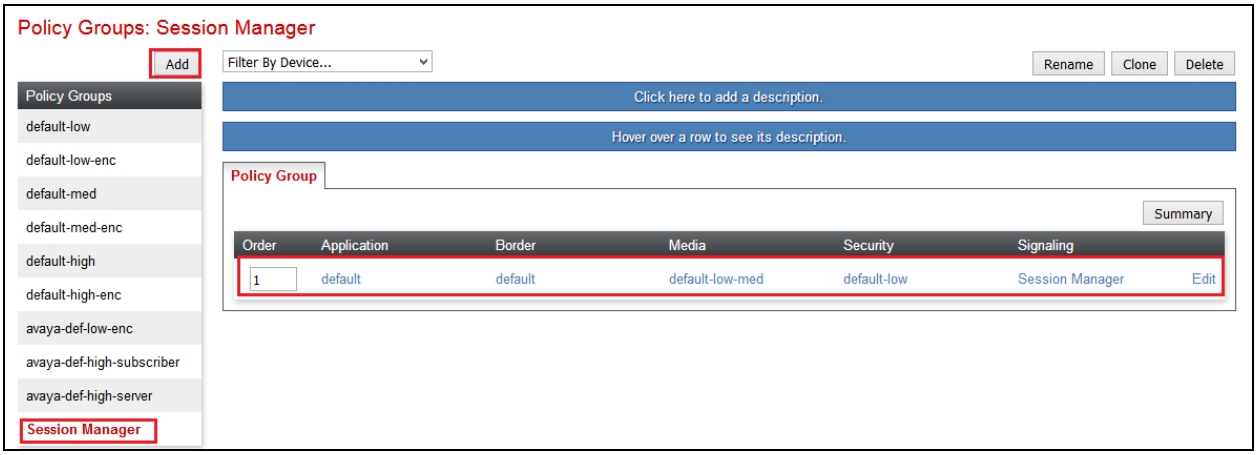
Row	Header Name	Response Code	Method Name	Header Criteria	Action	Proprietary	Direction		
1	Alert-Info	1XX	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
2	Alert-Info	2XX	ALL	Forbidden	Remove Header	No	IN	Edit	Delete
3	Av-Global-Session-ID	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
4	Av-Global-Session-ID	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
5	P-AV-Message-Id	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
6	P-AV-Message-Id	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
7	P-Charging-Vector	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
8	P-Charging-Vector	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
11	x-nt-e164-clid	1XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete
12	x-nt-e164-clid	2XX	ALL	Forbidden	Remove Header	Yes	IN	Edit	Delete

7.3.6 Endpoint Policy Groups

End point policy groups are required to implement the signaling rules. In the solution as tested, one group was defined.

To add a new policy group for Session Manager, navigate to **Domain Policies > End Point Policy Groups** in the main menu on the left hand side:

1. Click on **Add** button to add a new policy group, name it as **Session Manager**.
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 **Session Manager** (created in **Section 7.3.5**) for **Signaling Rules**.

