Application Notes for Configuring ASBCE for SIP Trunk Solution using SIP Trunk and Mitel 3300 with Avaya Session Border Controller for Enterprises – Issue 1.0

Abstract

These Application Notes describe a sample configuration using Session Initiation Protocol (SIP) trunking between SIP Trunk and Mitel 3300. In the sample configuration, the Mitel solution consists of a sole controller, embedded voicemail, and Mitel endpoints.

A Service Provider SIP Trunk is used as reference Test SIP Trunk for this Validation. The SIP offer referenced within these Application Notes enables a business to send and receive calls via standards-based SIP trunks, without the need for additional TDM enterprise gateways or TDM cards and the associated maintenance costs.

Information in these Application Notes has been obtained through Tekvizion labs interoperability testing and additional technical discussions. Testing was conducted in the Tekvizion Test Lab, utilizing a service provider SIP Trunk test service.

Table of Contents

1. Introduction

These Application Notes describe a sample configuration using Session Initiation Protocol (SIP) trunking between SIP Trunking Service and Mitel 3300 solution. In the sample configuration, the Mitel 3300 solution consists of a controller, embedded voicemail, and Mitel endpoints.

In the sample configuration, An Avaya Session Border Controller for Enterprise (SBCE) is used as session border controller device between the Mitel 3300 and SIP Trunk Service. Any SIP trunk can be deployed in the same mode as required for the field deployment. The Avaya SBCE performs SIP header manipulation and provides topology hiding with other multiple SBC functionalities.

Customers using Mitel and the SIP Trunk service with Avaya Session Border controller are able to send and receive PSTN via the SIP protocol. The converged network solution is an alternative to traditional PSTN trunks such as ISDN-PRI.

2. General Test Approach and Test Results

The Mitel 3300 location was connected to the SIP test service, as depicted in **Figure 1**. The Avaya SBCE and Mitel 3300 were configured to use the test SIP trunk. This allowed Mitel 3300 to receive and send calls from the PSTN via the SIP protocol.

2.1. Interoperability Compliance Testing

To summarize, the testing included the following successful SIP trunk interoperability compliance testing:

- SIP OPTIONS monitoring of the health of the SIP trunk was not verified.
- Incoming calls from the PSTN were routed to the numbers assigned by SIP Trunk service provider to the Mitel 3300 location. These incoming calls arrived via the SIP Line and were answered by Mitel telephones and Mitel embedded voicemail.
- Proper disconnect when either party hangs up an active call.
- Proper disconnect when the PSTN caller abandons (i.e., hangs up) a call before the Mitel 3300 party has answered.
- Proper SIP 486 response and busy tone heard by the caller when a PSTN user calls a number directed to a busy Mitel 3300 user.
- Proper termination of an inbound call left in a ringing state for a relatively long duration.
- The display of caller ID on display-equipped Mitel 3300 telephones was verified. The Mitel 3300 capability to use the caller ID received from the SIP Trunk service provider to look up and display a name from a configurable directory was also exercised successfully.
- Privacy requests for inbound calls from the PSTN were verified. That is, when privacy is requested by a PSTN caller (e.g., dialing *67), the inbound call can be successfully completed to a Mitel 3300 telephone user while presenting a “WITHHELD” or anonymous display to a Mitel 3300 user (i.e., rather than the caller’s telephone number).
- Inbound long holding time call stability.

- Mitel 3300 complies with RFC 3261 SIP Methods.
- Mitel 3300 can use UDP for SIP transport with SIP Trunk service provider.
- Mitel 3300 accepts the full SIP headers sent by SIP Trunk service provider.
- Mitel 3300 sends SIP 180 RINGING (no SDP in 180) for inbound calls and ring back tone is heard by the caller.
- Mitel 3300 does not return a SIP 302 to SIP Trunk service provider.
- Telephony features such as hold and resume, transfer of calls to other Mitel 3300 users, and conference calls.
- Incoming voice calls using the G.729(a) and G.711 ULAW codecs, and proper protocol procedures related to media.
- DTMF transmission using RFC 2833. Successful Mitel 3300 embedded voice mail menu navigation for incoming calls.
- Outgoing calls from the Mitel 3300 location to the PSTN were routed via a SIP Line to the SIP Trunk test service. The display of caller ID on display-equipped PSTN telephones was verified. In the context of inbound calls using SIP trunk test service, inbound calls arriving via the SIP Line could be forwarded to the SIP Trunk test Service.
- Call forwarding of calls to PSTN destinations via the SIP Trunk service documented in reference, presenting true calling party information to the PSTN phone.
- Mitel 3300 have analog phone ports. This allowed the testing of Fax calls. Fax testing requires a separate piece of hardware. IADs or Media Gateways can be used

2.2. Test Observations

The following observations may be noteworthy:

1. Although the SIP trunking test service supports transfer using the SIP REFER method. Mitel 3300 does not support sending REFER, Mitel 3300 did not send REFER to SIP Trunk service provider in the verified configuration.

2. During compliance testing, one Avaya SBCE was used to support SIP trunk test service for inbound and outbound calls. One SIP Trunk was created on Mitel 3300 to connect the Avaya SBCE.

3. The SIP The SIP protocol allows sessions to be refreshed for calls that remain active for some time. In the tested configuration, neither SIP Trunk service provider nor Mitel 3300 send SIP re-INVITE or UPDATE messages to refresh a session. This is transparent to the users of the call and media path remains established.

4. Proper DiffServ markings for Avaya SBCE SIP signaling and RTP media were not tested. The QOS markings are not propagated by our Internet Service Provider.

5. IP address and port were used instead of FQDNs. DNS SRV resolution was not tested.

6. To get ringback on blind transfers to PSTN scenarios, the “Suppress Use of SDP Inactive Media Streams” needs to be set to “Yes” on the Mitel 3300.

2.3. Test Results

Interoperability testing of the sample configuration was completed with successful results.

The SIP Trunk Service passed compliance testing.

2.4. Support

2.4.1. Avaya

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

2.4.2. Mitel 3300

For technical support on the Mitel products described in these application notes visit http://www.mitel.com/services-support/

3. Reference Configuration

Figure 1 illustrates an example Mitel 3300 solution connected to the SIP Trunk test service through ASBCE. The Mitel 3300 and ASBCE equipment is located on a private IP subnet. An enterprise edge router provides access to the SIP Trunk service network via a SIP Trunk Providers VPN. This VPN is optional based on the deployment requirement and is provisioned for the SIP Trunk test service as Service provider requirement.

In the sample configuration, the Avaya SBCE receives traffic from the service provider SIP trunk test service on port 5060 and sends traffic to port 5072, using UDP for network transport, as required by the service provider SIP Trunk test service. The Avaya SBCE in turn sends and receives traffic to and from Mitel 3300 using UDP/TCP port 5060. Service provider gave two numbers associated with the SIP Trunk test service. These numbers were mapped Mitel 3300 directory numbers.

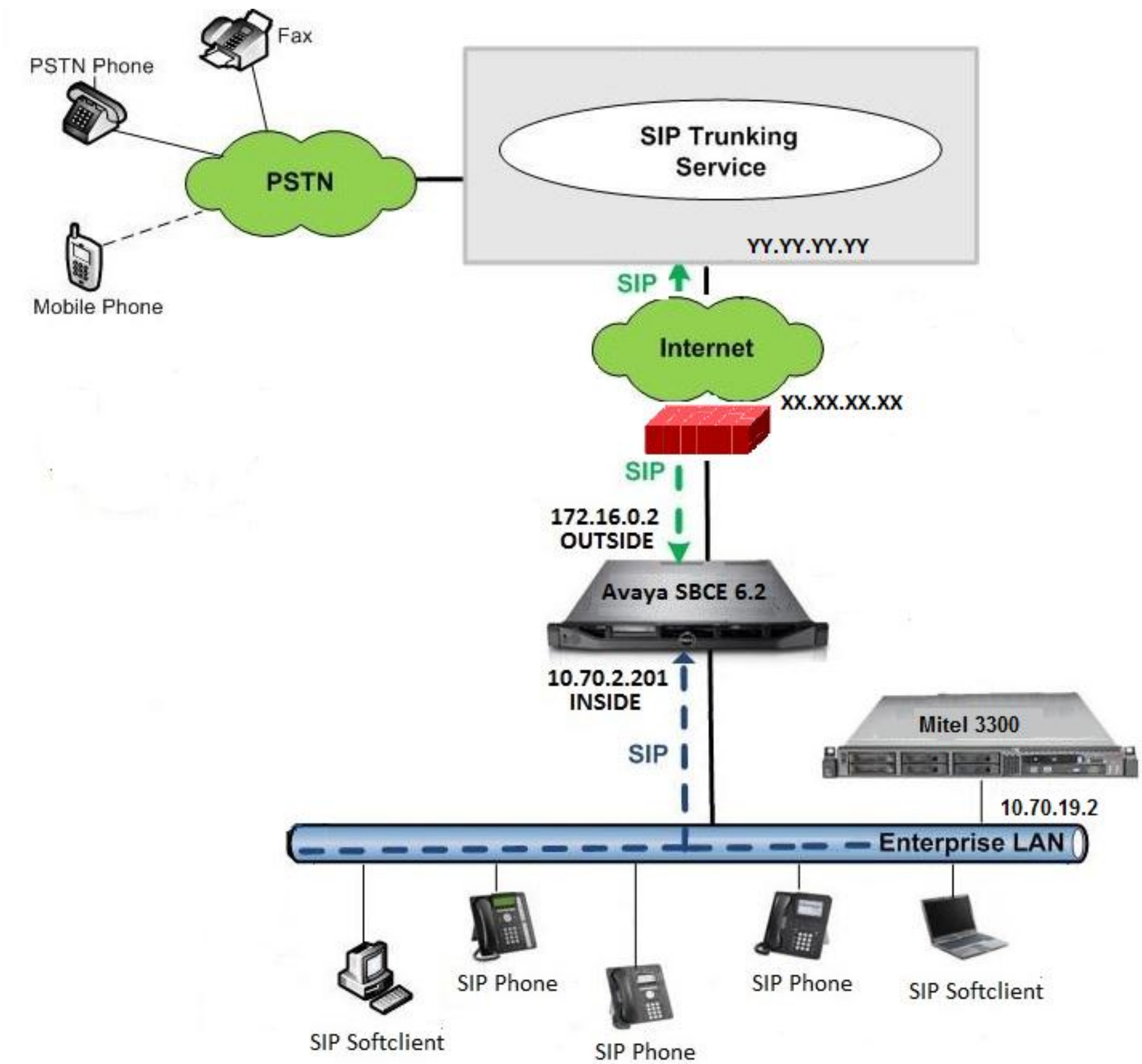


Figure 1: Mitel 3300 with SIP Trunk Service.

Note: Firewall between Service Provider and the Enterprise edge (in this case Test Lab environment) is optional component and can be setup based on the network planning requirements of the customer.

4. Equipment and Software Validated

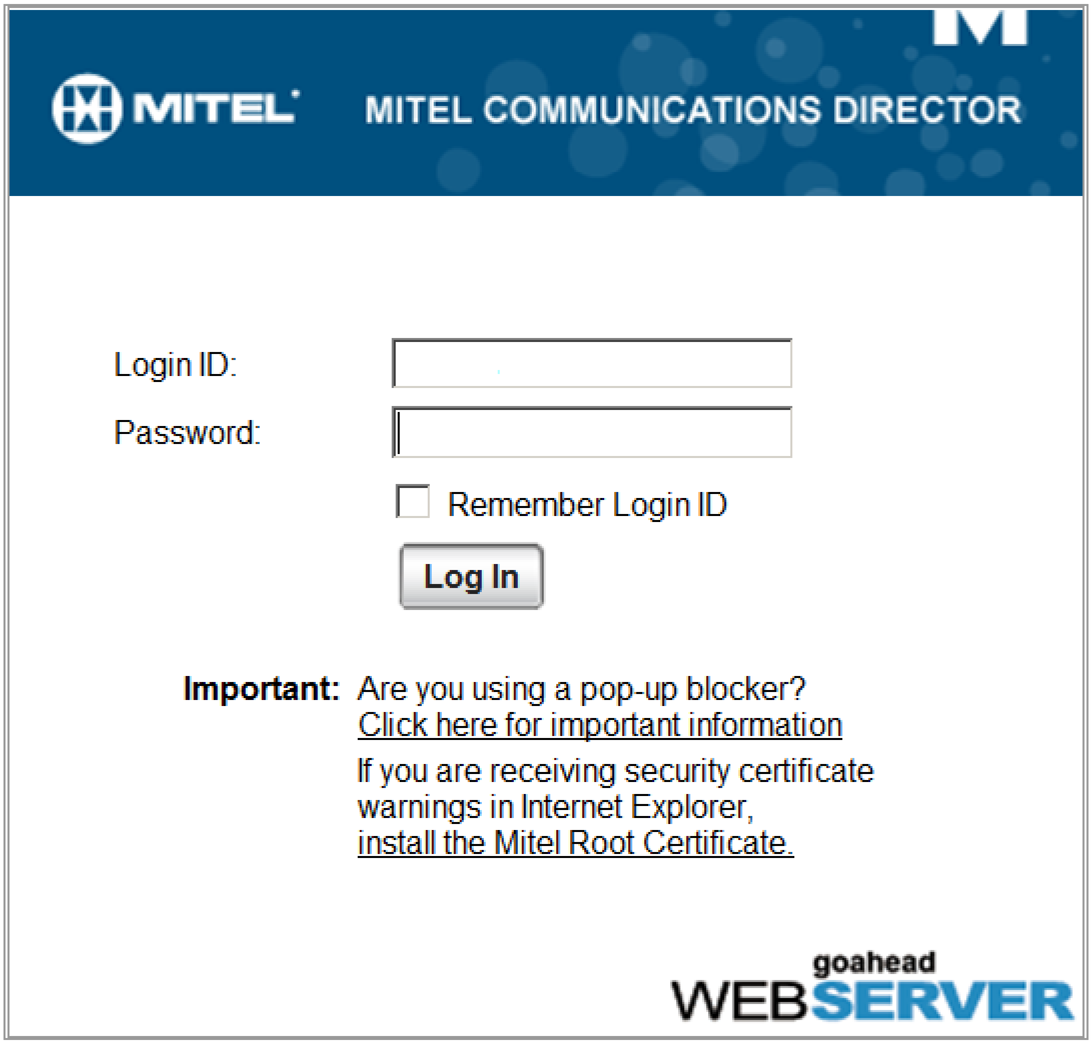
Table 1 shows the equipment and software used in the sample configuration.

Equipment	Software
Avaya Session Border Controller for Enterprise	Release 6.2 (Q54)
Mitel 3300	Release 6.0
Mitel 5360 IP Phone	05.02.00.15
Mitel 5224 IP Phone	02.05.00.05

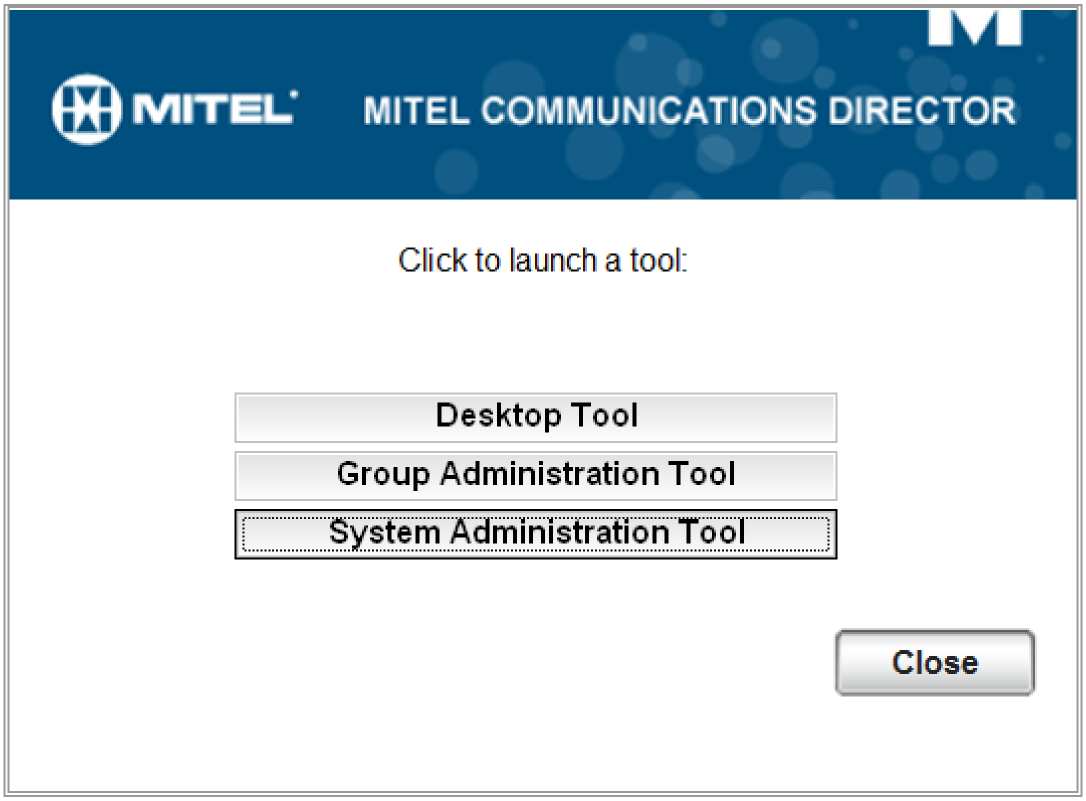
Table 1: Equipment and Software Tested

5. Mitel 3300

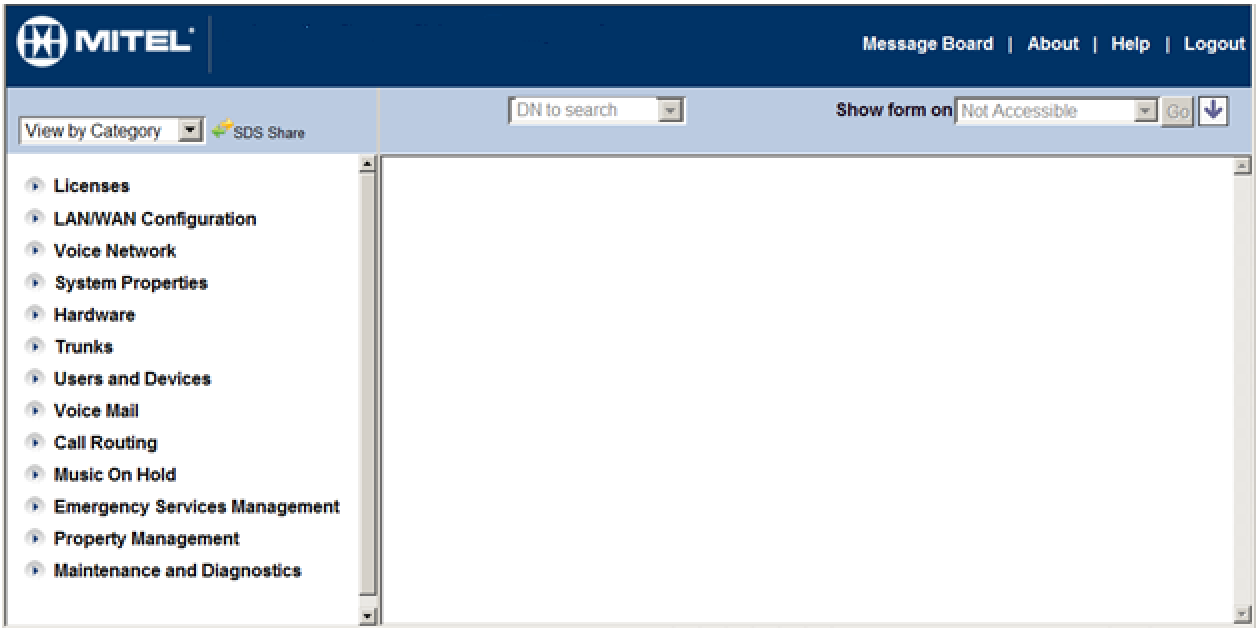
Mitel 3300 is configured via http://<IP address or FQDN>. For more information Mitel 3300, consult reference [2]. From the Mitel Communications Director web page, enter the **Login ID** and **password** ant the Click the **Log in** button.


MITEL
MITEL COMMUNICATIONS DIRECTOR
Login ID:
Password:
Remember Login ID
Log In
Important: Are you using a pop-up blocker?
Click here for important information
If you are receiving security certificate warnings in Internet Explorer,
install the Mitel Root Certificate.
goahead
WEBSERVER

The launch tool is displayed. Click in the **System Administration Tool** button.



The system administration tool appears.



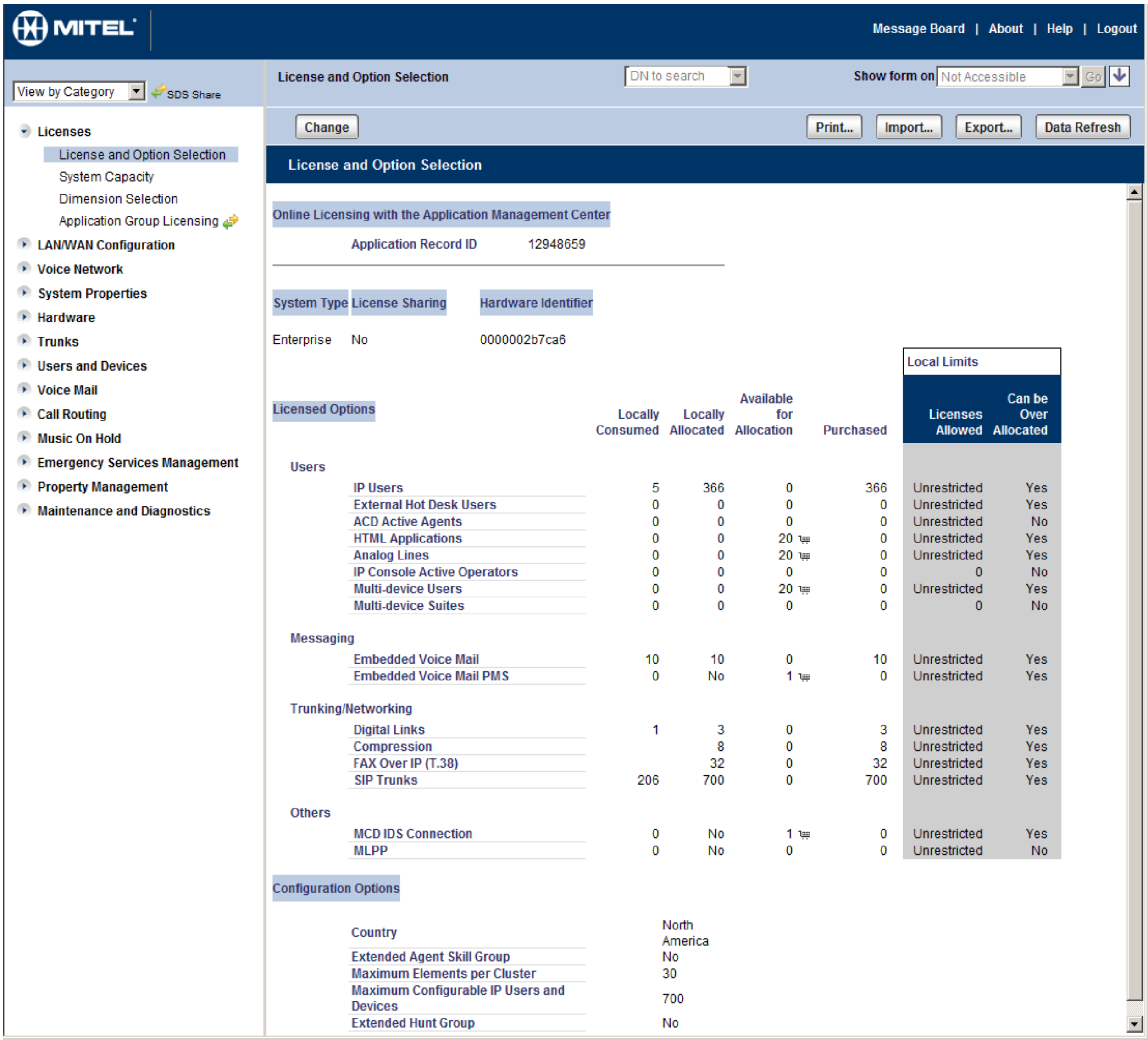
5.1. Physical Network

The Mitel 3300 network configuration is typically done during installation. Consult reference [1] for more information on the topics in this section.