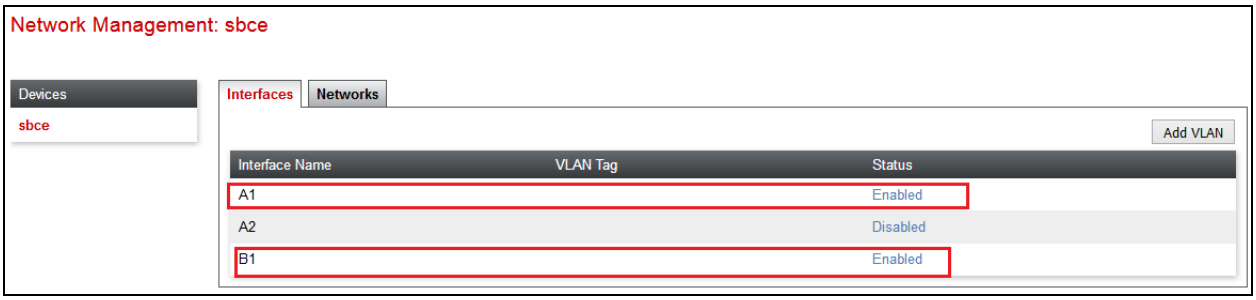


7.4 Device Specific Settings

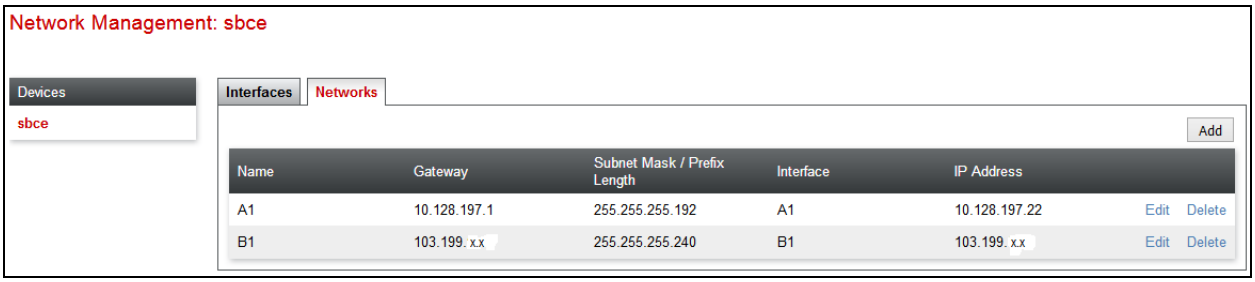
The **Device Specific Settings** feature for SIP allows you to view aggregate system information, and manage various device-specific parameters which determine how a particular device will function when deployed in the network. Specifically, you have the ability to define and administer various device-specific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

7.4.1 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.



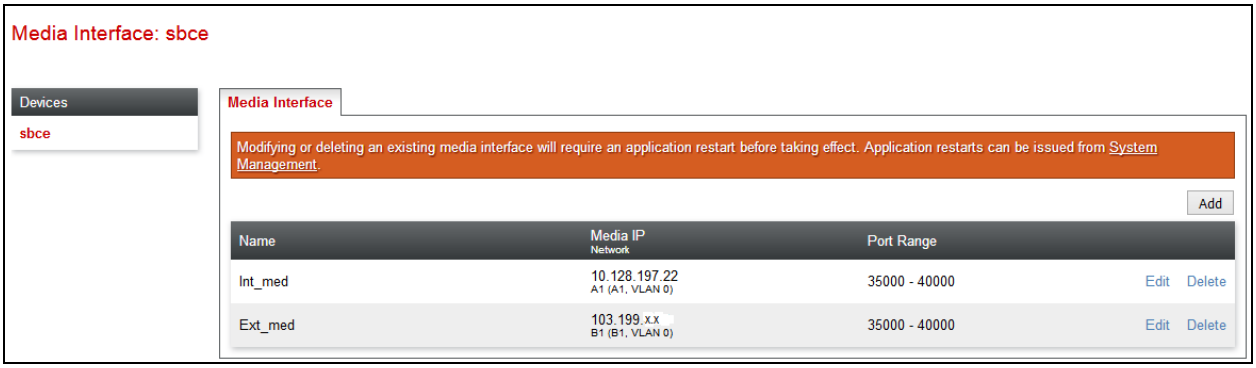
3. Select the **Networks** tab to display the IP provisioning for the A1 and B1 interfaces. These values are normally specified during installation. These can be modified by selecting **Edit**; however, some of these values may not be changed if associated provisioning is in use.