5.2. Licensing

The configuration and features described in these Application Notes require the Mitel 3300 system to be licensed appropriately. If a desired feature is not enabled or there is insufficient capacity, contact an authorized Mitel sales representative. License information can be found on reference[2].

To verify that there are sufficient licenses, in the left navigation pane select **Licenses -> License and Option Selection.**



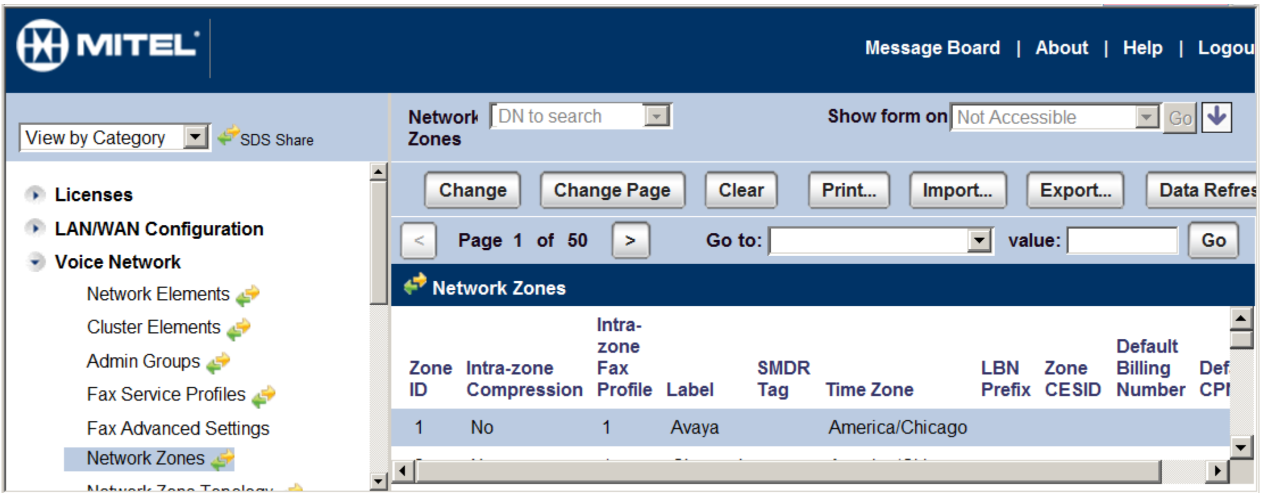
5.3. System Settings

This section illustrates the configuration of system settings. The settings presented here simply illustrate the sample configuration and are not intended to be prescriptive. Make sure that installation instructions in reference [1] were followed and the servers are ready to be configured. Default values were used as possible to provision information.

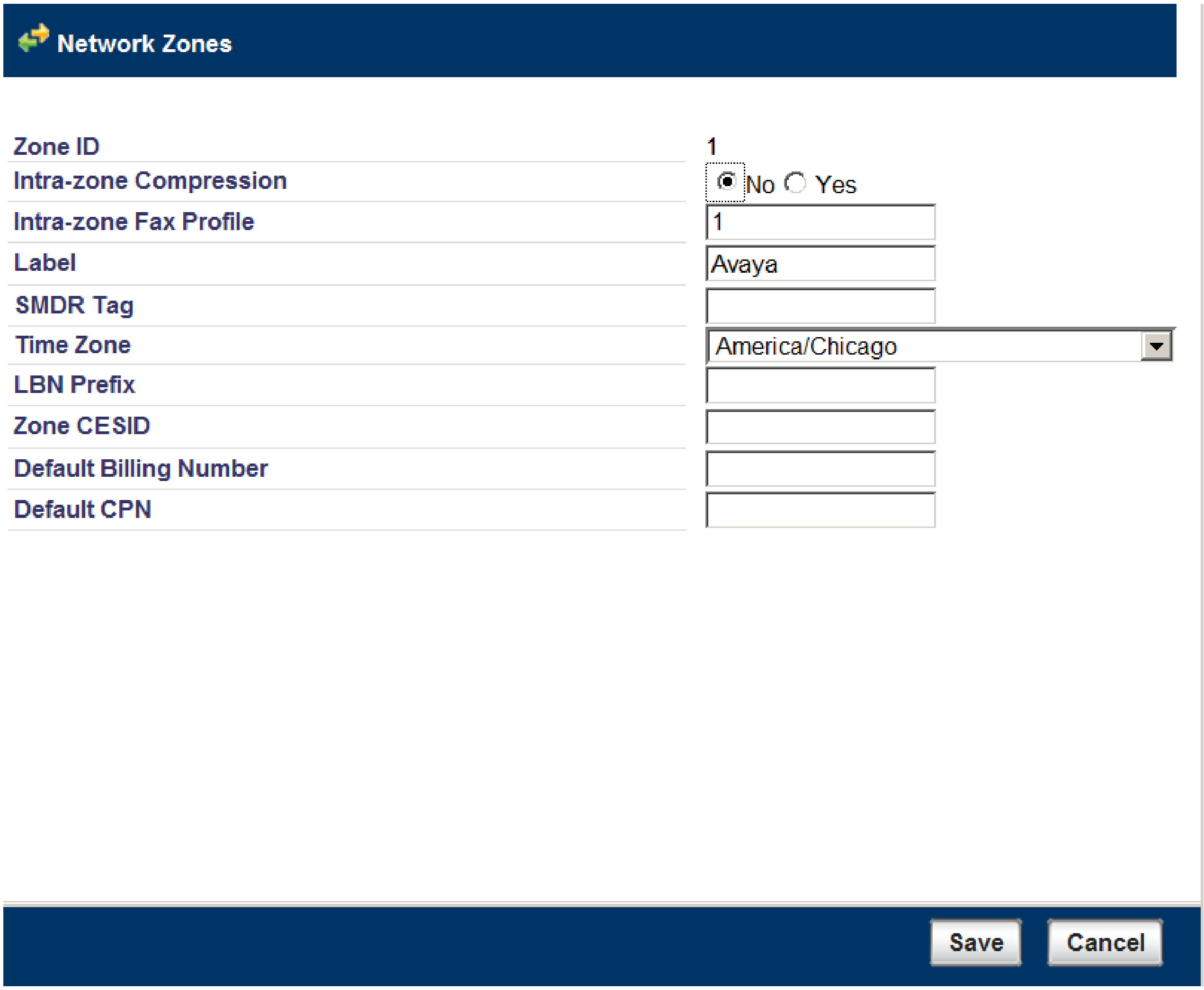
There are several elements required to be created to communicate with Avaya Session Border Controller for Enterprise.

5.3.1. Network Zone

To configure a network zone from the **Voice Network** Menu Select **Network Zones**. Then select one of the available zones and click the **Change** button.

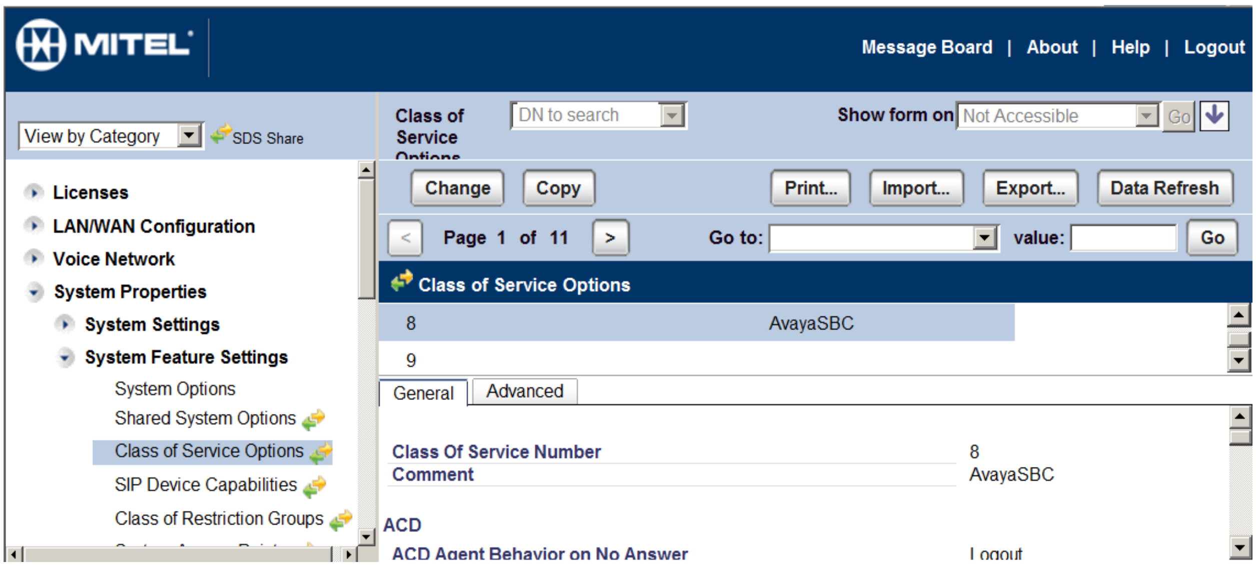


The **Network Zones** window appears. Enter a label name in the **Label field.** Select the appropriate **Time Zone**. Click the **Save** button.


Network Zones
Zone ID
1
Intra-zone Compression
No Yes
Intra-zone Fax Profile
1
Label
Avaya
SMDR Tag
Time Zone
America/Chicago
LBN Prefix
Zone CESID
Default Billing Number
Default CPN
Save
Cancel

5.3.2. Class of Service Options

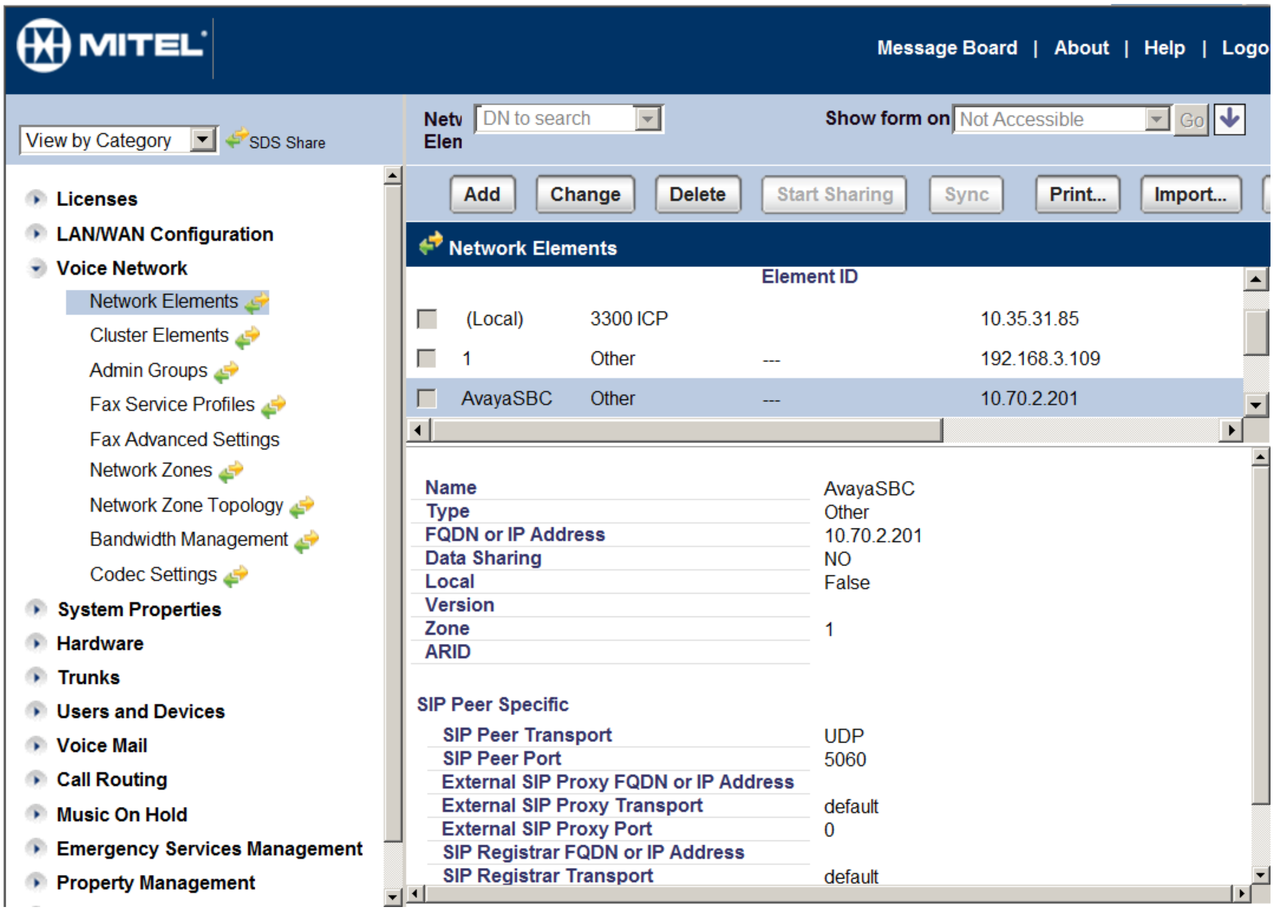
1. Navigate to **System Properties-> System Feature Settings-> Class of Service Options**.
2. In right frame of the window, select a Class of Service Number and click on **Change**.



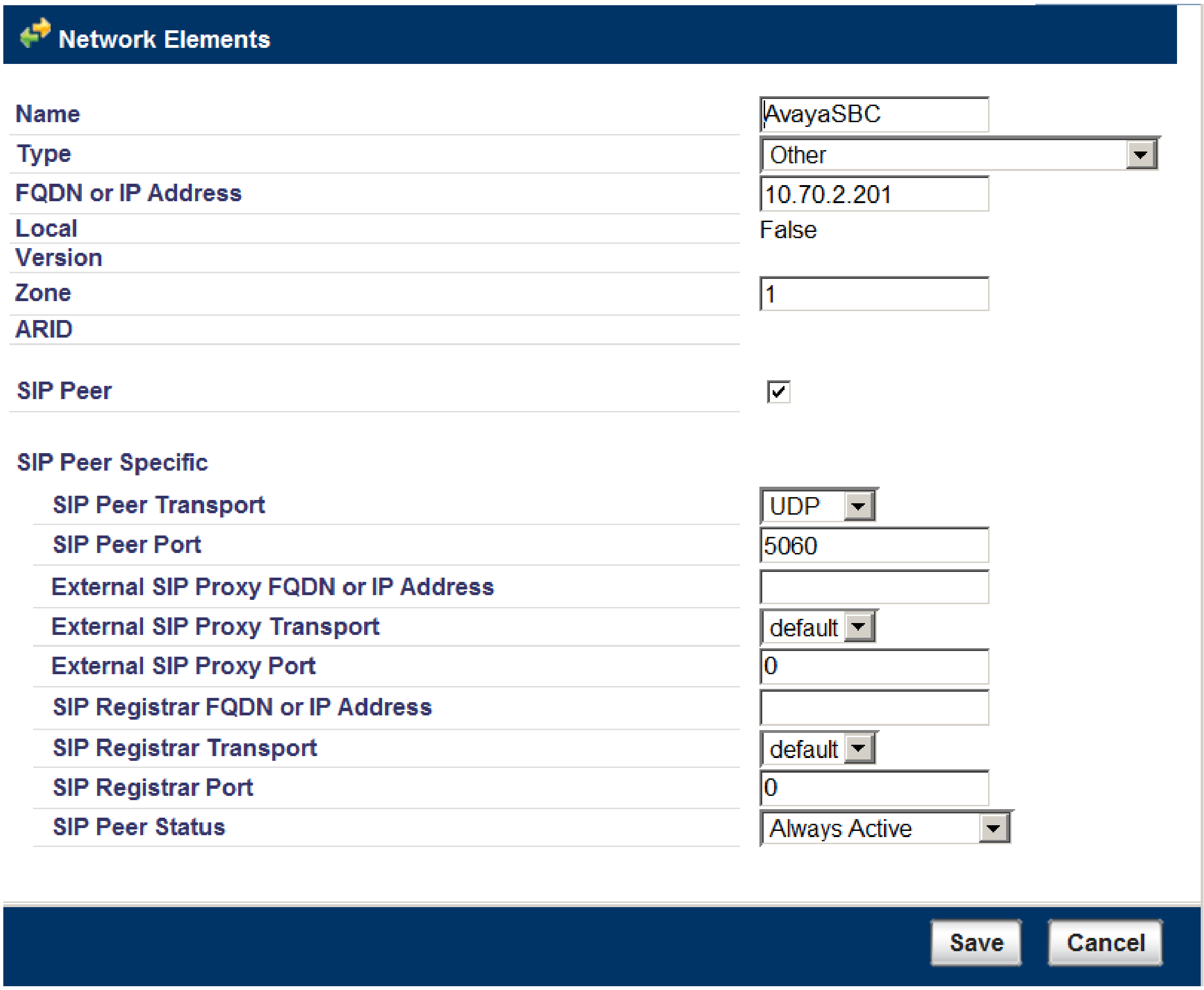
Enter a **Comment**. In our example AvayaSBC was entered. You can leave the rest of the fields with the defaults values.

5.3.3. Network Element

1. Navigate to **Voice Network > Network Elements.**
2. In the Right Frame of the window Click **Add**.

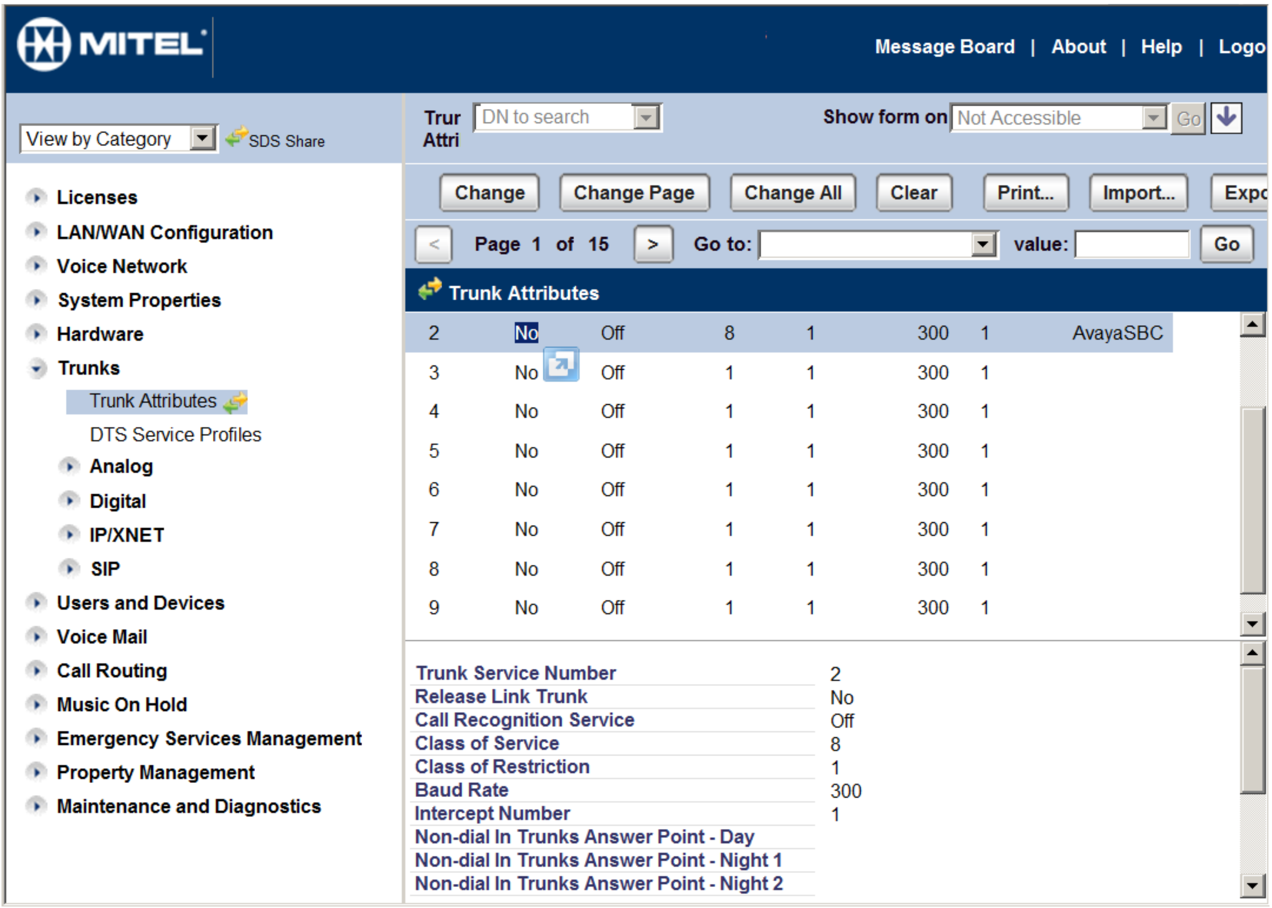


1. A new pop-up window opens as shown in the figure below.
2. Set **Name**: AvayaSBC is given for this example.
3. Set **Type**: Other is selected from the drop down menu.
4. Set **FQDN or IP Address**: Enter the internal IP address of the SBC.
5. Set **Zone**: 1 is given for this example.
6. Set **Peer Transport**: UDP is selected from drop down menu.
7. Set **SIP Peer Port**: 5060.
8. Set **SIP Peer Status**: Always Active is selected from drop down menu.
9. Click **Save**.