7.4.2 Media Interfaces

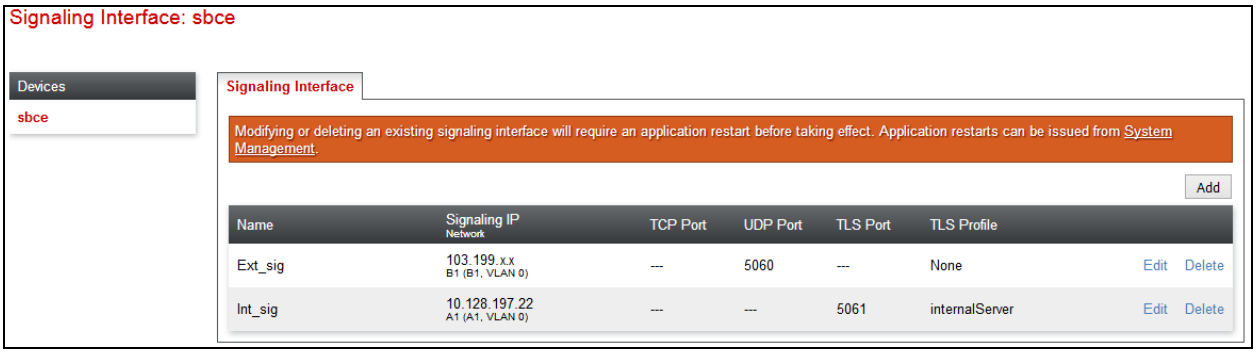
1. Navigate to **Device Specific Settings** from the menu on the left-hand side (not shown).
2. Select **Media Interface**.
3. Click on **Add** (not shown). The **Add Media Interface** window will open. Enter the following:
   - **Name**: **Int_med**.
   - **IP Address**: **10.128.197.22** (Avaya SBCE A1 address).
   - **Port Range**: **35000-40000**.
4. Click on **Finish** (not shown).

5. Click on **Add** (not shown). The **Add Media Interface** window will open. Enter the following:
   - **Name**: **Ext_med**.
   - **IP Address**: **103.199.x.x** (Avaya SBCE B1 address).
6. **Port Range**: **35000-40000**.
7. Click on **Finish** (not shown). Note that changes to these values require an application restart. The completed **Media Interface** screen is shown below.