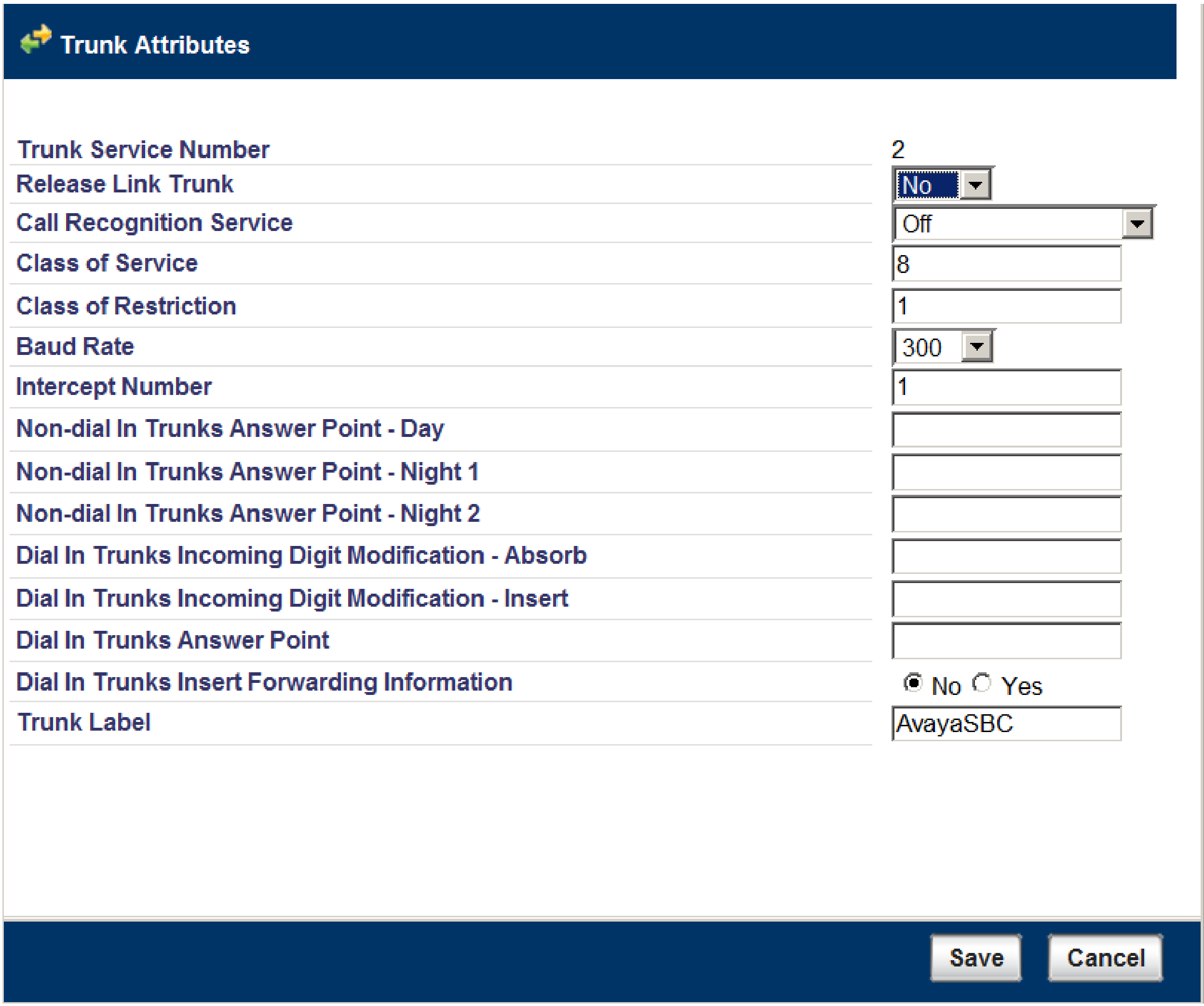


5.3.4. Trunk Attributes

1. Navigate To **Trunks > Trunk Attributes**.
2. Right click on the Trunk Service number and click **Change**.

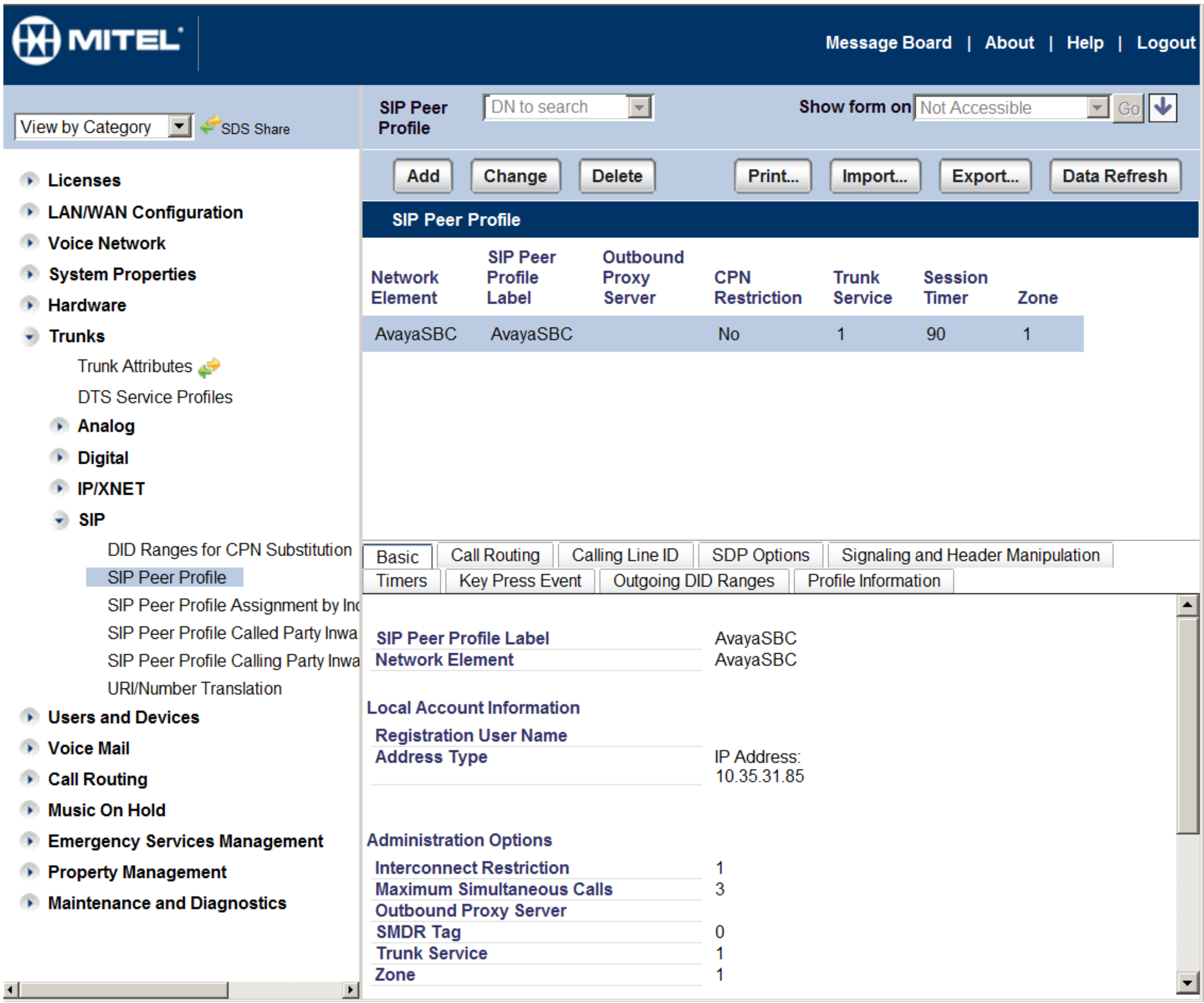


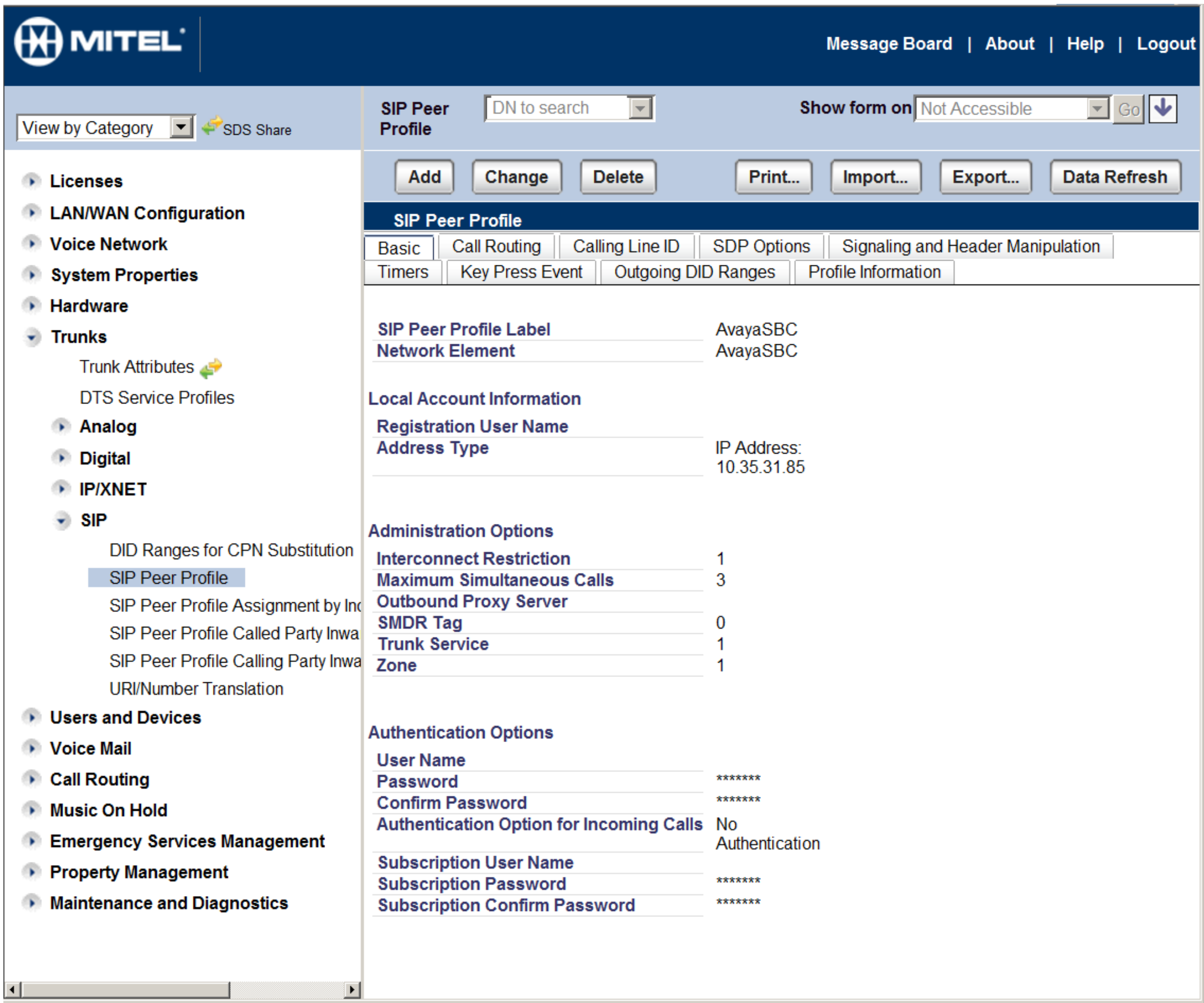
1. A new pop-up window opens as shown in the figure below.
2. Set **Release Link Trunk**: NO
3. Set **Call Recognition Service**: Off
4. Set **Class of Service**: Enter the Class of Service Number you have created before.
5. Set **Class of Restriction**: Set the Class of Restriction, 1 is used here for example
6. Set **Baud Rate**: 300
7. Set **Intercept Number**: 1
8. Confirm Non-dial In Trunks Answer Point-Day: is blank (no data)
9. Confirm Non-dial In Trunks Answer Point-Night1: is blank (no data)
10. Confirm Non-dial In Trunks Answer Point-Night2: is blank (no data)
11. Set **Dial In Trunks Incoming Digit Modification-Absorb**: 6
12. Confirm Dial In Trunks Incoming Digit Modification-Insert: is blank (no data)
13. Confirm Dial In Trunks Answer Point: is blank (no data)
14. Set **Dial In Trunks Insert Forwarding Information**: No
15. Set **Trunk Label**: Set a label for the trunk you are currently creating, "AvayaSBC" is used here for example.
16. Click **Save**.

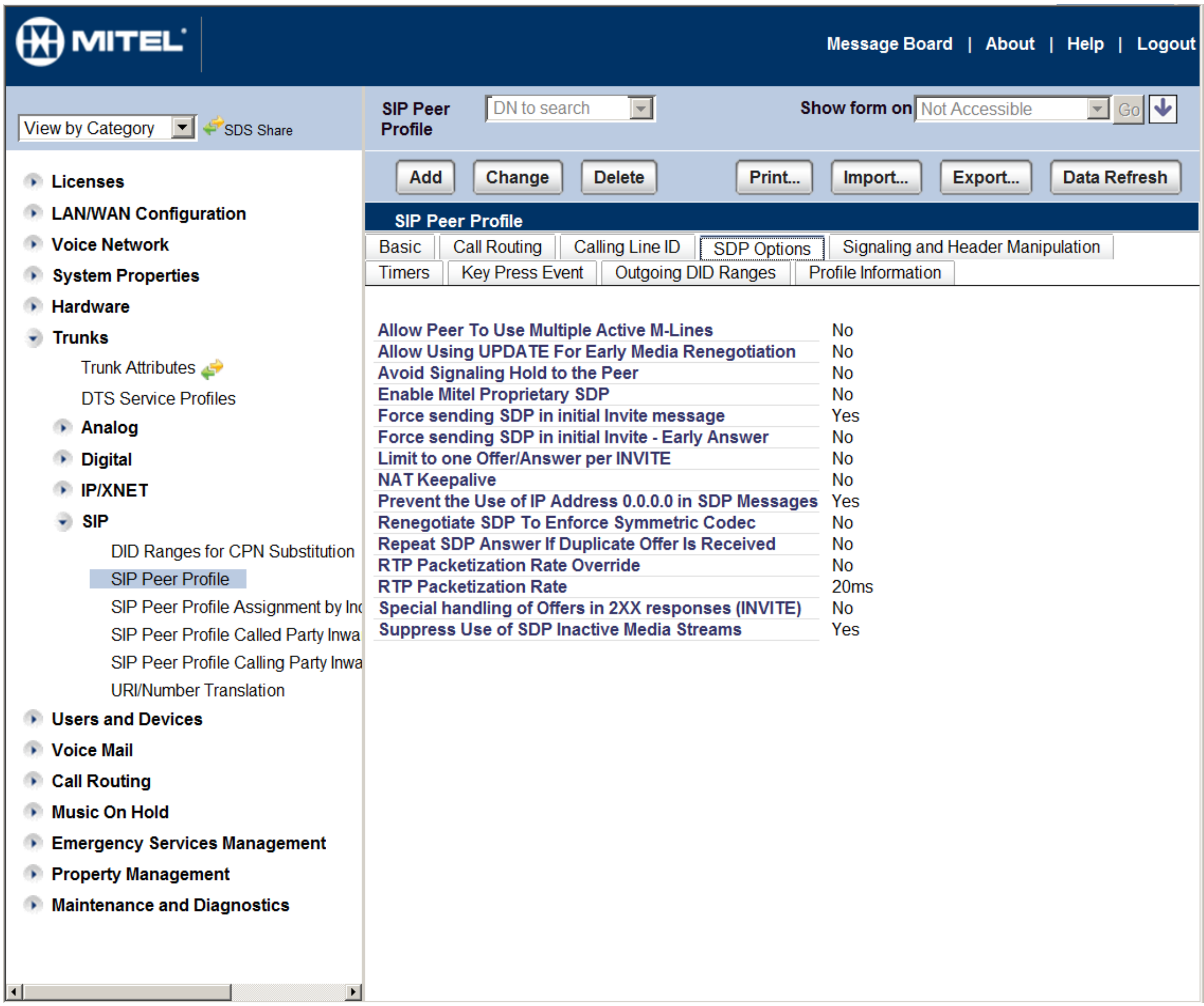


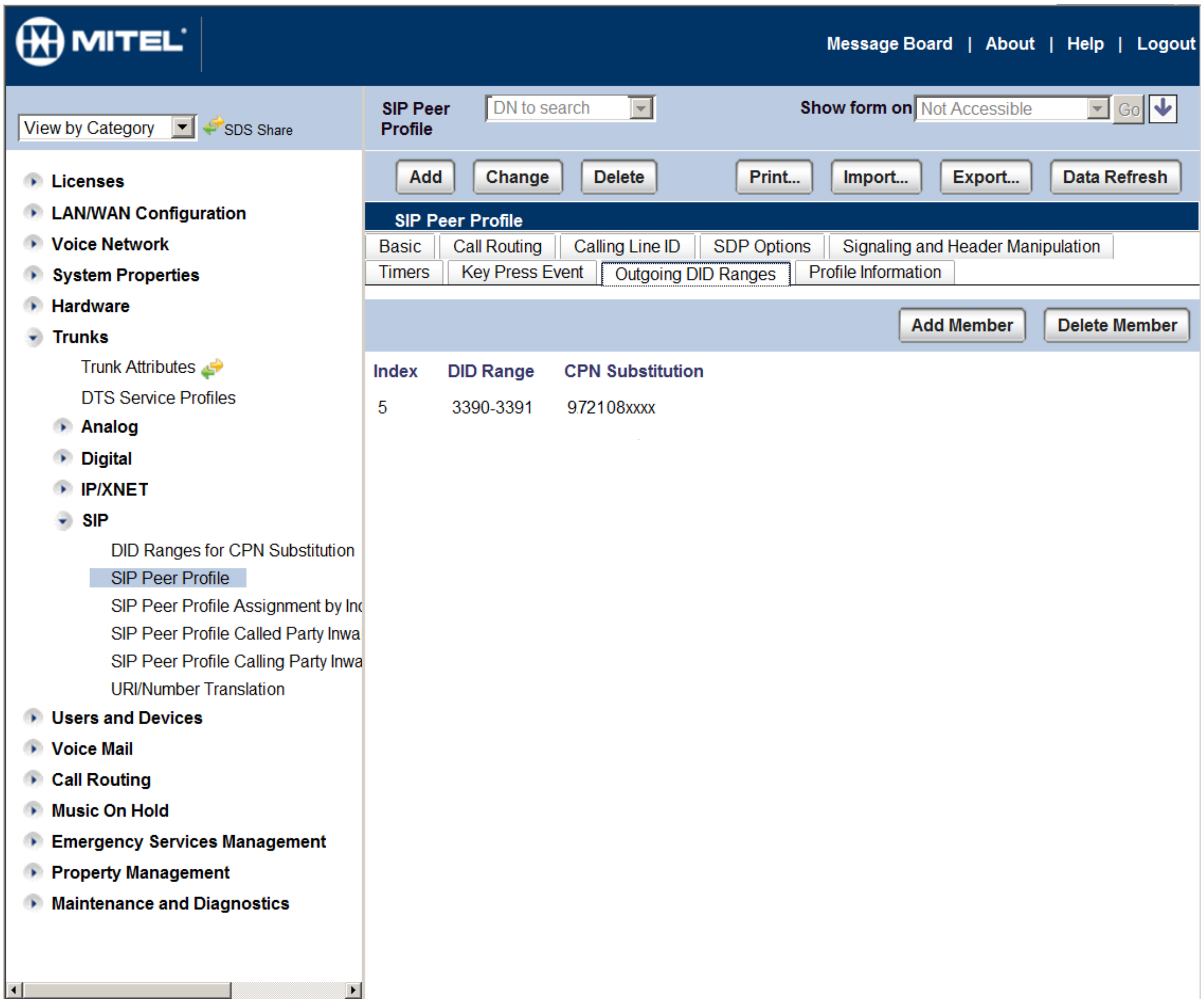
5.3.5. SIP Peer Profile

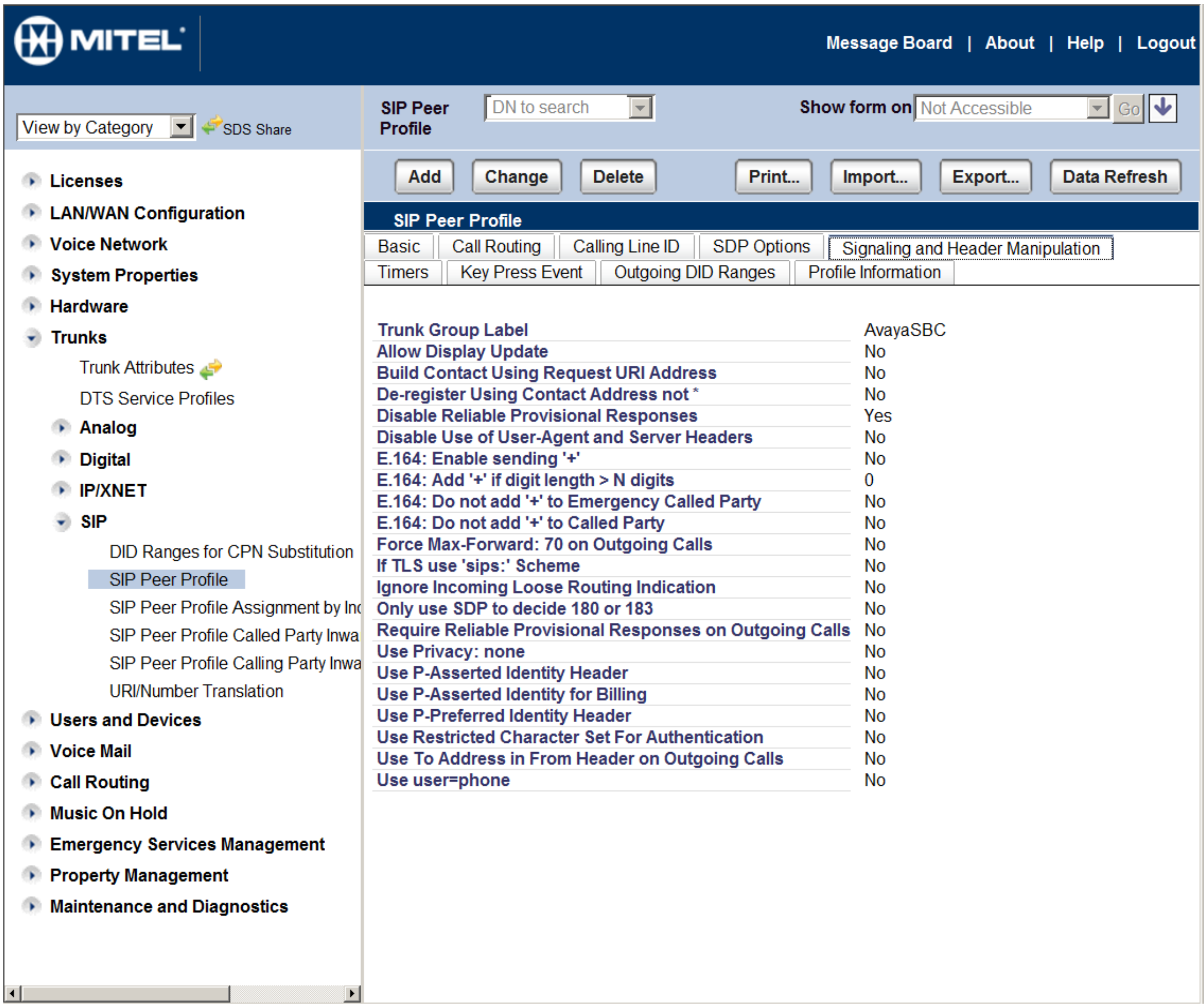
1. Navigate to **Trunks** > **SIP** > **SIP Peer Profile.**
2. Right click on the Trunk Service number and click **Add**.