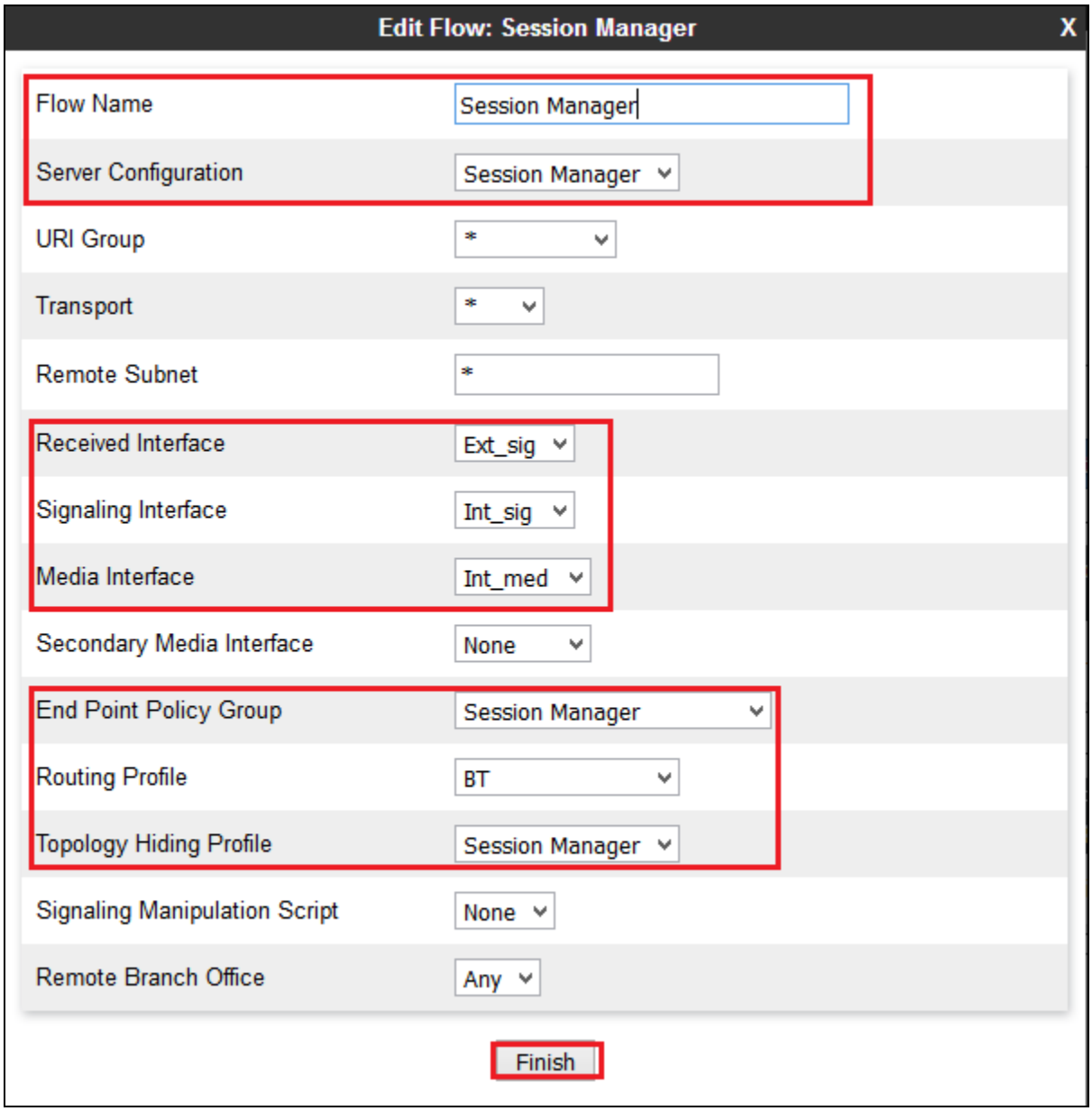
7.4.3 Signaling Interface

1. Navigate to **Device Specific Settings** from the menu on the left-hand side (not shown).
2. Select **Signaling Interface**.
3. Click on **Add** (not shown) and enter the following:
   - **Name**: **Int_sig**.
   - **IP Address**: **10.128.197.22** (Avaya SBCE A1 address).
   - **TLS Port: 5061**.
4. Click on **Finish** (not shown).
5. Click on **Add** again, and enter the following:
   - **Name**: **Ext_sig**.
   - **IP Address**: **103.199.x.x** (Avaya SBCE B1 address).
   - **UDP Port: 5060.**
6. Click on **Finish** (not shown). Note that changes to these values require an application restart.