MITEL
Message Board | About | Help | Logout
View by Category
SDS Share
SIP Peer Profile
DN to search
Show form on
Not Accessible
Go
Add
Change
Delete
Print...
Import...
Export...
Data Refresh
Licenses
LAN/WAN Configuration
Voice Network
System Properties
Hardware
Trunks
Trunk Attributes
DTS Service Profiles
Analog
Digital
IP/XNET
SIP
DID Ranges for CPN Substitution
SIP Peer Profile
SIP Peer Profile Assignment by Inc
SIP Peer Profile Called Party Inwa
SIP Peer Profile Calling Party Inwa
URI/Number Translation
Users and Devices
Voice Mail
Call Routing
Music On Hold
Emergency Services Management
Property Management
Maintenance and Diagnostics
SIP Peer Profile
Network Element
SIP Peer Profile Label
Outbound Proxy Server
CPN Restriction
Trunk Service
Session Timer
Zone
AvayaSBC
AvayaSBC
No
1
90
1
Basic
Call Routing
Calling Line ID
SDP Options
Signaling and Header Manipulation
Timers
Key Press Event
Outgoing DID Ranges
Profile Information
SIP Peer Profile Label
AvayaSBC
Network Element
AvayaSBC
Local Account Information
Registration User Name
Address Type
IP Address: 10.35.31.85
Administration Options
Interconnect Restriction
1
Maximum Simultaneous Calls
3
Outbound Proxy Server
SMDR Tag
0
Trunk Service
1
Zone
1


MITEL
Message Board | About | Help | Logout
View by Category
SDS Share
SIP Peer Profile
DN to search
Show form on
Not Accessible
Go
Add
Change
Delete
Print...
Import...
Export...
Data Refresh
Licenses
LAN/WAN Configuration
Voice Network
System Properties
Hardware
Trunks
Trunk Attributes
DTS Service Profiles
Analog
Digital
IP/XNET
SIP
DID Ranges for CPN Substitution
SIP Peer Profile
SIP Peer Profile Assignment by Inc
SIP Peer Profile Called Party Inwa
SIP Peer Profile Calling Party Inwa
URI/Number Translation
Users and Devices
Voice Mail
Call Routing
Music On Hold
Emergency Services Management
Property Management
Maintenance and Diagnostics
SIP Peer Profile
Basic
Call Routing
Calling Line ID
SDP Options
Signaling and Header Manipulation
Timers
Key Press Event
Outgoing DID Ranges
Profile Information
SIP Peer Profile Label AvayaSBC
Network Element AvayaSBC
Local Account Information
Registration User Name
Address Type IP Address: 10.35.31.85
Administration Options
Interconnect Restriction 1
Maximum Simultaneous Calls 3
Outbound Proxy Server
SMDR Tag 0
Trunk Service 1
Zone 1
Authentication Options
User Name
Password *******
Confirm Password *******
Authentication Option for Incoming Calls No Authentication
Subscription User Name
Subscription Password *******
Subscription Confirm Password *******

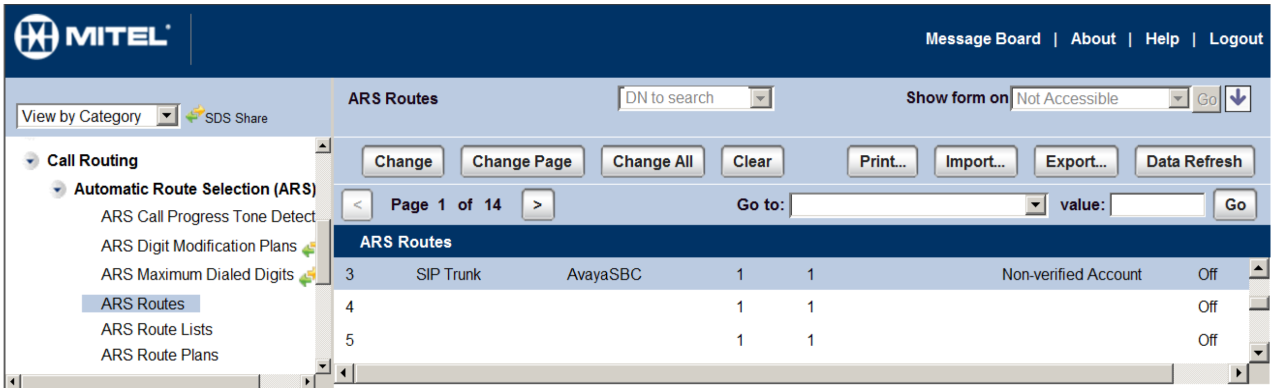

MITEL
Message Board | About | Help | Logout
View by Category
SDS Share
SIP Peer Profile
DN to search
Show form on
Not Accessible
Go
Add
Change
Delete
Print...
Import...
Export...
Data Refresh
Licenses
LAN/WAN Configuration
Voice Network
System Properties
Hardware
Trunks
Trunk Attributes
DTS Service Profiles
Analog
Digital
IP/XNET
SIP
DID Ranges for CPN Substitution
SIP Peer Profile
SIP Peer Profile Assignment by Inc
SIP Peer Profile Called Party Inwa
SIP Peer Profile Calling Party Inwa
URI/Number Translation
Users and Devices
Voice Mail
Call Routing
Music On Hold
Emergency Services Management
Property Management
Maintenance and Diagnostics
SIP Peer Profile
Basic
Call Routing
Calling Line ID
SDP Options
Signaling and Header Manipulation
Timers
Key Press Event
Outgoing DID Ranges
Profile Information
Allow Peer To Use Multiple Active M-Lines No
Allow Using UPDATE For Early Media Renegotiation No
Avoid Signaling Hold to the Peer No
Enable Mitel Proprietary SDP No
Force sending SDP in initial Invite message Yes
Force sending SDP in initial Invite - Early Answer No
Limit to one Offer/Answer per INVITE No
NAT Keepalive No
Prevent the Use of IP Address 0.0.0.0 in SDP Messages Yes
Renegotiate SDP To Enforce Symmetric Codec No
Repeat SDP Answer If Duplicate Offer Is Received No
RTP Packetization Rate Override No
RTP Packetization Rate 20ms
Special handling of Offers in 2XX responses (INVITE) No
Suppress Use of SDP Inactive Media Streams Yes

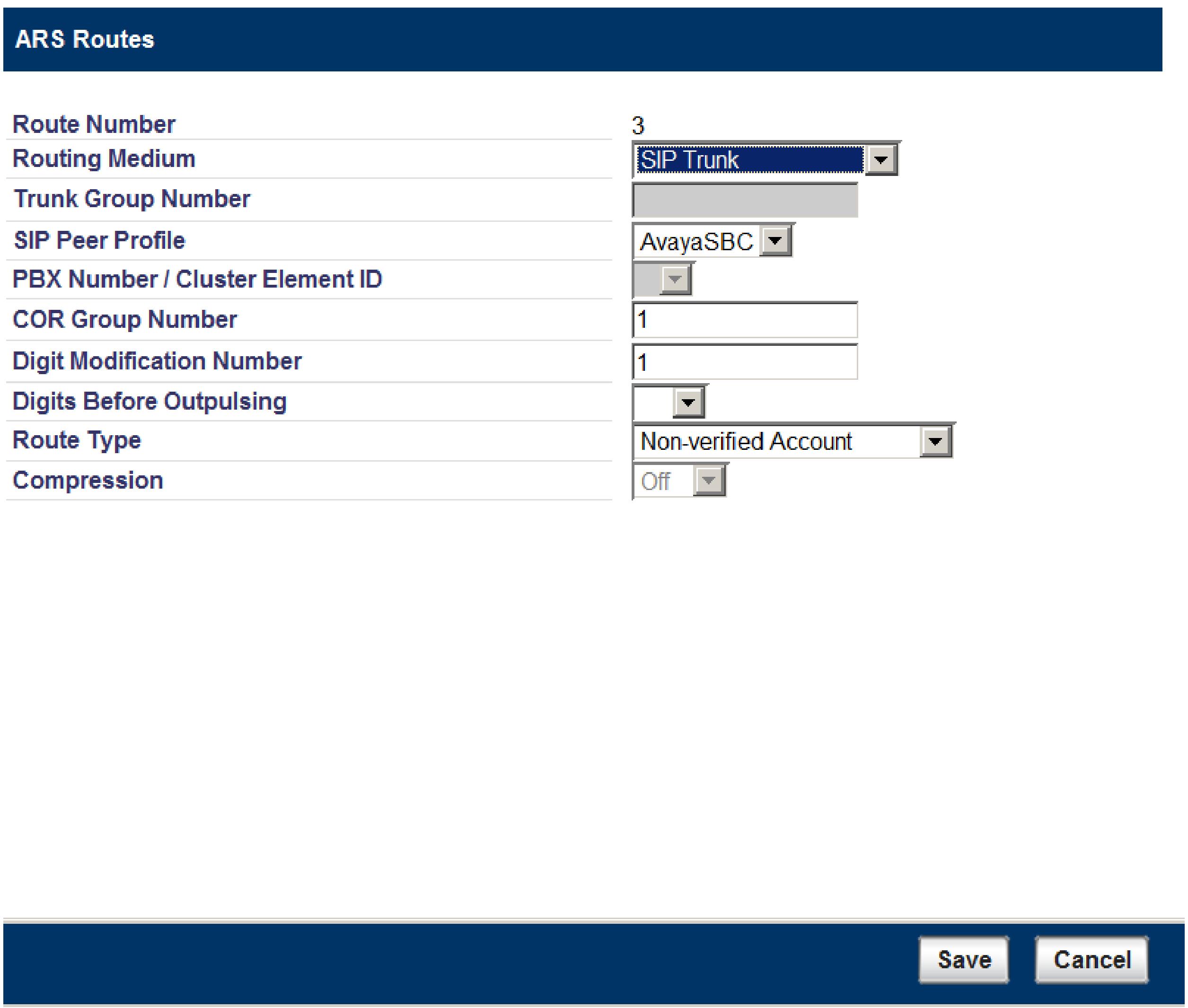

MITEL
Message Board | About | Help | Logout
View by Category
SDS Share
SIP Peer Profile
DN to search
Show form on
Not Accessible
Go
Add
Change
Delete
Print...
Import...
Export...
Data Refresh
Licenses
LAN/WAN Configuration
Voice Network
System Properties
Hardware
Trunks
Trunk Attributes
DTS Service Profiles
Analog
Digital
IP/XNET
SIP
DID Ranges for CPN Substitution
SIP Peer Profile
SIP Peer Profile Assignment by Inc
SIP Peer Profile Called Party Inwa
SIP Peer Profile Calling Party Inwa
URI/Number Translation
Users and Devices
Voice Mail
Call Routing
Music On Hold
Emergency Services Management
Property Management
Maintenance and Diagnostics
SIP Peer Profile
Basic
Call Routing
Calling Line ID
SDP Options
Signaling and Header Manipulation
Timers
Key Press Event
Outgoing DID Ranges
Profile Information
Add Member
Delete Member
Index
DID Range
CPN Substitution
5
3390-3391
972108xxxx



5.3.1. Call Routing

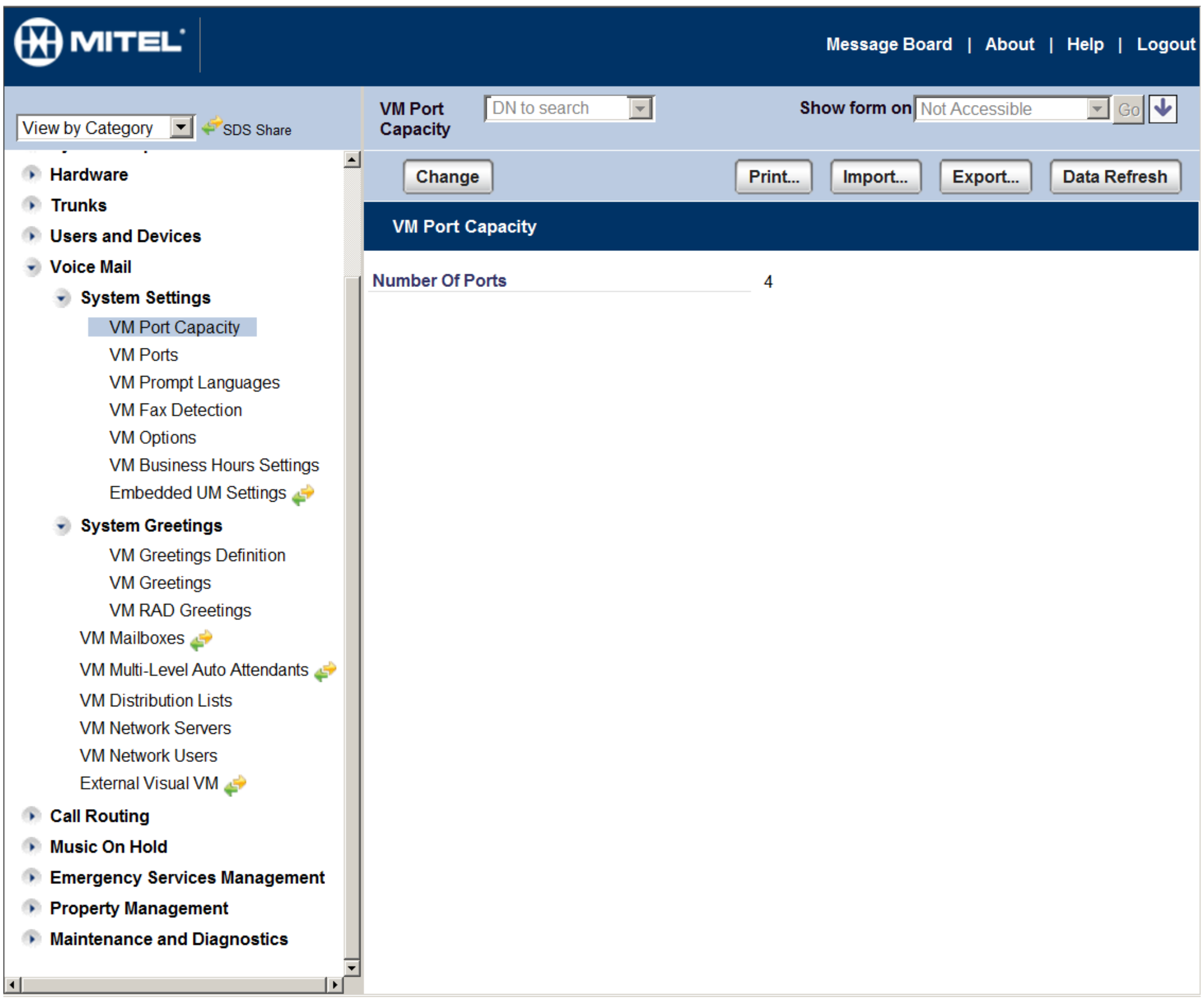
1. Navigate to **Call Routing > Automatic Route Selection (ARS) > ARS Routes.**


MITEL
Message Board | About | Help | Logout
View by Category
SDS Share
ARS Routes
DN to search
Show form on Not Accessible
Go
Call Routing
Automatic Route Selection (ARS)
ARS Call Progress Tone Detect
ARS Digit Modification Plans
ARS Maximum Dialed Digits
ARS Routes
ARS Route Lists
ARS Route Plans
Change
Change Page
Change All
Clear
Print...
Import...
Export...
Data Refresh
Page 1 of 14
Go to:
value:
Go
ARS Routes
3 SIP Trunk AvayaSBC 1 1 Non-verified Account Off
4 1 1 Off
5 1 1 Off


ARS Routes
Route Number
3
Routing Medium
SIP Trunk
Trunk Group Number
SIP Peer Profile
AvayaSBC
PBX Number / Cluster Element ID
COR Group Number
1
Digit Modification Number
1
Digits Before Outpulsing
Route Type
Non-verified Account
Compression
Off
Save
Cancel

5.3.2. Voicemail

To view or change voicemail settings, select the **Voice Mail** menu as shown in the following screen. Consult reference [2] for more information on the topics in this section.



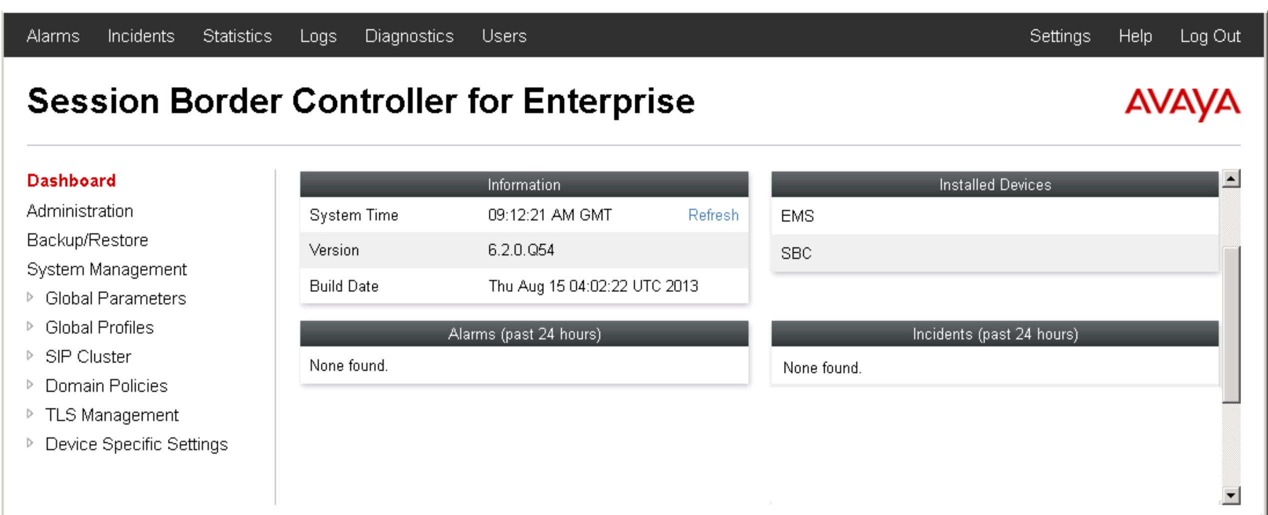
6. Configure Avaya Session Border Controller for Enterprise

This section covers the configuration of the Avaya SBCE. It is assumed that the Avaya SBCE software has already been installed. Also, it is assumed the management configuration, licensing and initial commissioning of the SBC has already been done

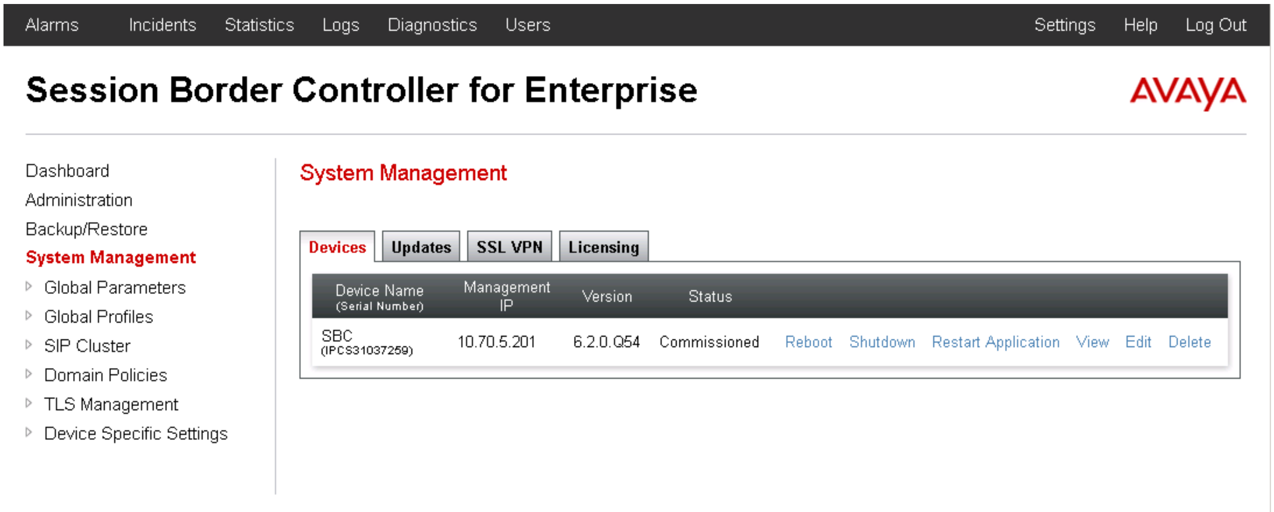
Use a WEB browser to access the Element Management Server (EMS) web interface, and enter https://<ip-addr>/sbc in the address field of the web browser, where <ip-addr> is the management LAN IP address of the Avaya SBCE.

Enter appropriate credentials and click **Log In**.

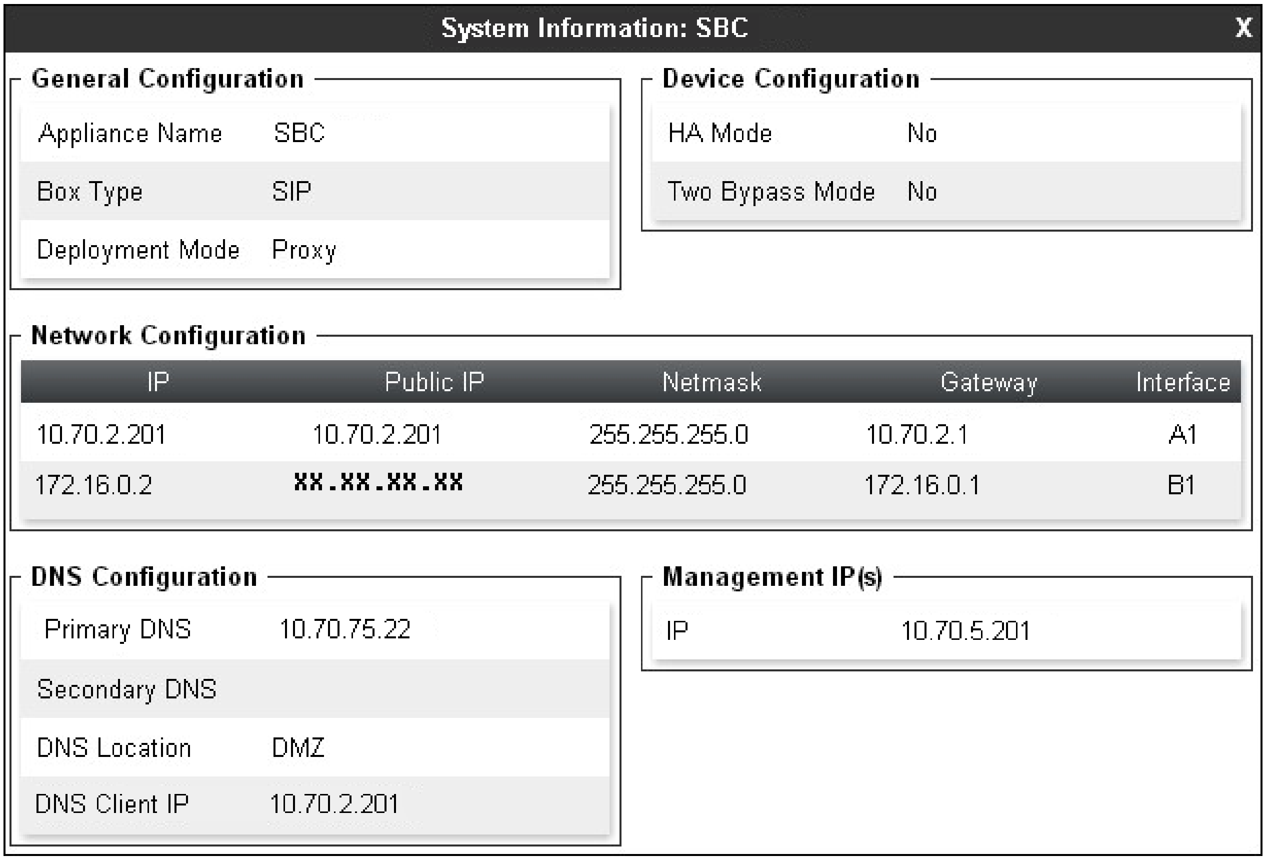
The Dashboard for the Avaya SBCE will appear.



To view system information that was configured during installation, click on **System Management**. A list of installed devices is shown in the right pane. In the case of the sample configuration, a single device named **SBC** is shown. To view the configuration of this device, click **View** as highlighted below.



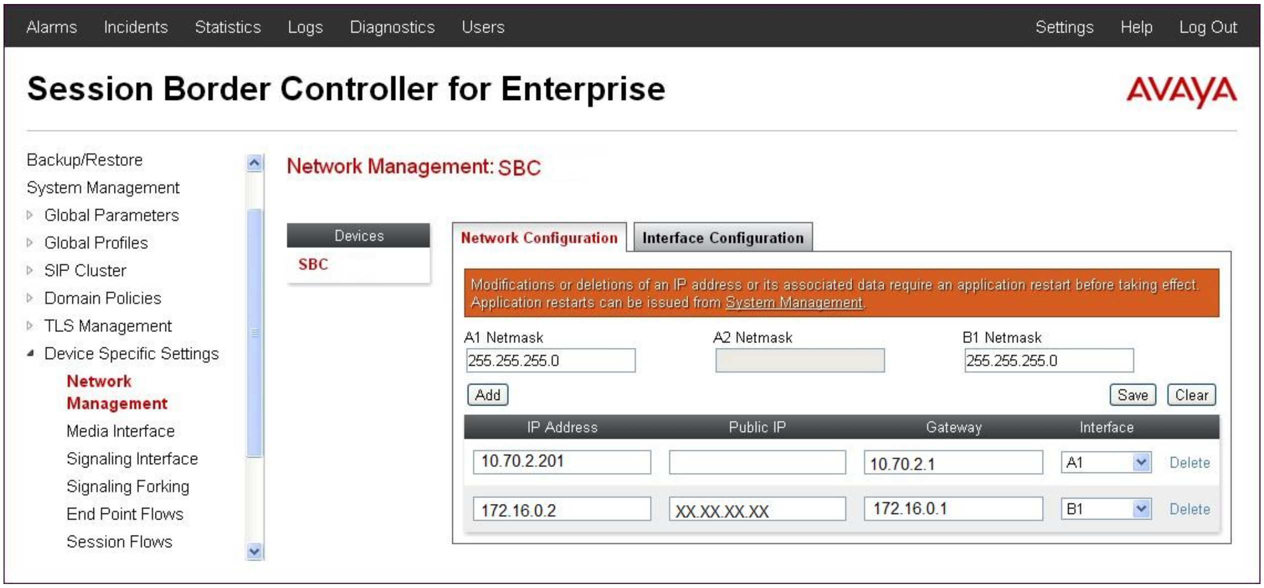
The **System Information** screen shows the **Network Configuration**, **DNS Configuration** and **Management IP(s)** information provided during installation and corresponds to **Figure 1**. IP address was given to include DNS. Default values were used for all other fields.



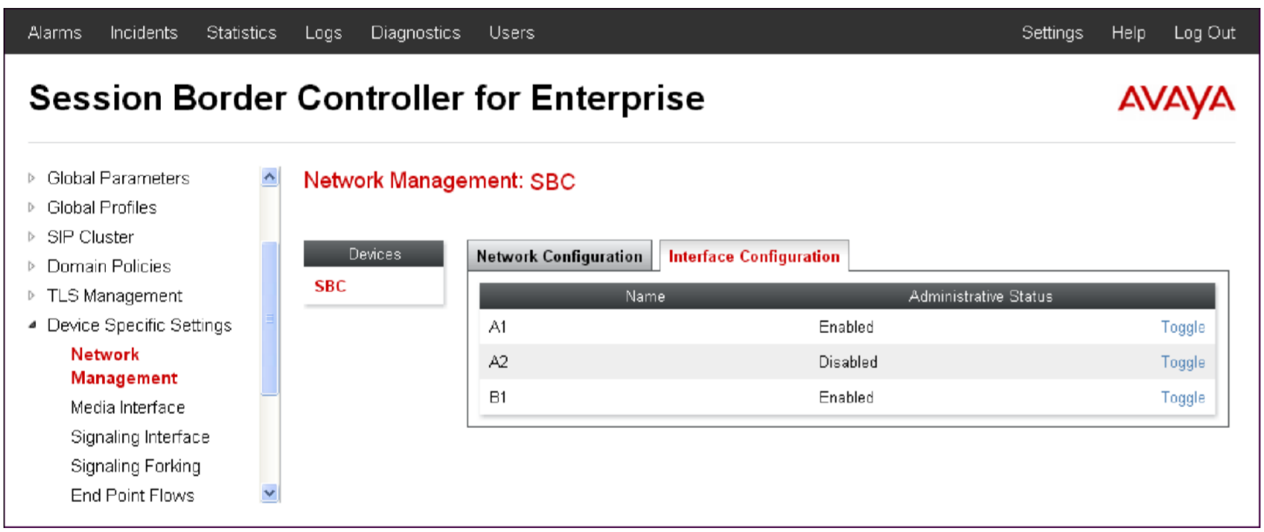
6.1. Network Management

The Network Management screen is where the network interface settings are configured and enabled. During the installation process of Avaya SBCE, certain network-specific information is defined such as device IP address(es), public IP address(es), netmask, gateway, etc. to interface the device to the network. It is this information that populates the various Network

Management tab displays, which can be edited as needed to optimize device performance and network efficiency. Navigate to **Device Specific Settings → Network Management** and verify the IP addresses assigned to the interfaces and that the interfaces are enabled. The following screen shows the enterprise interface is assigned to **A1** and the interface towards SIP Trunk provider is assigned to **B1**. The public interface is shown as XX.XX.XX.XX as an example. In a deployment, if the Firewall is Natting the SBC IP enter the Public IP field is used to put the Natted public IP of the SBC. If there is no NAT then that field is kept blank.



The following screen shows interface **A1** and **B1** are **Enabled**. To enable an interface click the corresponding **Toggle** button.

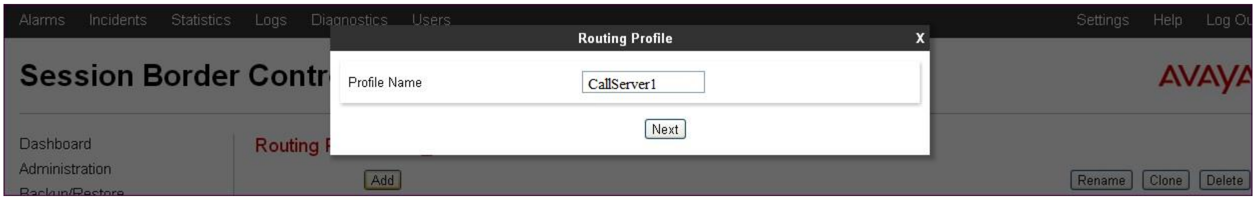


Note**: Screenshots are obtained with Portwell CAD version of ASBCE. Based on the platform used the number of interfaces will vary.**

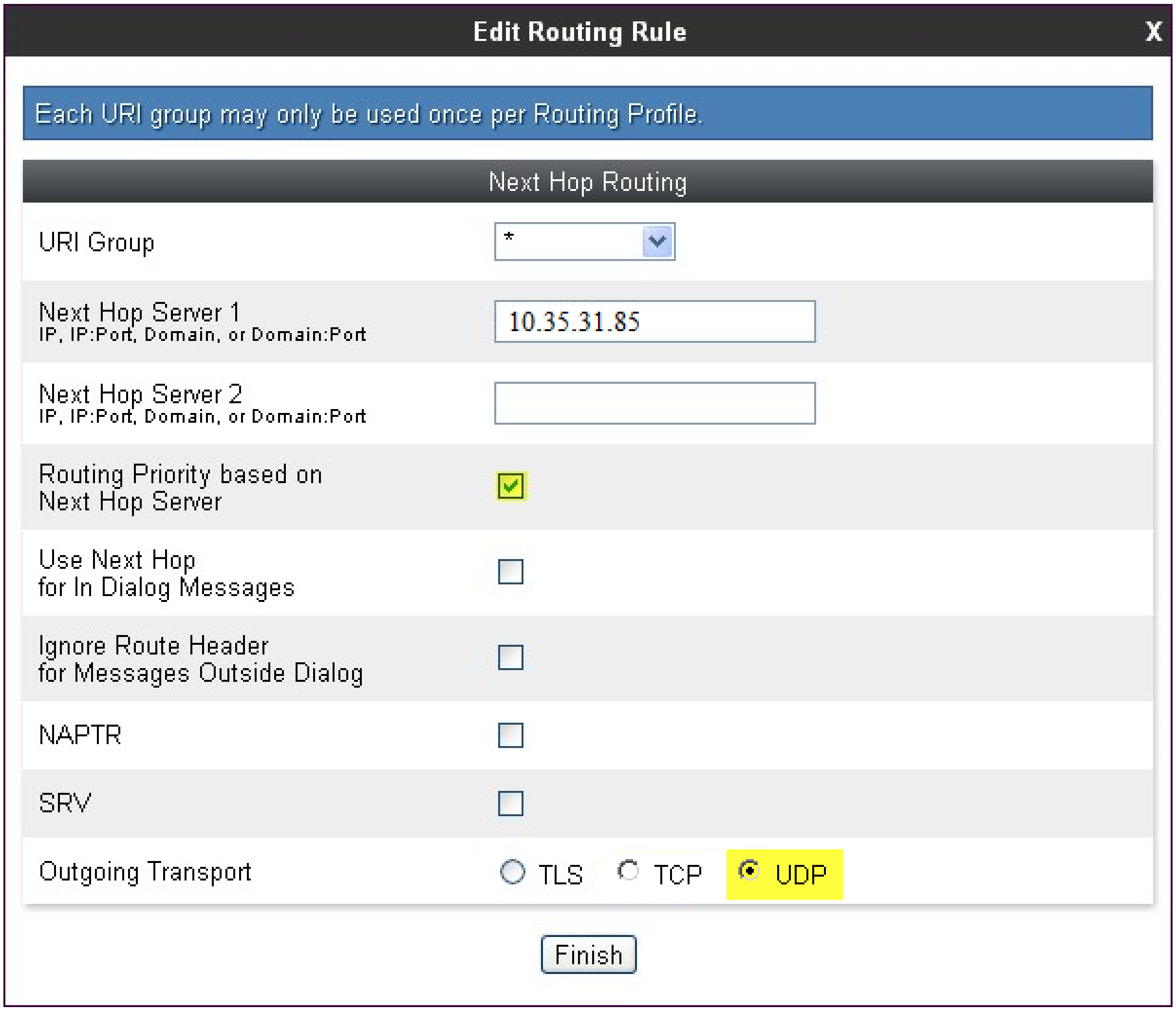
6.2. Routing Profile

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

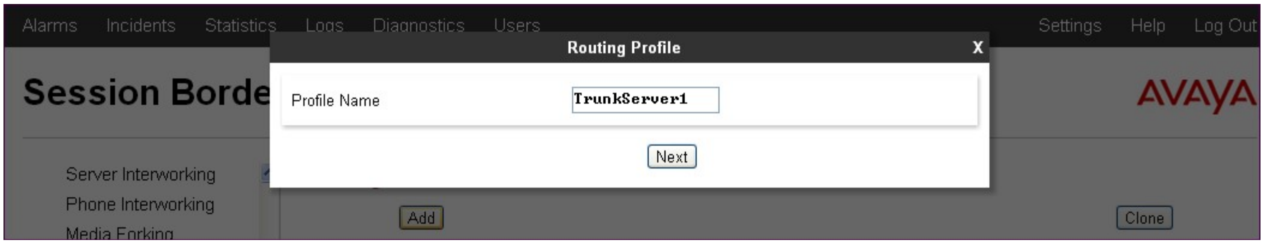
To add a routing profile for Mitel 3300, navigate to **Global Profiles → Routing** and select **Add** (not shown). Enter a **Profile Name** and click **Next** to continue.

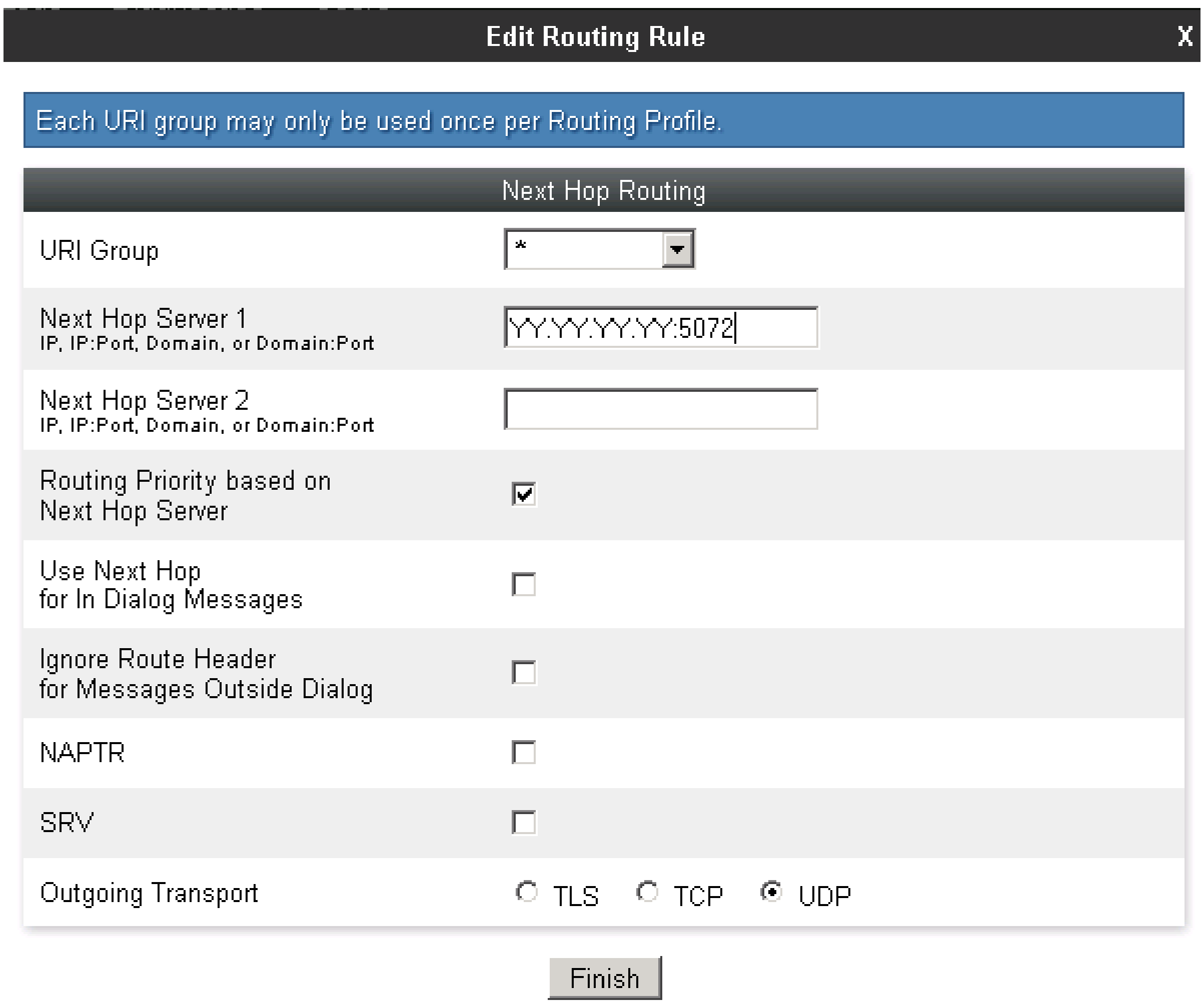


The following screen illustrates the Routing Profile named "CallServer1" created in the sample configuration for Mitel 3300. The **Next Hop Server 1** IP address must match the IP address of the Mitel 3300 LAN settings in Figure 1. Followed by a colon and the corresponding port settings in Figure 1. Port is only required if it is not the standard 5060 port. Leave the **Routing Priority based on Next Hop Server** box checked and select **TCP or UDP** for the **Outgoing Transport field.** In our example **UDP** was selected. When using a non-default port beside 5060 or 5061 the port must be included in the Next Hop Server configuration.


Edit Routing Rule
X
Each URI group may only be used once per Routing Profile.
Next Hop Routing
URI Group
*
Next Hop Server 1
IP, IP:Port, Domain, or Domain:Port
10.35.31.85
Next Hop Server 2
IP, IP:Port, Domain, or Domain:Port
Routing Priority based on Next Hop Server
Use Next Hop for In Dialog Messages
Ignore Route Header for Messages Outside Dialog
NAPTR
SRV
Outgoing Transport
TLS
TCP
UDP
Finish

A new routing profile named “TrunkServer1” was created for the SIP Trunk test service. The **Next Hop Server 1** IP address must match the IP address and port of the SIP Trunk test service in Figure 1. Leave the **Routing Priority based on Next Hop Server** box checked and select **UDP** or TCP for the **Outgoing Transport field. Current Example is shown with UDP**





6.3. Server Interworking Profile

The Server Internetworking profile is used for configuring and managing various SIP call server and deployment specific Interworking parameters such as RFC normalization, Session timers, URI Manipulation, Header Manipulation and Vendor/Deployment specific SIP Manipulations to interoperate between different servers. Interworking Profile features are configured based on different Servers. There are default profiles available that may be used, or new profiles can be configured as described below.

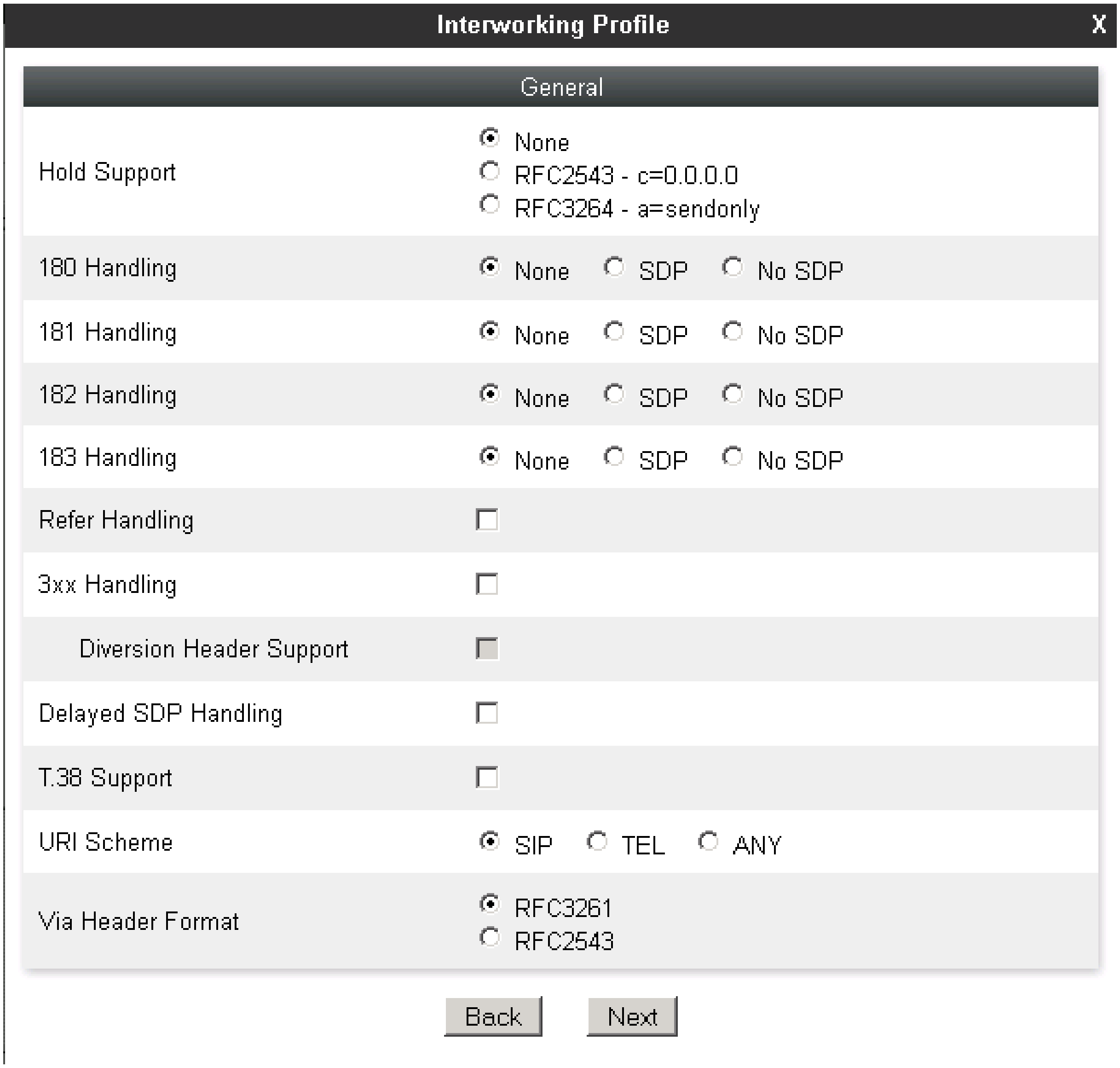
In the sample configuration, separate Server Interworking profiles were created for Mitel 3300 and SIP Trunk test service.

This is the description of Server Configuration.

6.3.1. Server Interworking Profile – Mitel 3300

In the sample configuration, the Mitel 3300 Server Interworking profile was created. To add a Server Interworking Profile for Mitel 3300, navigate to **Global Profiles → Server Interworking**, click the **Add** button. Enter a **Profile Name** and click **Next** to continue. In the example callserver1 was used.

Use default values for all fields and click **Next** to continue.

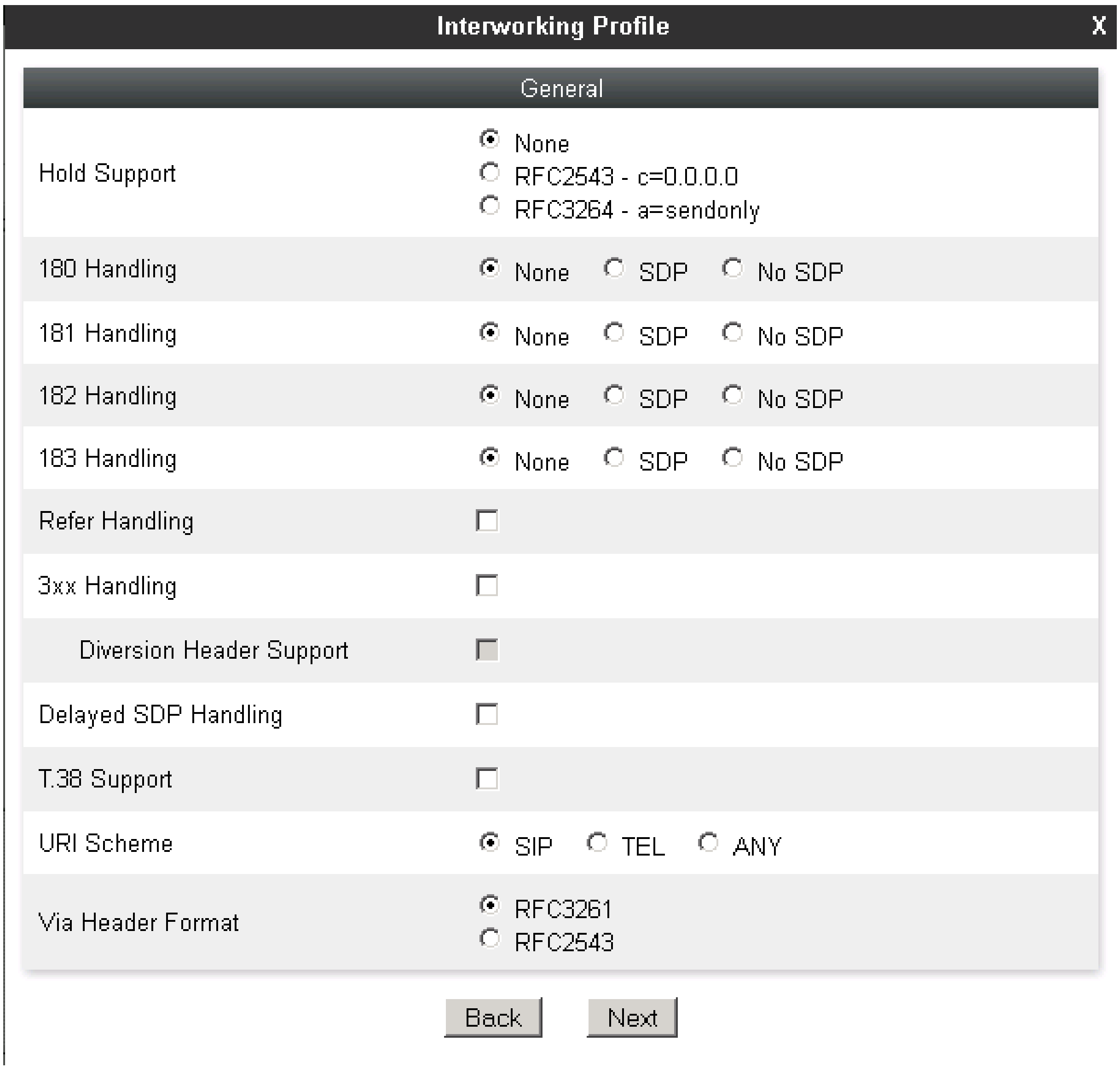


Default values can be used for the next windows that appear. Click **Next** to continue, then **Finish** to save the changes (not shown).