7.4.4 Endpoint Flows – For Session Manager

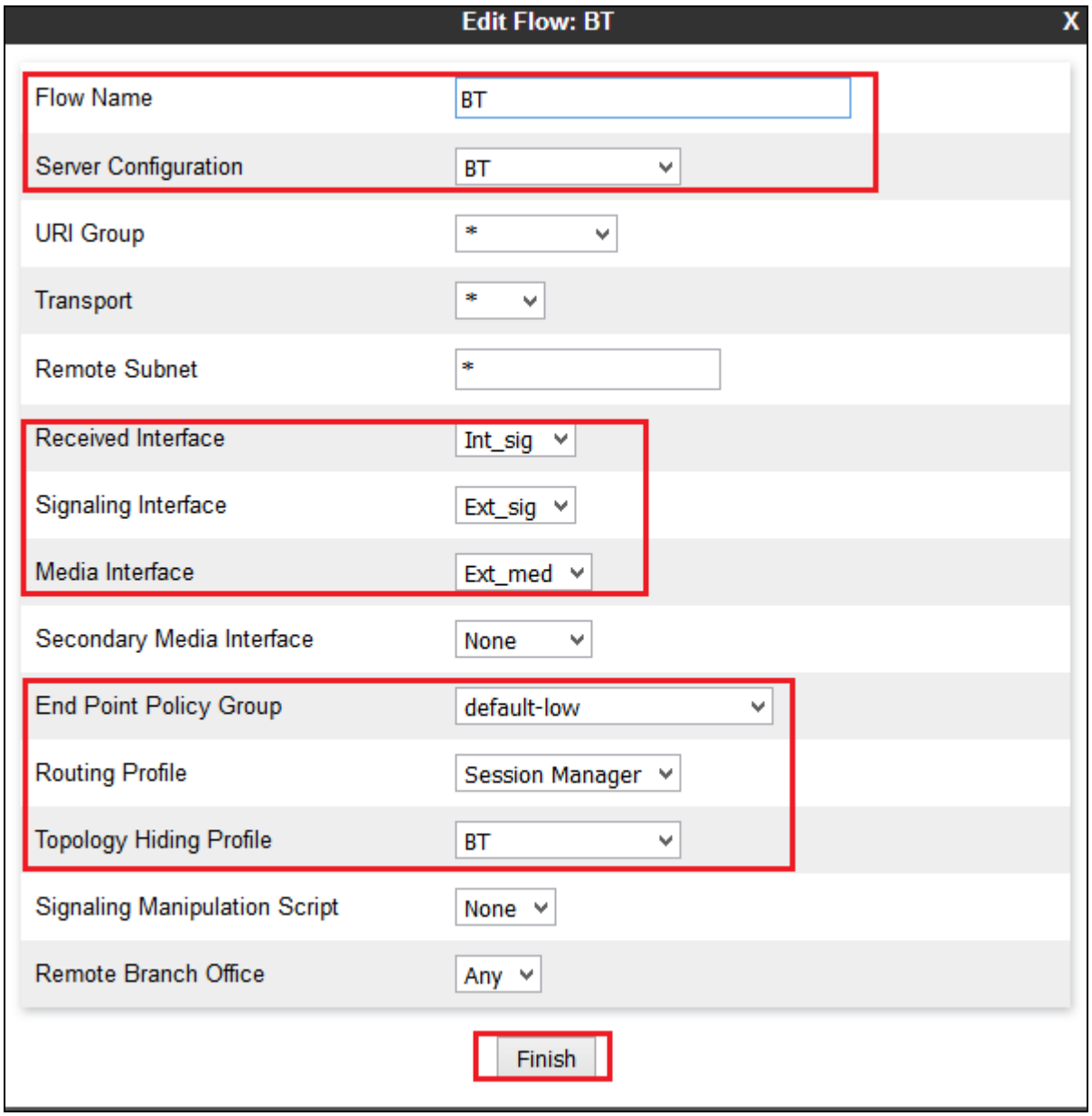
1. Navigate to **Device Specific Settings → Endpoint Flows** from the menu on the left-hand side (not shown).
2. Select the **Server Flows** tab (not shown).
3. Click on **Add**, (not shown) and enter the following:
   - **Name**: **Session Manager**.
   - **Server Configuration**: **Session Manager**.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



7.4.5 Endpoint Flows – For BT Wholesale

Repeat step **1** through **4** from **Section 7.4.4**, with the following changes:

- **Name**: **BT**.
- **Server Configuration**: **BT**.
- **Received Interface**: **Int_sig**.
- **Signaling Interface**: **Ext_sig**.
- **Media Interface**: **Ext_sig**.
- **End Point Policy Group**: **default-low**.
- **Routing Profile**: **Session Manager**.
- **Topology Hiding Profile**: **BT**.



8. Verification Steps

The following steps may be used to verify the configuration.

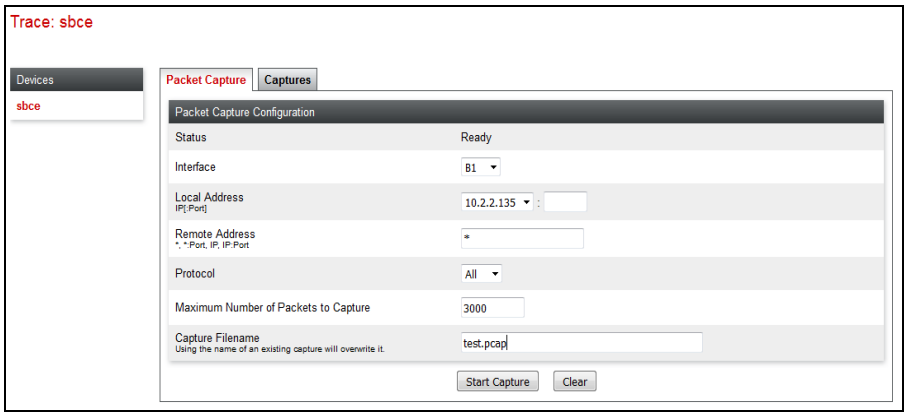
8.1 Avaya Session Border Controller for Enterprise

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.

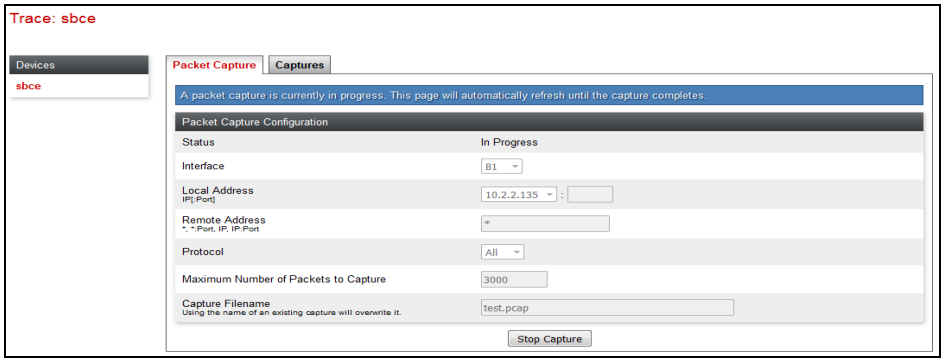
Protocol Traces

The Avaya SBCE can take internal traces of specified interfaces.

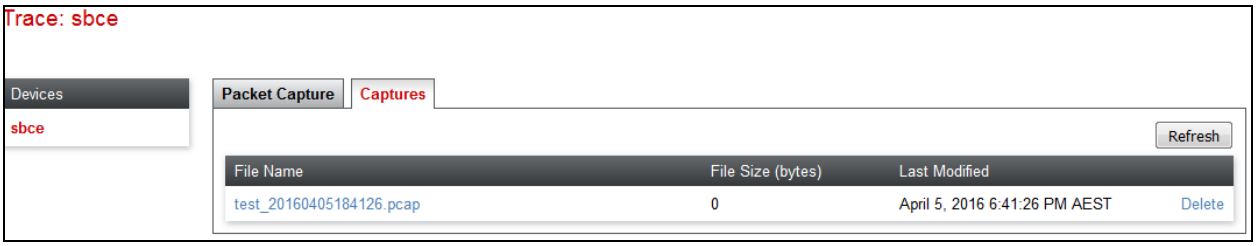
1. Navigate to **Device Specific Settings → Troubleshooting → Trace**.
2. Select the **Packet Capture** tab and select the following:
   - Select the desired **Interface** from the drop down menu (e.g., **All**).
   - Specify the **Maximum Number of Packets to Capture** (e.g., **5000**).
   - Specify 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:



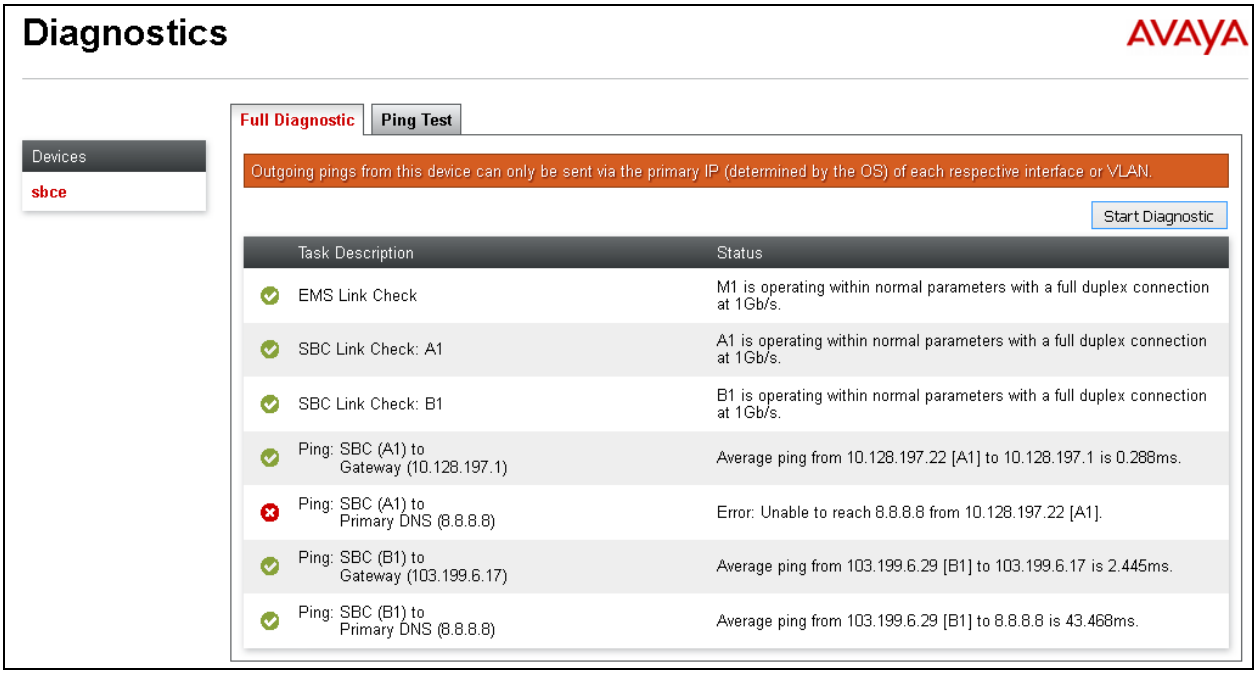
3. Run the test.
4. When the test is completed, select the **Stop Capture** button shown above.
5. Click on the **Captures** tab and the packet capture is listed as a *.pcap* file with the date and time added to filename specified in **Step 2**.
6. Click on the **File Name** link to download the file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

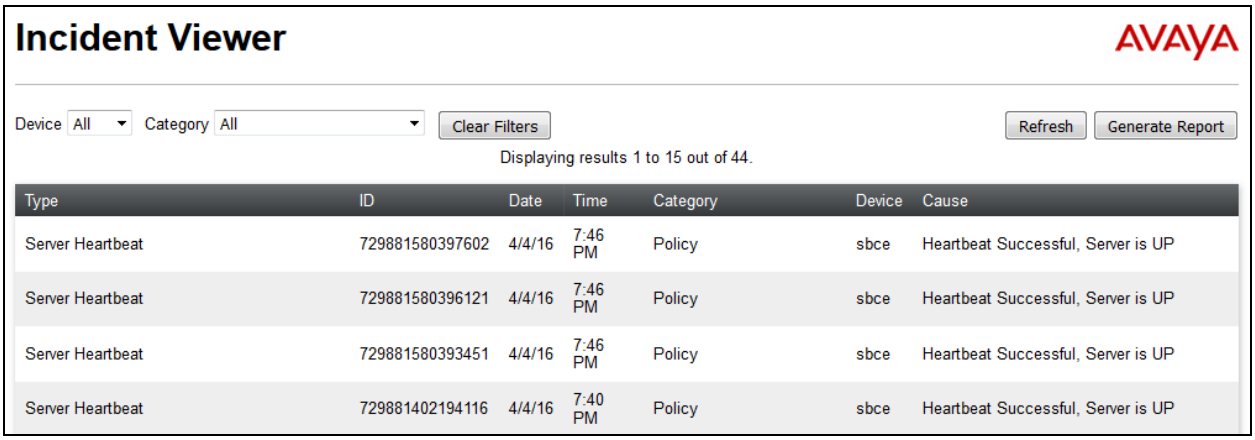


The following section details various methods and procedures to help diagnose call failure or service interruptions. As detailed in previous sections, the demarcation point between the BT Wholesale Hosted SIP Trunking Service and the customer SIP PABX is the customer SBC.