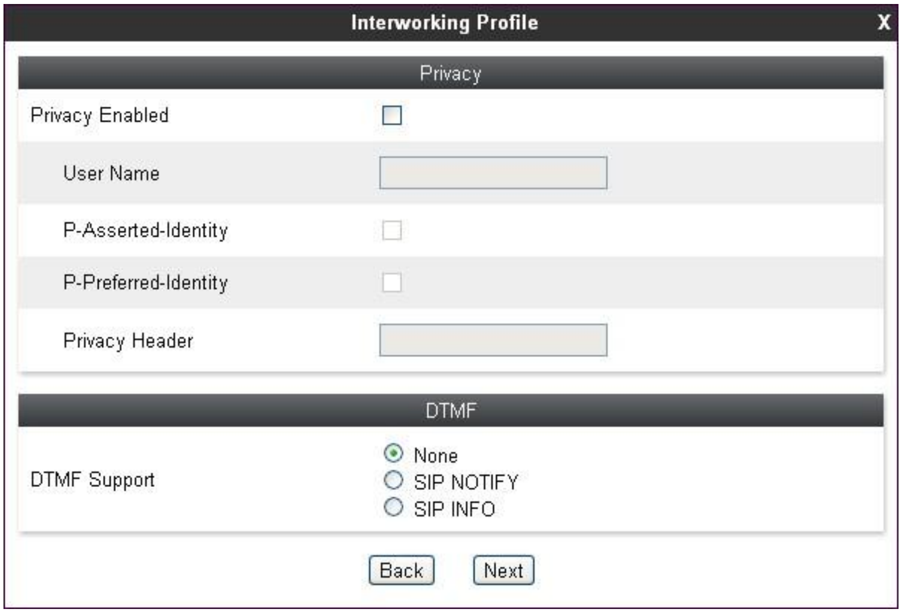
6.3.2. Server Interworking Profile – SIP Trunk Service

To create a new Server Interworking Profile for SIP Trunk service, navigate to **Global Profiles → Server Interworking** and click **Add** as shown below. Enter a **Profile Name** and click **Next**. In the example TrunkServer1 was used.

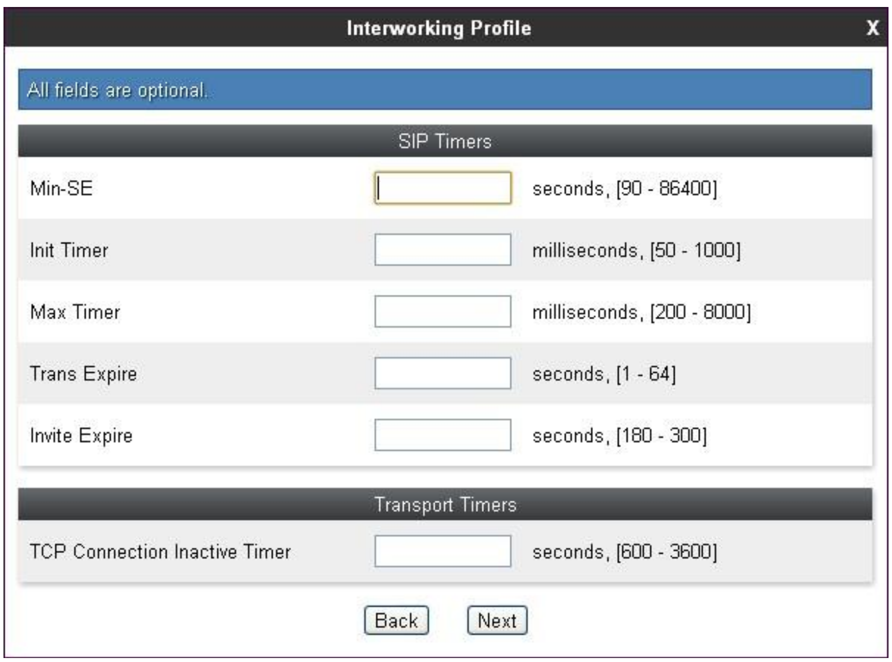
Use default values for all remaining fields. Click **Next** to continue.



Default values can be used for the **Privacy** and **DTMF** sections on the following screen. Click **Next** to continue.



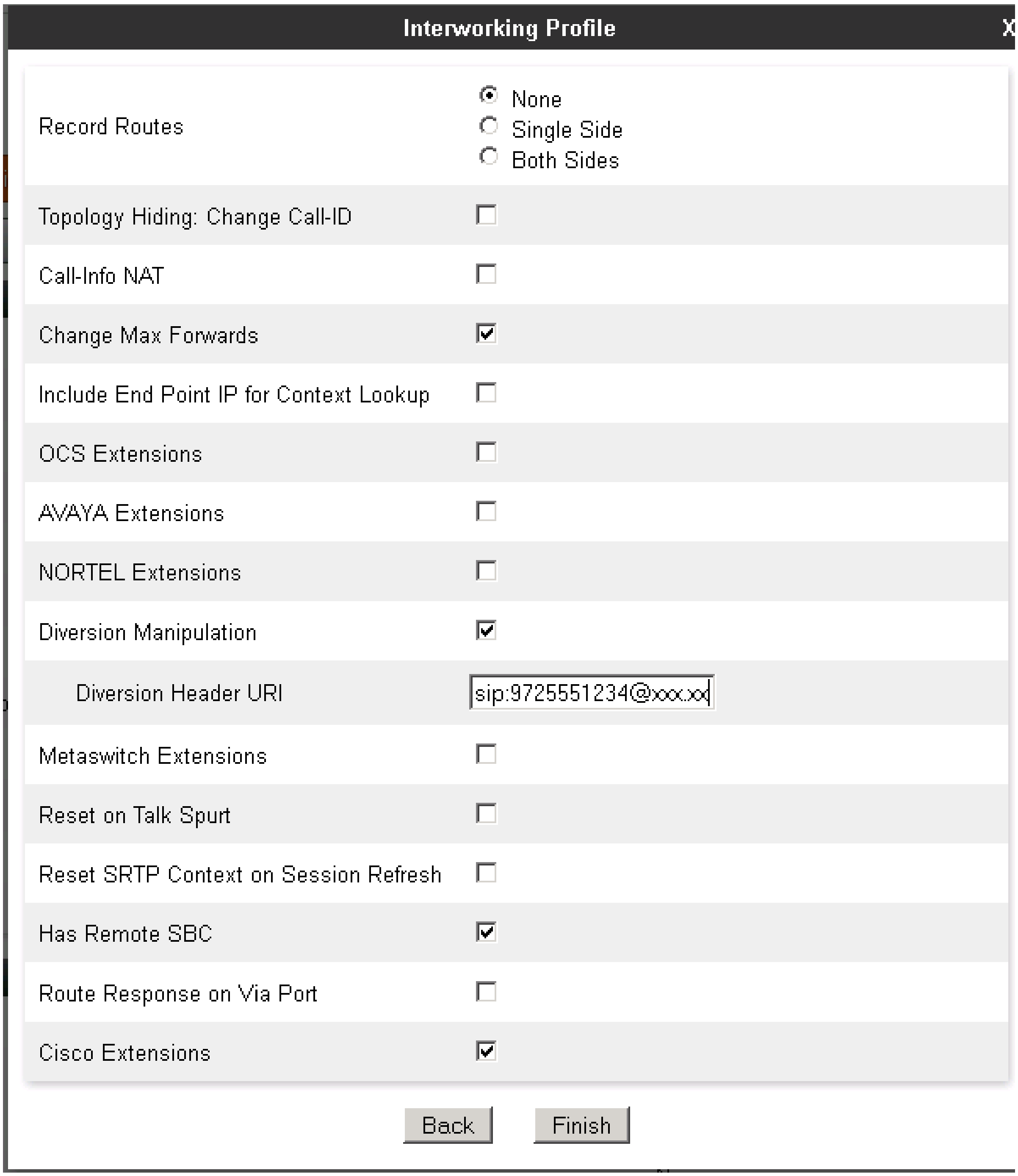
Default values can be used for the **SIP Timers** and **Transport Timers** sections on the following screen. Click **Next** to continue.



Select "None" for **Record Routes**. This is the setting that was used for testing. Check **Diversion Manipulation**. This setting is required for some call forward and transfer to PSTN scenarios. If this field is check all calls will include a DIVERSION header. If this is not desirable, it can be left uncheck. However, some call forward and transfer scenarios will not work which requires Diversion support. If the Diversion support is required, Enable the **Diversion Manipulation** field then enter the main number assigned to the company in the format sip:MainNumber@FirewallPublicIP. In our case the main number is 9728551234 and the

Firewall IP is represented by xx.xx.xx.xx. Use the Natted public IP of the SBC, Default values can be used for all remaining fields. Click **Finish** to save changes.

SIP Test trunk required to add a diversion header so this example shows how to add a Diversion header in the profile; by default this is not used unless Trunk provider requires it.



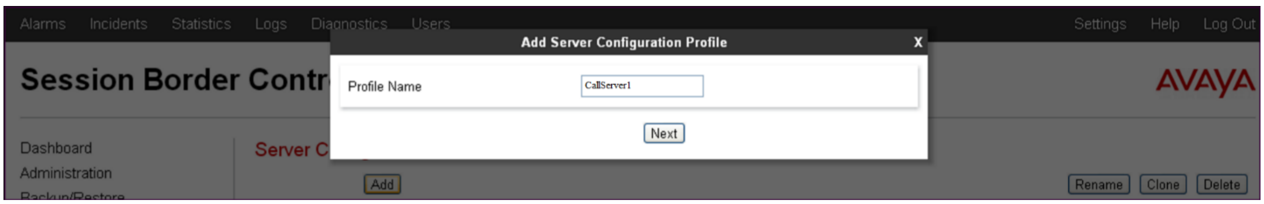
6.4. Server Configuration

The **Server Configuration** screen contains four tabs: **General**, **Authentication**, **Heartbeat**, and **Advanced**. Together, these tabs are used to configure and manage various SIP call server specific parameters such as UDP, TCP and TLS port assignments, heartbeat signaling parameters, Server DOS security feature configuration and linkage to appropriate Interworking, Signaling Manipulation profiles created for respective server.

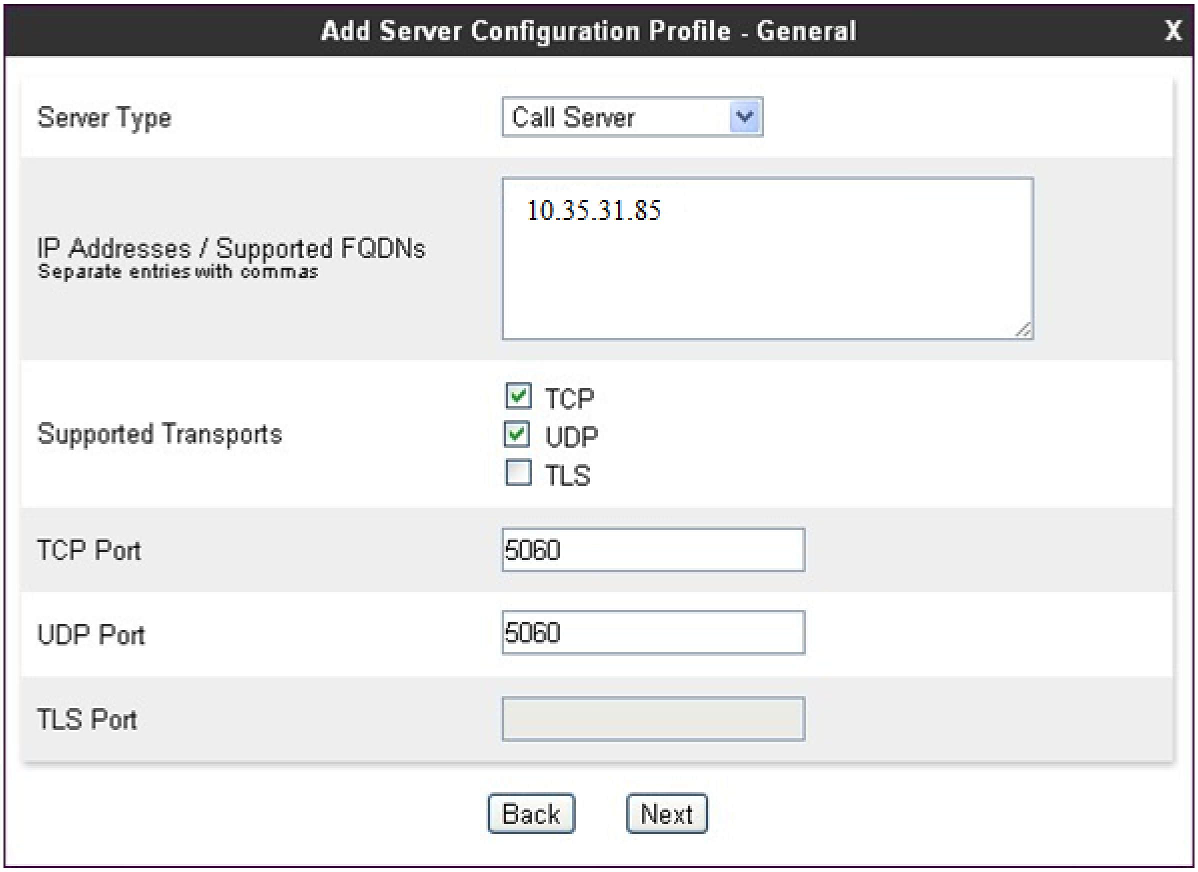
In the sample configuration, separate Server Configurations were created for Mitel 3300 and SIP Trunk test service.

6.4.1. Server Configuration – Mitel 3300

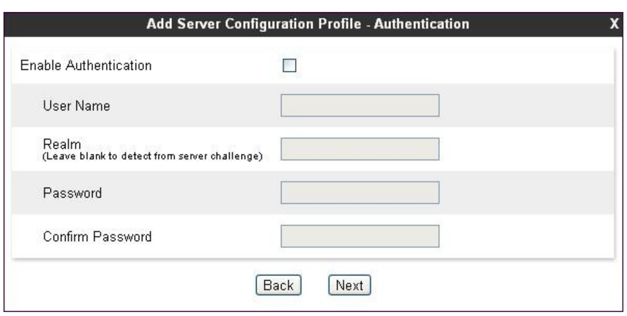
To add a Server Configuration Profile for Mitel 3300, navigate to **Global Profiles → Server Configuration** and click **Add** (not shown). Enter a descriptive name for the **Profile Name** and click **Next**.

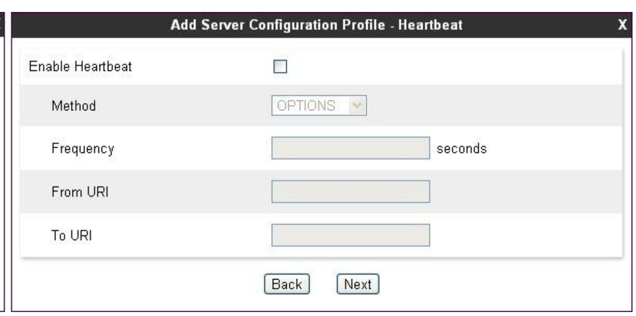


The following screens illustrate the Server Configuration for the Profile name "CallServer1". In the **General** parameters, select "Call Server" from the **Server Type** drop-down menu (not shown). In the **IP Addresses / Supported FQDNs** area, the IP Address of the Mitel 3300 interface in the sample configuration is entered. In the **Supported Transports** area, "UDP" and "TCP" is selected, and the **UDP Port** and **TCP port** is set to "5060". If adding a new profile, click **Next**. If editing an existing profile, click **Finish** (not shown).

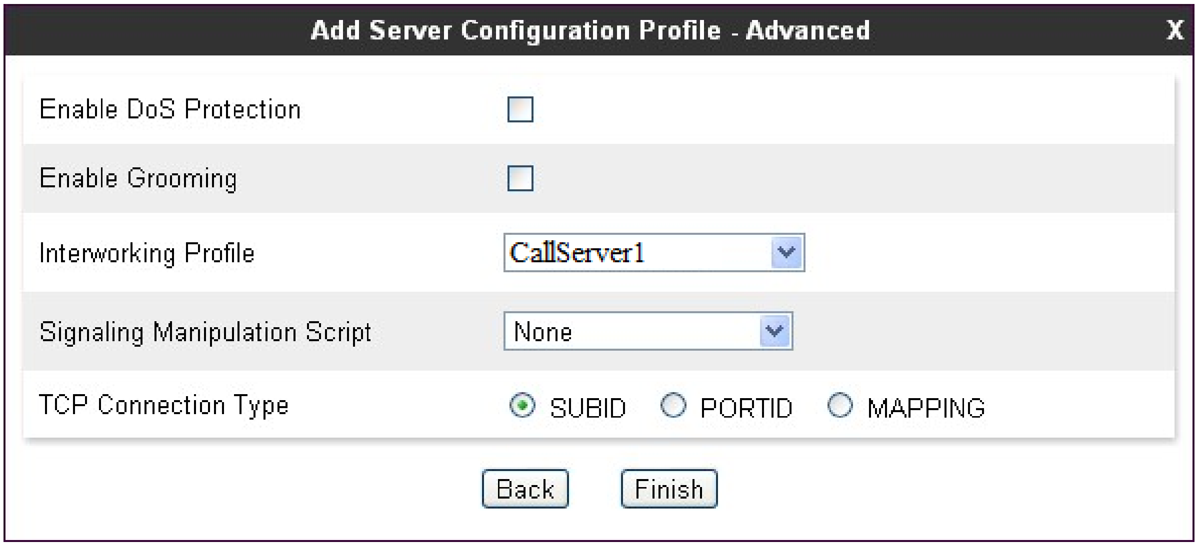


In the next two windows that appear, verify **Enable Authentication** and **Enable Heartbeat** are unchecked. Mitel 3300 does not require authentication and the Heartbeat feature is not necessary because Avaya SBCE will forward SIP OPTIONS from SIP Trunk test service to the Mitel 3300. Click **Next** to continue.





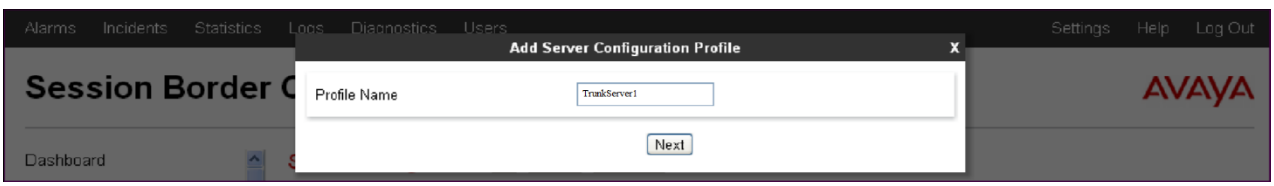
In the new window that appears, select the **Interworking Profile** created for Mitel 3300 in Section 6.3.1. Use default values for all remaining fields. Click **Finish** to save the configuration.



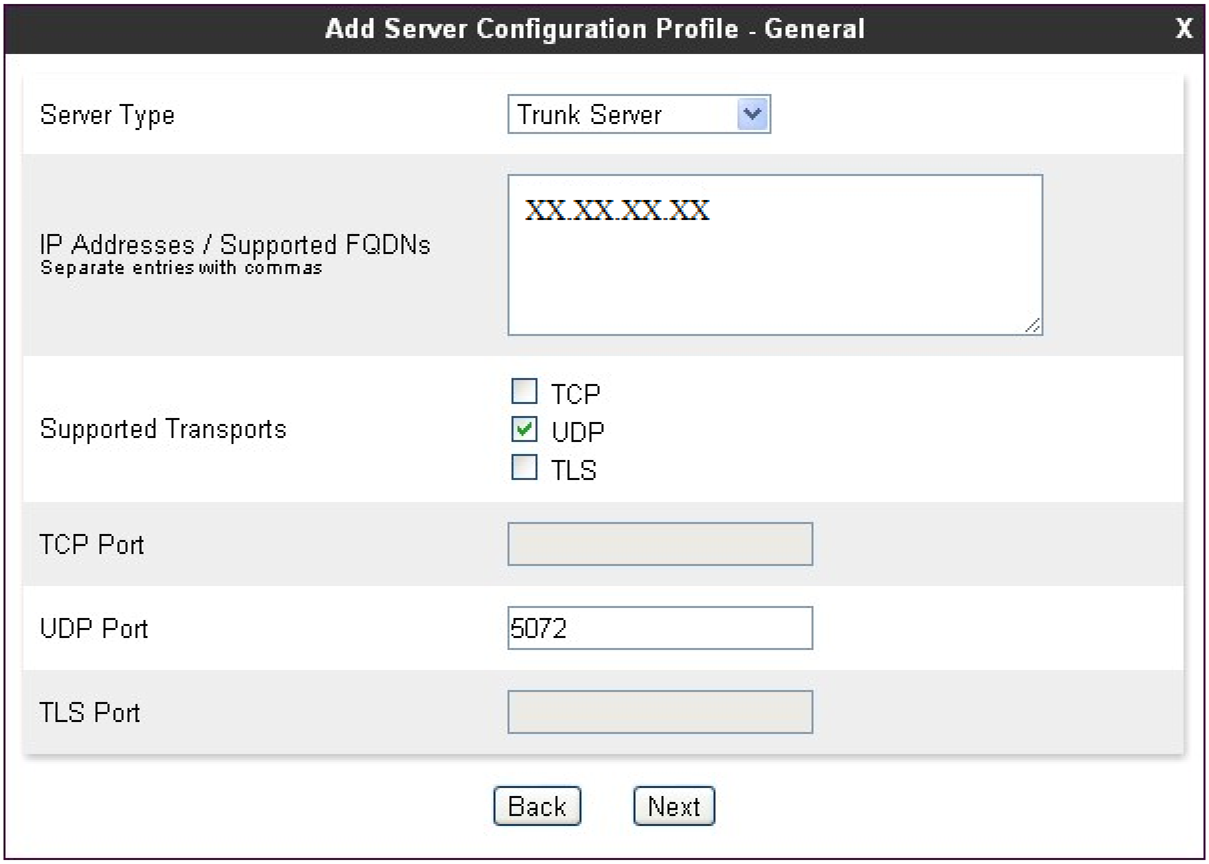
Note: If TCP was select as a protocol, then Selecting **Enable Grooming** is recommended.

6.4.2. Server Configuration – SIP Trunk Service

To add a Server Configuration Profile for SIP trunk service, navigate to **Global Profiles → Server Configuration** and click **Add**. Enter a descriptive name for the **Profile Name** and click **Next**.

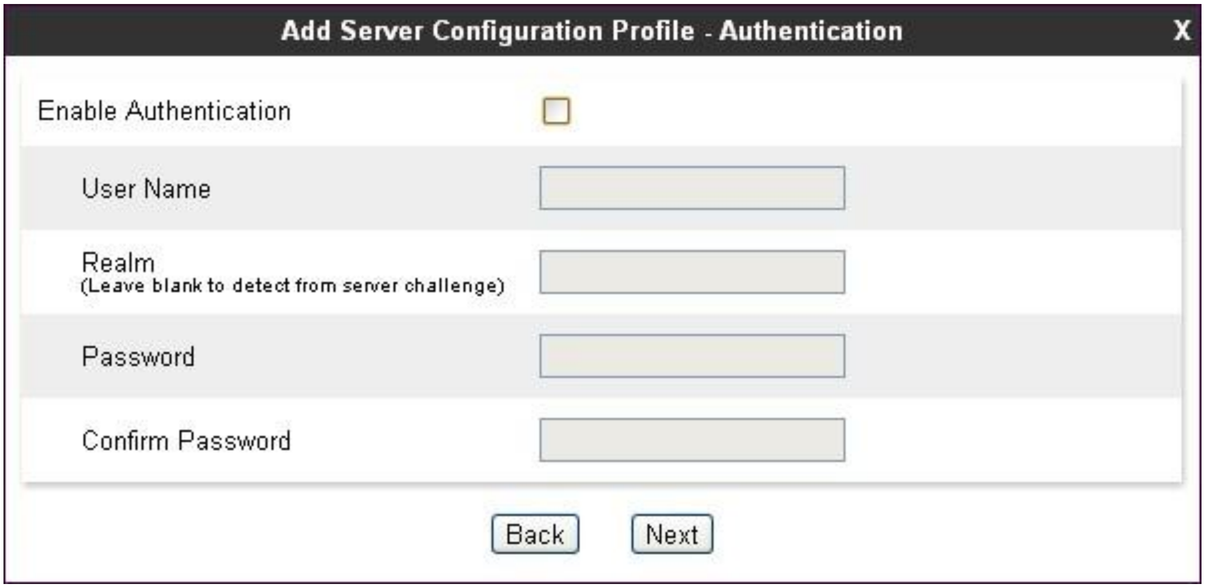


The following screens illustrate the Server Configuration for the Profile name "TrunkServer1". In the **General** parameters, select "Trunk Server" from the **Server Type** drop-down menu. In the **IP Addresses / Supported FQDNs** area, the SIP Trunk provider IP address is entered. In the sample configuration this is "XX.XX.XX.XX". In the **Supported Transports** area, UDP is selected, and the **UDP Port** is set to "5072". Click **Next** to continue. The actual values provided by SIP Trunk provider should be used.

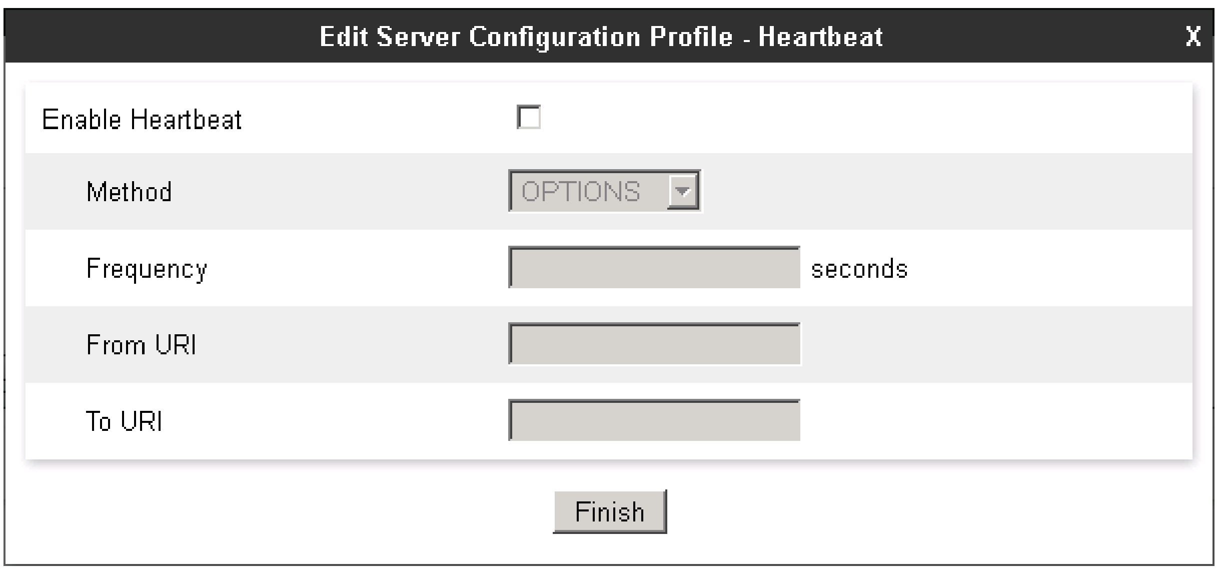


Note: The above configurations are as per the Server configuration profile in Avaya session border controller with SIP Test trunk Service with Transport and port number based on the provider. Above values shall be modified based on the field service provider and deployment requirements.

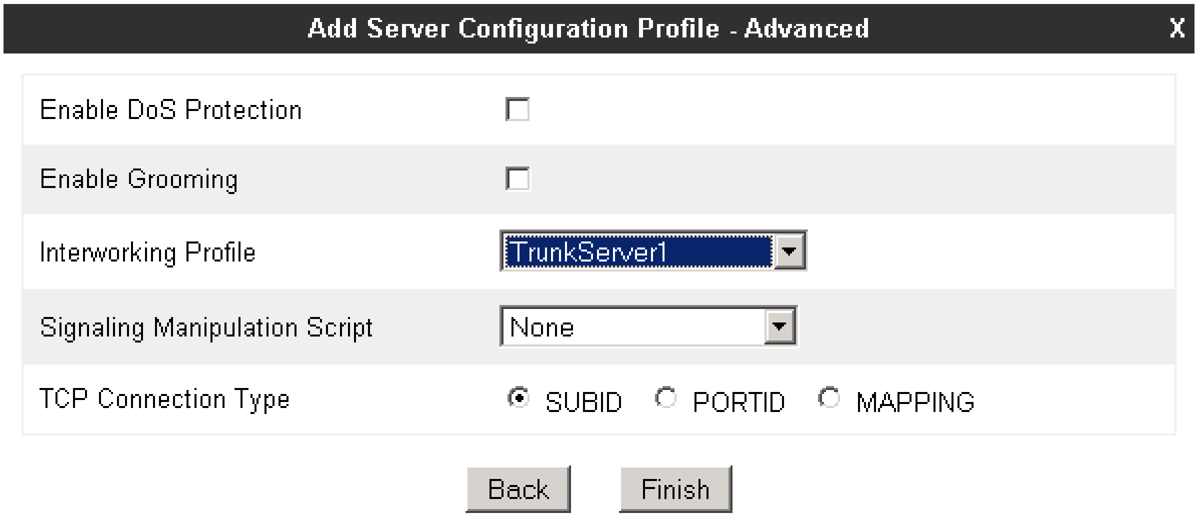
Verify **Enable Authentication** is unchecked as SIP Test trunk Service does not require authentication. Click **Next** to continue.



Click **Next** to continue.



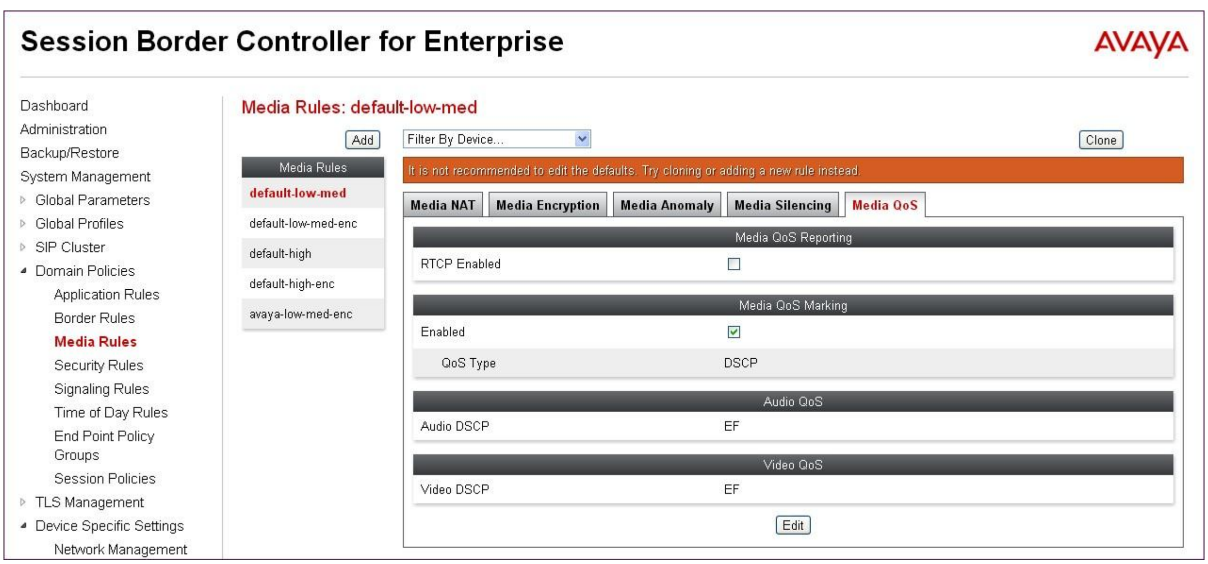
In the new window that appears, select the **Interworking Profile** “Trunkserver1” created previously in Section 6.3.2. Use default values for all remaining fields. Click **Finish** to save the configuration.



6.5. Media Rule

Media Rules define RTP media packet parameters such as prioritizing encryption techniques and packet encryption techniques. Together these media-related parameters define a strict profile that is associated with other SIP-specific policies to determine how media packets matching these criteria will be handled by the Avaya SBCE security product.

Select **Domain Policies → Media Rules** from the left-side menu as shown below. In the sample configuration, a single default media rule “default-low-med” was used with the **Audio and Video DSCP** values “EF” (**E**xpedited **F**orwarding) set for **Media QoS** as shown below.



Note: QOS Bit marking is not mandatory and can be disabled. If QOS Bit marking is required the above procedure can be used to achieve the requirement.

6.6. Signaling Rule

Signaling Rules define the action to be taken (Allow, Block, Block with Response, etc.) for each type of SIP-specific signaling request and response message. When SIP signaling packets are received by Avaya SBCE, they are parsed and "pattern-matched" against the particular signaling criteria defined by these rules. Packets matching the criteria defined by the Signaling Rules are tagged for further policy matching.

The "default" signaling rule can be used for SIP Trunk provider and Mitel 3300.

6.7. Application Rule

Application Rules define which types of SIP-based Unified Communications (UC) applications the Avaya SBCE security device will protect: voice, video, and/or Instant Messaging (IM). In addition, user can determine the maximum number of concurrent voice and video sessions the network will process in order to prevent resource exhaustion.

Select **Domain Policies → Application Rules** from the left-side menu as shown below. In the sample configuration, a single default application rule "default" was used. For field deployment create an application rule with the concurrent sessions purchased (not shown).

6.8. Endpoint Policy Groups

The rules created within the Domain Policy section are assigned to an Endpoint Policy Group. The Endpoint Policy Group is then applied to a Server Flow in Section 6.11.

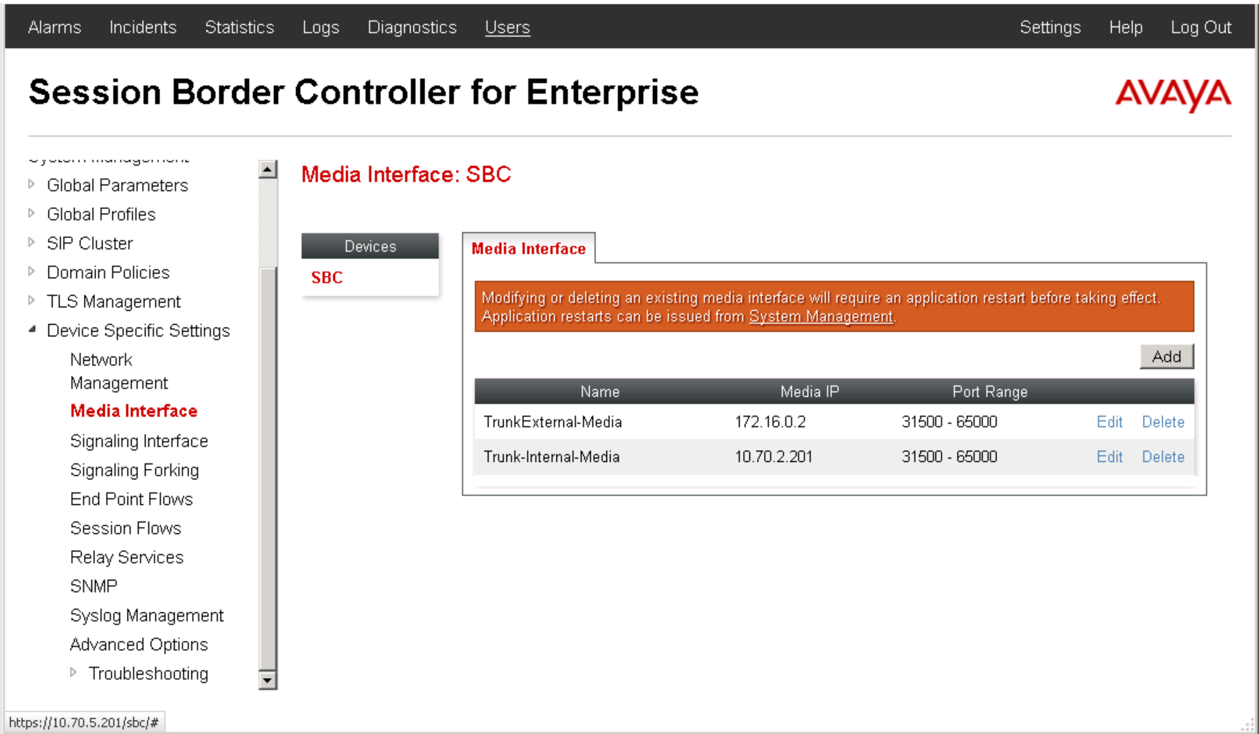
To create a new policy group, navigate to **Domain Policies → Endpoint Policy Groups** and click on **Add** (not shown)**.** The "default-low" predefined Endpoint Policy Group was used for both Mitel 3300 and SIP Trunk provider in section 6.11.

For field deployments create appropriate endpoint policy groups based on the domain policies created for Mitel and specific SIP trunk provider.

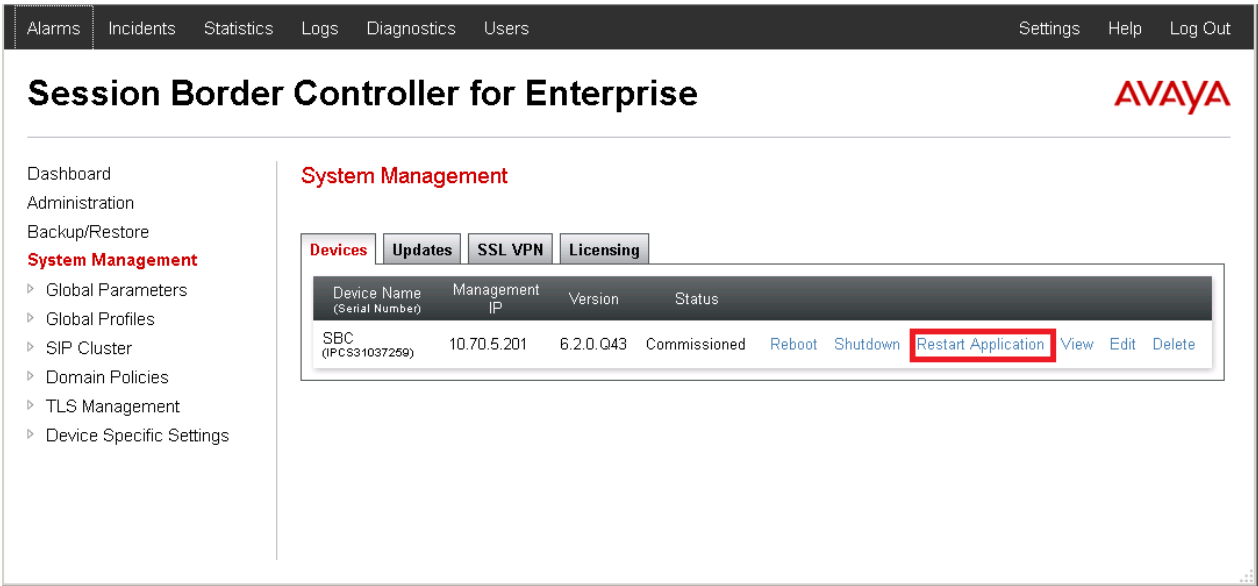
6.9. Media Interface

The Media Interface screen is where the SIP media ports are defined. Avaya SBCE will send SIP media on the defined ports. Create a SIP media interface for the inside and outside IP interfaces.

To create a new Media Interface, navigate to **Device Specific Settings → Media Interface** and click **Add**. The following screen shows the media interfaces defined for the sample configuration.



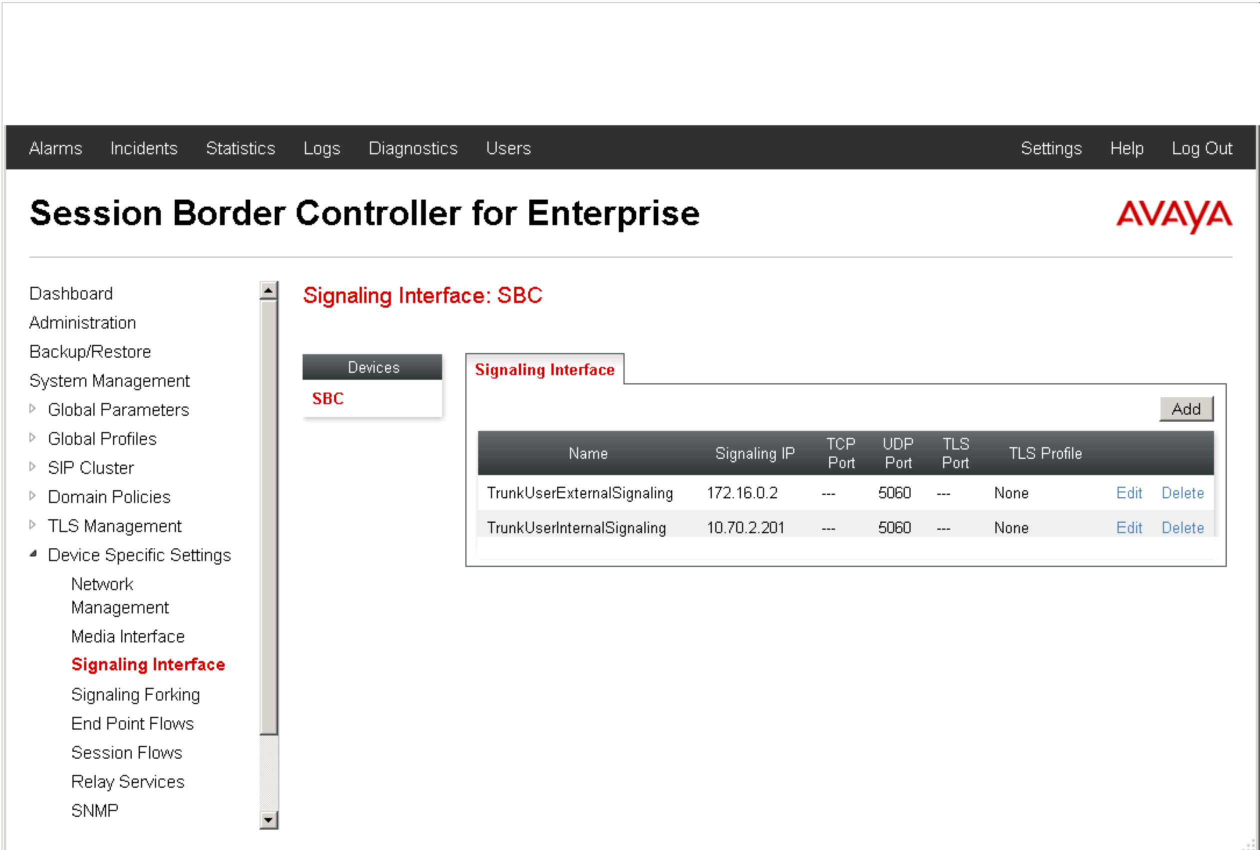
After the media interfaces are created, an application restart is necessary before the changes will take effect. Navigate to **System Management** and click **Restart Application** as highlighted below.



6.10. Signaling Interface

The Signaling Interface screen is where the SIP signaling ports are defined. Avaya SBCE will listen for SIP requests on the defined ports. Create a signaling interface for the inside and outside IP interfaces.

To create a new Signaling Interface, navigate to **Device Specific Settings → Signaling Interface** and click **Add**. The following screen shows the signaling interfaces defined for the sample configuration.



Note: TCP and/or UDP can be used for configuration as required for deployment.

6.11. Topology Hiding

Topology hiding allows to manipulate the Request-Line, FROM, TO, RECORD-ROUTE, VIA headers and SDP.

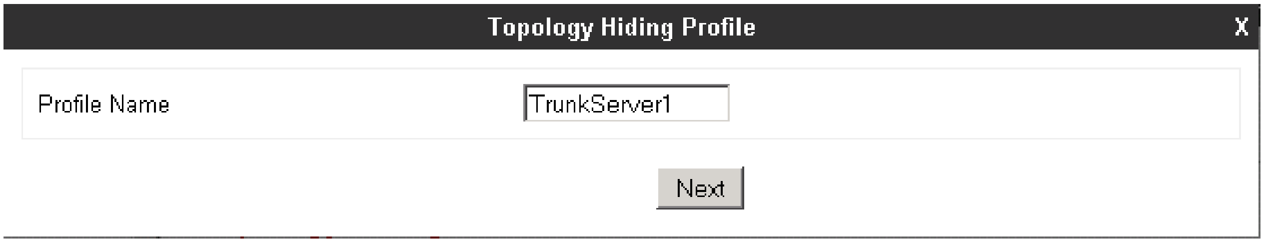
6.11.1. Topology Hiding – Mitel 3300

A topology profile is not necessary for Mitel. It is recommended to clone “default” and to use Auto if nothing specific is required

6.11.2. Topology Hiding - SIP Trunk Service

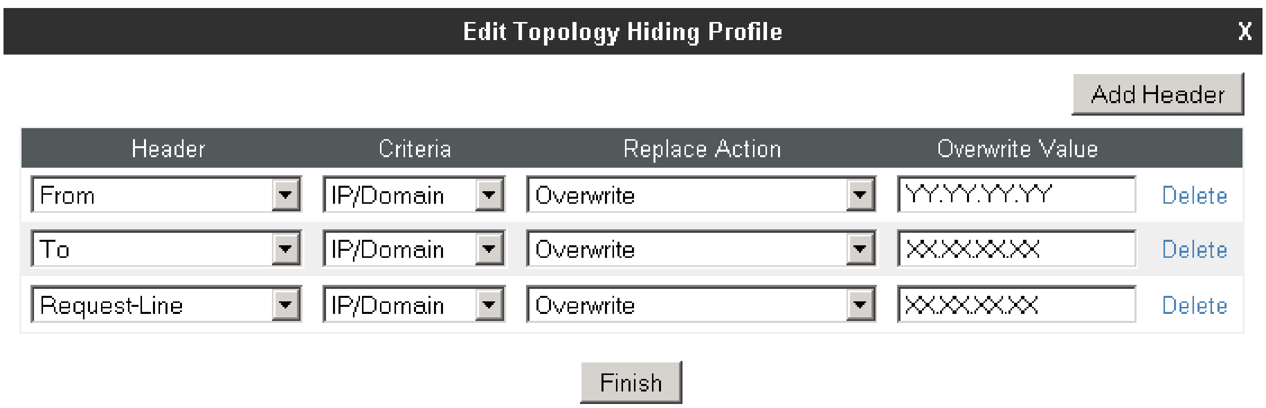
A topology profile is created to manipulate URI to match the Public NATted IP.

Go to **Global Profiles-> Topology hiding**. Click the **Add** button. Enter a profile name. Click the **Next** button.



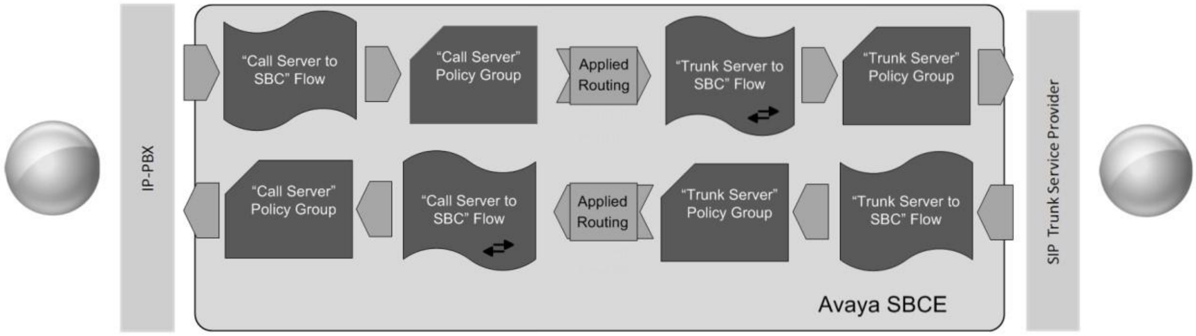
Make sure that the **Request-Line** and **TO** headers are added. Select Overwrite as the **Replace Action** for both headers. Enter the public IP of the Firewall **Overwrite Value**. Add the **FROM** header. Select Overwrite as the **Replace Action.** Enter the IP address of SIP trunk service. Click the **Finish** button. In our example the Public IP address is shown as XX.XX.XX.XX. Enter the NATted public IP of the SBC. Also, SIP Trunk service IP is represented by YY.YY.YY.YY. In here apply the IP address given by SIP Trunk Service.