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 network gateway.
- Ping from the SBC to DNS.
- 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 92 0
009 UNIT(S) IDLE
001 UNIT(S) BUSY
000 UNIT(S) DSBL
000 UNIT(S) MBSY
```

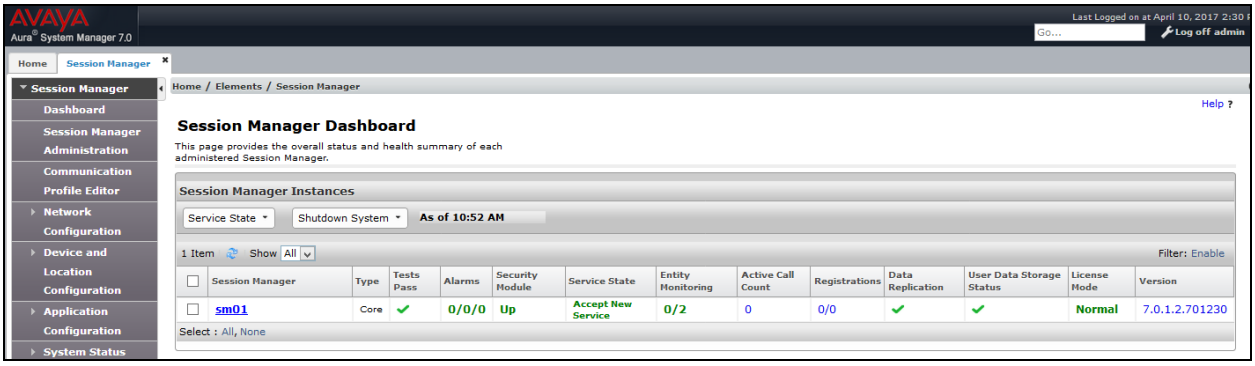
After the call is released, check that SIP trunk status. It should change to the **IDLE** state.

```
>ld 32
NPR000
.stat 92 0
010 UNIT(S) IDLE
000 UNIT(S) BUSY
000 UNIT(S) DSBL
000 UNIT(S) MBSY
```

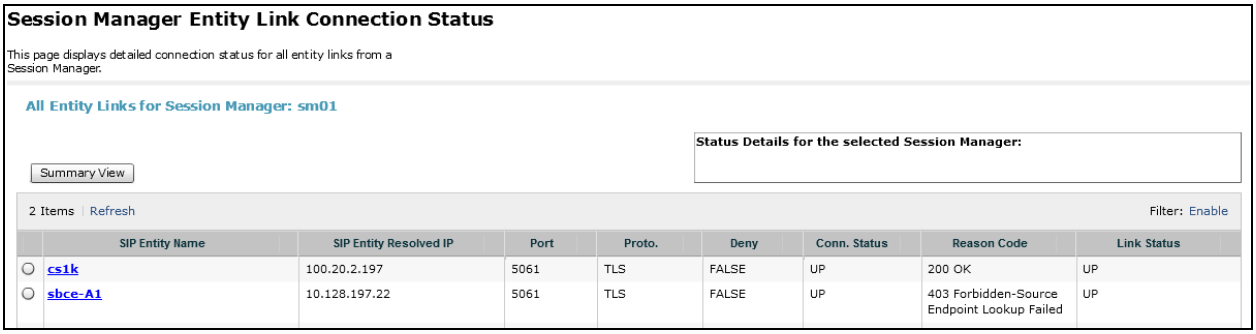
8.3 Avaya Aura® Session Manager Status

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.
3. Clicking on the **0/2** 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 SP8, Avaya Aura® Session Manager Release 7.0.1 SP2, and Avaya Session Border Control for Enterprise Release 7.1 SP2 can be configured to interoperate successfully with BT Wholesale Hosted SIP Trunking Service. This solution allows enterprise users access to the PSTN using the BT Wholesale Hosted 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 Release 7.0.1*.
[2] *Administering Avaya Aura® System Manager for Release 7.0.1*.
[3] *Administering Avaya Aura® Session Manager Release 7.0.1*.
[4] *Deploying Avaya Aura Session Manager Release 7.0.1*.
[5] *Deploying Avaya SBCE on VMware in Virtualized Environment Release 7.1*.
[6] *Administering Avaya Session Border Controller Release 7.1*.
[7] *Document Collection - Communication Server 1000 Release 7.6*.
[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 BT Wholesale Hosted SIP Trunking Service is available from BT Wholesale.

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.