This was used for test trunk and that in the field it is recommended to clone the default with all Auto unless SIP trunk provider wants something specific overwritten.

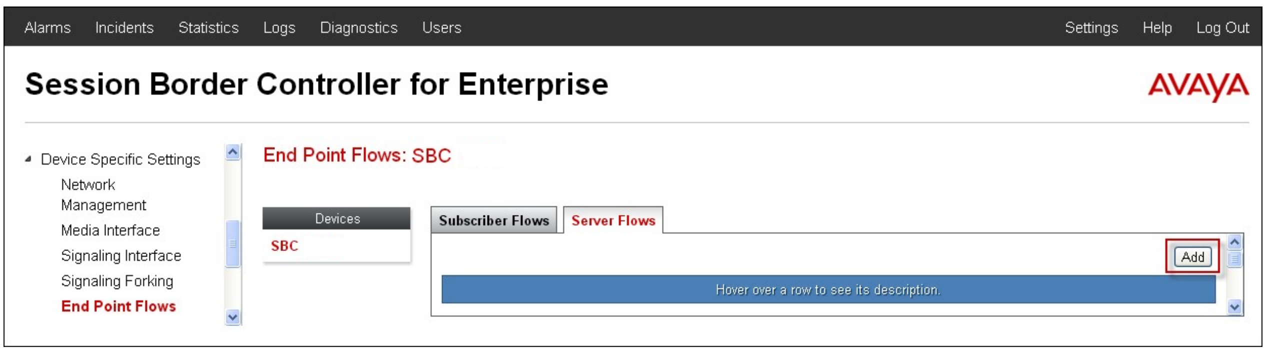


6.12. End Point Flows - Server Flow

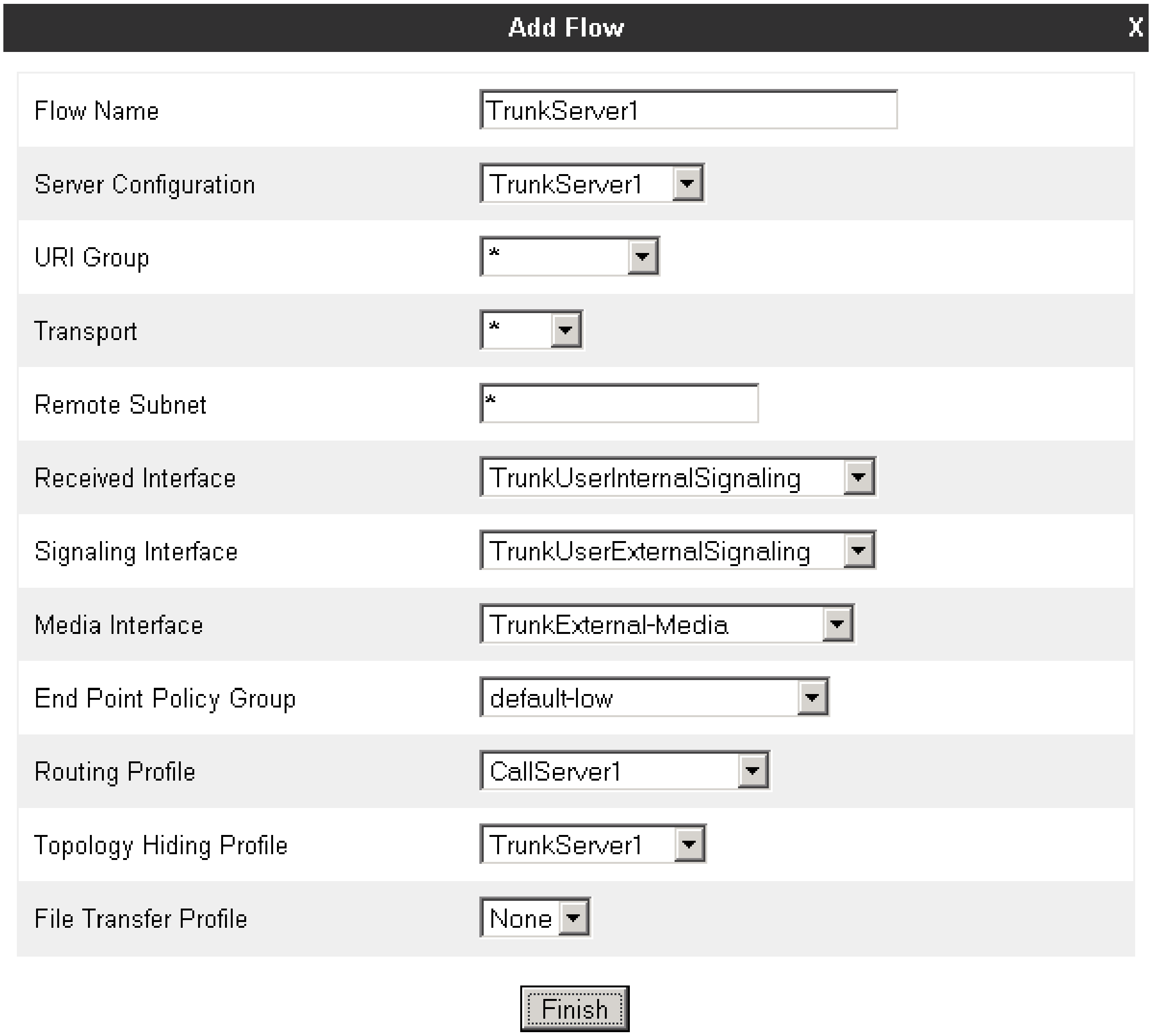
When a packet is received by Avaya SBCE, the content of the packet (IP addresses, URIs, etc.) is used to determine which flow it matches. Once the flow is determined, the flow points to a policy which contains several rules concerning processing, privileges, authentication, routing, etc. Once routing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



To create a Server Flow for Mitel 3300 and SIP Trunk service, navigate to **Device Specific Settings → End Point Flows**. Select the **Server Flows** tab and click **Add** as highlighted below.



The following screen shows the flow named "TrunkServer1" configured in the sample configuration. This flow uses the interfaces, polices, and profiles defined in previous sections. Click **Finish**.



Similarly, “CallServer1” was configured in this sample configuration as shown below.

Add Flow

Flow Name	CallServer1
Server Configuration	CallServer1
URI Group	*
Transport	*
Remote Subnet	*
Received Interface	TrunkUserExternalSignaling
Signaling Interface	TrunkUserInternalSignaling
Media Interface	Trunk-Internal-Media
End Point Policy Group	default-low
Routing Profile	TrunkServer1
Topology Hiding Profile	CallServer1
File Transfer Profile	None

Finish

7. Service Provider Configuration

For service provisioning, SIP trunk Service provider will require the customer IP address of the Avaya Session Border Controller if placed at edge of the network or the Data firewall in front of the Avaya Session Border Controller for Enterprise as required for Trunk provider to route traffic to the customer environment. SIP Trunk Provider provided the following information for the compliance testing: the IP address and port used by the SIP Trunk Server, and the numbers. This information was used to complete the configuration for Avaya Session Border Controller for Enterprise shown in Section 6 and the Mitel 3300 1.8 shown in Section 5.

Note: Verizon SIP Trunk was used as test Trunk in this test environment. Any SIP trunk service can be configured in Avaya session border controller with minor changes to this application notes on trunk server specific configurations as applicable to the customer deployment.

8. Troubleshooting

This section provides example verifications of the Avaya configuration with SIP Trunk service.

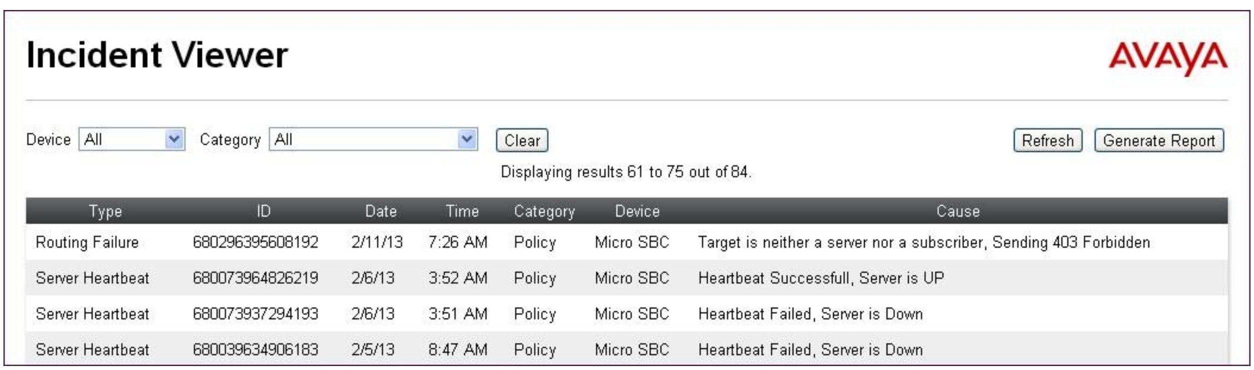
8.1. Avaya SBCE

This section provides verification steps that may be performed with the Avaya SBCE.

8.1.1. Incidents

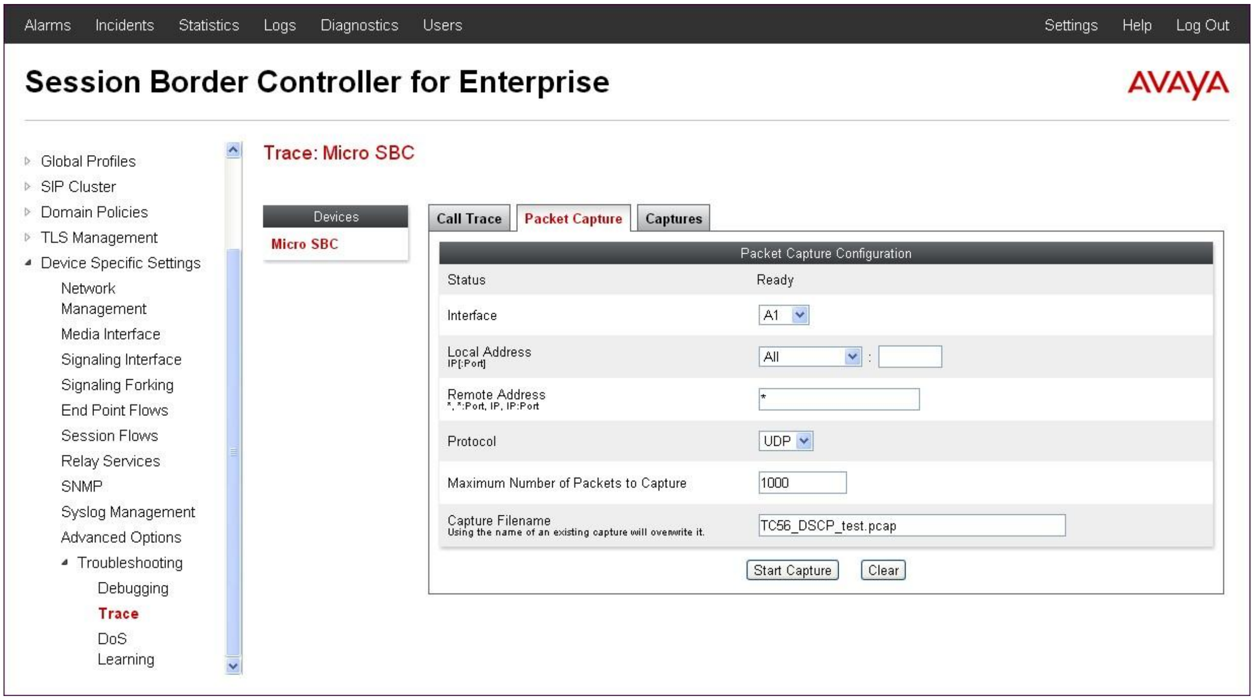
The Incident Viewer can be accessed from the Avaya SBCE Dashboard as highlighted in the screen shot below.

Use the Incident Viewer to verify Server Heartbeat and to troubleshoot routing failures. This verification is applicable if the Trunk server supports Heartbeat mechanism and is configured in the deployment.

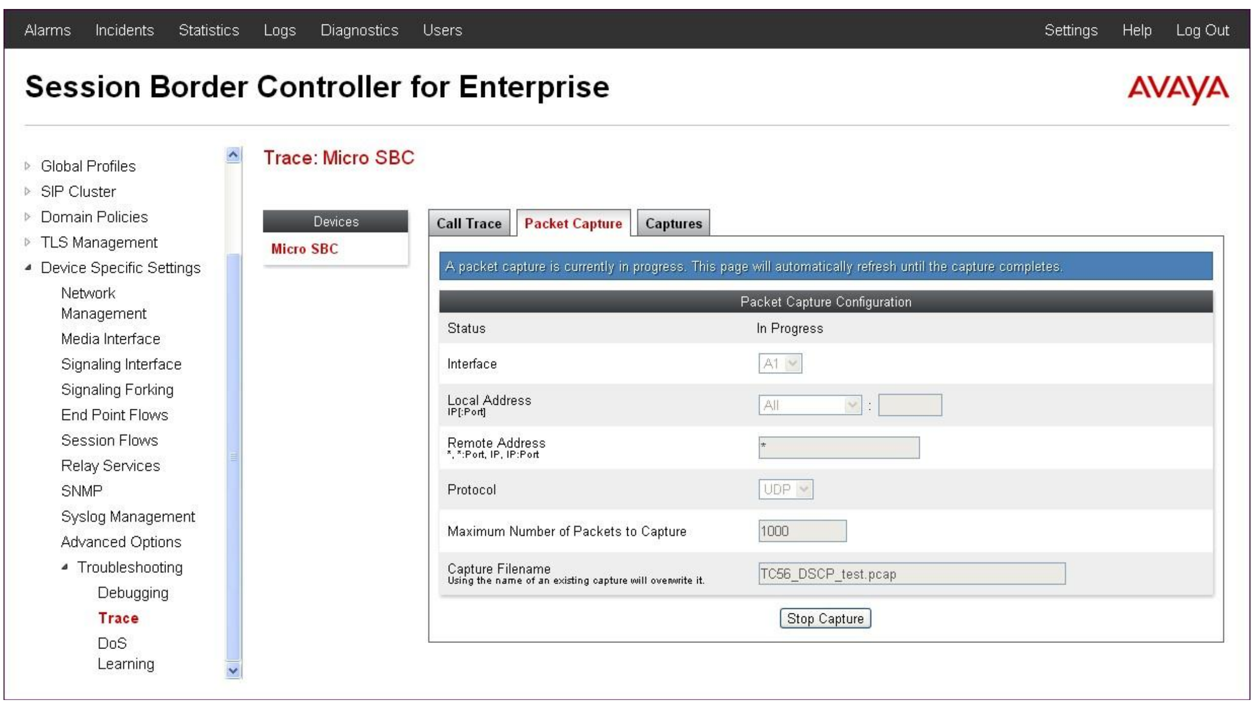


8.1.2. Tracing

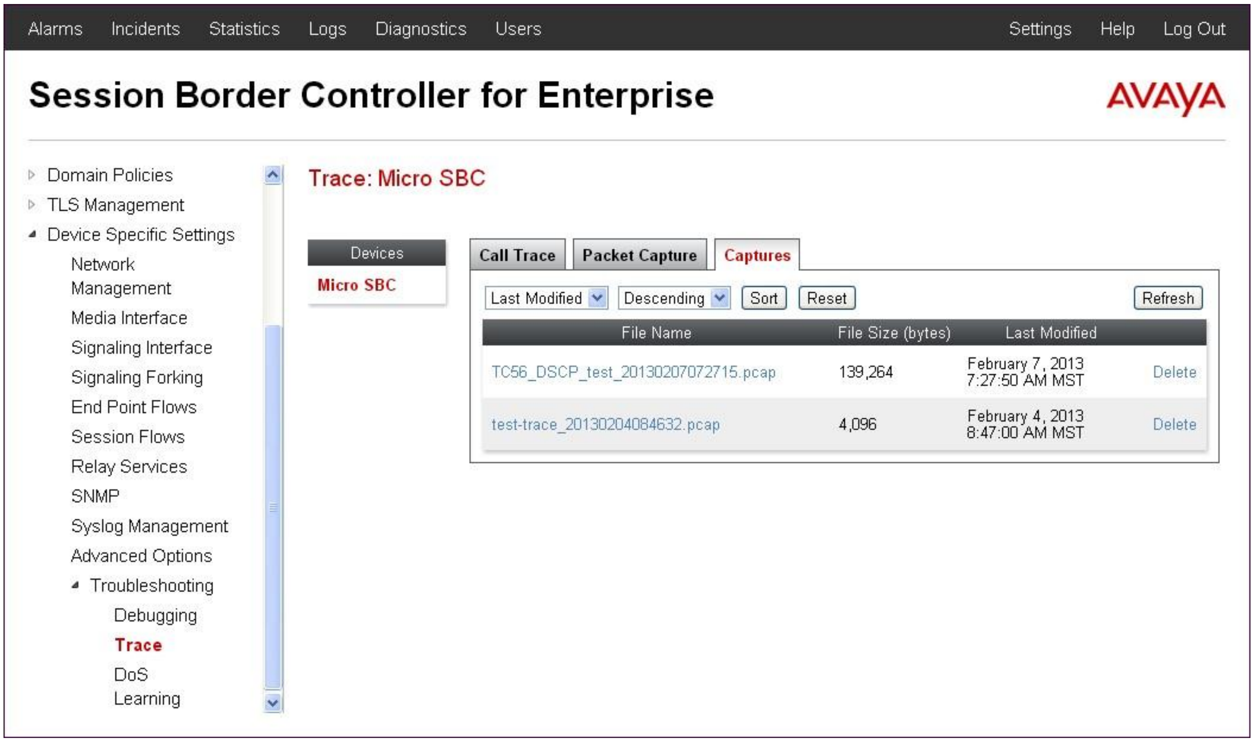
To take a call trace, navigate to **Device Specific Settings → Trace** and select the **Packet Capture** tab. Populate the fields for the capture parameters and click **Start Capture** as shown below.



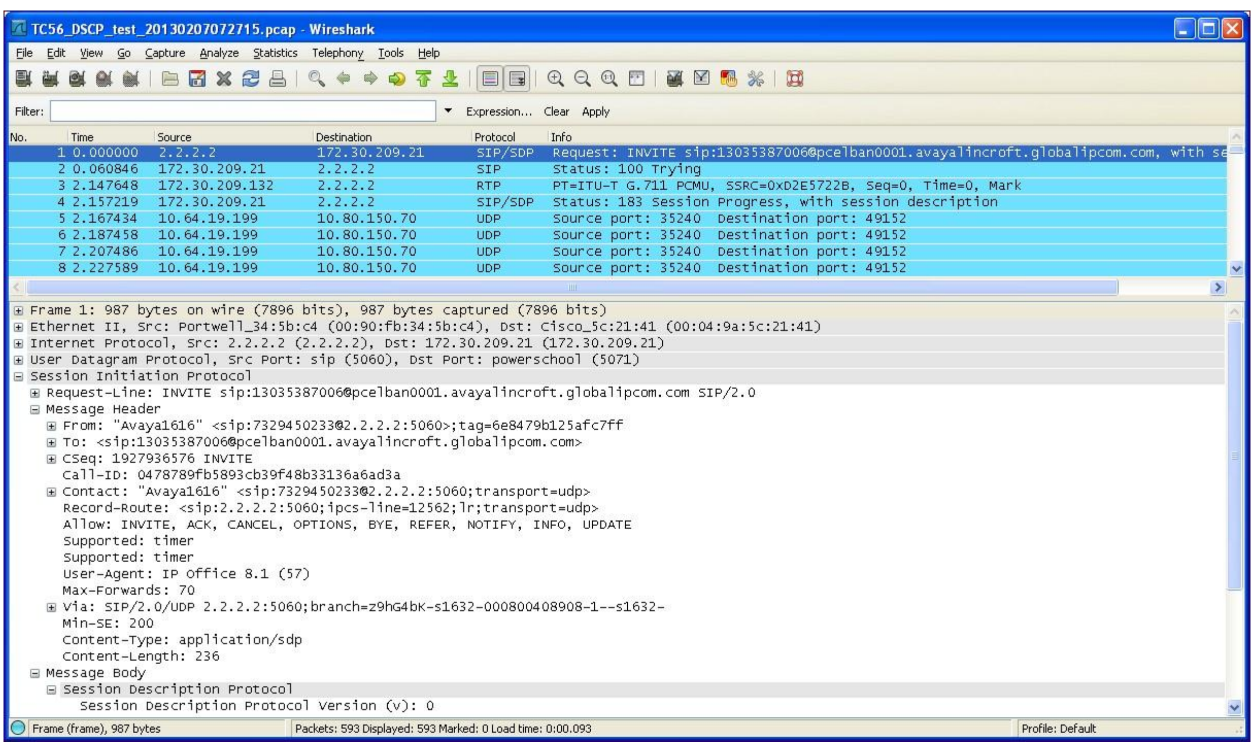
When tracing has reached the desired number of packets the trace will stop automatically, or alternatively, hit the **Stop Capture** button at the bottom.



Select the **Captures** tab to view the files created during the packet capture.



The packet capture file can be downloaded and then viewed using a Network Protocol Analyzer like WireShark.



8.2. Mitel 3300

This section provides verification steps that may be performed with the Mitel 3300.

8.2.1. Troubleshooting

Several tools and aides can be used to troubleshoot issues with Mitel 3300. Please consult reference [3] with any hardware and software problems.

9. Conclusion

Avaya Session border Controller for Enterprise advances state-of-the-art enterprise communications and collaboration. It serves as the foundation to deliver session management, voice, video, messaging, mobility, web conferencing, and security in a flexible way that bridges systems and protects investments.

These Application Notes demonstrated how Avaya Session Border Controller for Enterprise Release 6.2 and Mitel 3300 can be successfully combined with a SIP Trunk service connection to enable a business to receive and send calls. Utilizing this solution, Mitel 3300 customers can leverage the operational efficiencies and cost savings associated with SIP trunk while gaining the advanced technical features provided through the marriage of best of breed technologies from Avaya and SIP trunk Providers.

Mitel 3300 with Avaya Session Border Controller for Enterprise Release 6.2 has not been independently certified by Service Providers. This application Notes is based on the testing utilizing Test Trunk service available in Test Lab. This Application notes can be utilized for administering and configuring SIP trunk Deployments with Avaya Session Border Controller with minor appropriate modifications as required for the deployments.

10. Additional References

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

[1] *3300 Integrated Communications Platform Technician's Handbook Mitel Communications Director, Release 6.0 57011493 Rev B,* February 2013

[2] *Mitel Communications Director, Release 6.0 Rev. B,* February 2013

[3] *Troubleshooting Guide Mitel Director, Release 6.0 Rev. A,* January, 2013

[4] *Administering Avaya Session Border Controller*, Document Number 08-604063, Sept. 2012

The Application Notes referenced below correspond to the formal compliance testing by Tekvizion labs for Mitel 3300 MCD release 6.0 with SIP Trunking and Avaya Service Session Border Controller for Enterprise 6.2

[RFC-3261] RFC 3261 *SIP: Session Initiation Protocol* http://www.ietf.org/rfc/rfc3261.txt
[RFC-2833] RFC 2833 *RTP Payload for DTMF Digits, Telephony Tones and Telephony Signals* http://www.ietf.org/rfc/rfc2833.txt