Configuration Note

AudioCodes Professional Services – Interoperability Lab

Generic IP-PBX and Telia Entry SIP Trunk using AudioCodes Mediant™ E-SBC

Version 7.2

Table of Contents

This page is intentionally left blank.

Notice

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document can be downloaded from https://www.audiocodes.com/library/technical-documents.

This document is subject to change without notice.

Date Published: February-20-2018

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our Web site at https://www.audiocodes.com/services-support/maintenance-and-support.

Document Revision Record

LTRT	Description
39275	Initial document release for Version 7.2.

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our Web site at https://online.audiocodes.com/documentation-feedback.

This page is intentionally left blank.

1 Introduction

This Configuration Note describes how to set up AudioCodes Enterprise Session Border Controller (hereafter, referred to as *E-SBC*) for interworking between Telia Entry's SIP Trunk and Generic IP-PBX environment.

You can also use AudioCodes' SBC Wizard tool to automatically configure the E-SBC based on this interoperability setup. However, it is recommended to read through this document in order to better understand the various configuration options. For more information on AudioCodes' SBC Wizard including the download option, visit AudioCodes Web site at https://www.audiocodes.com/partners/sbc-interoperability-list.

1.1 Intended Audience

The document is intended for engineers, or AudioCodes and Telia Entry Partners who are responsible for installing and configuring Telia Entry's SIP Trunk and IP-PBX for enabling VoIP calls using AudioCodes E-SBC.

1.2 About AudioCodes E-SBC Product Series

AudioCodes' family of E-SBC devices enables reliable connectivity and security between the Enterprise's and the service provider's VoIP networks.

The E-SBC provides perimeter defense as a way of protecting Enterprises from malicious VoIP attacks; mediation for allowing the connection of any PBX and/or IP-PBX to any service provider; and Service Assurance for service quality and manageability.

Designed as a cost-effective appliance, the E-SBC is based on field-proven VoIP and network services with a native host processor, allowing the creation of purpose-built multiservice appliances, providing smooth connectivity to cloud services, with integrated quality of service, SLA monitoring, security and manageability. The native implementation of SBC provides a host of additional capabilities that are not possible with standalone SBC appliances such as VoIP mediation, PSTN access survivability, and third-party value-added services applications. This enables Enterprises to utilize the advantages of converged networks and eliminate the need for standalone appliances.

AudioCodes E-SBC is available as an integrated solution running on top of its field-proven Mediant Media Gateway and Multi-Service Business Router platforms, or as a software-only solution for deployment with third-party hardware.

This page is intentionally left blank.

2 Component Information

2.1 AudioCodes E-SBC Version

Table 2-1: AudioCodes E-SBC Version

SBC Vendor	AudioCodes
Models	▪ Mediant 500 Gateway & E-SBC ▪ Mediant 500L Gateway & E-SBC ▪ Mediant 800B Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 2600 E-SBC ▪ Mediant 4000 SBC ▪ Mediant 4000B SBC ▪ Mediant 9000 SBC ▪ Mediant Software SBC (SE and VE)
Software Version	7.20A.158.009
Protocol	▪ SIP/UDP or SIP/TCP (to both, Telia Entry SIP Trunk and IP-PBX)
Additional Notes	None

2.2 Telia Entry SIP Trunking Version

Table 2-2: Telia Entry Version

Vendor/Service Provider	Telia Entry
SSW Model/Service	
Software Version	
Protocol	SIP
Additional Notes	None

2.3 IP-PBX Version

Table 2-3: IP-PBX Version

Vendor	Due to constraints tests were performed remotely; only X-Lite, Ekiga and Linphone softphones were used for IP-PBX simulation.
Model	
Software Version	
Protocol	SIP
Additional Notes	None

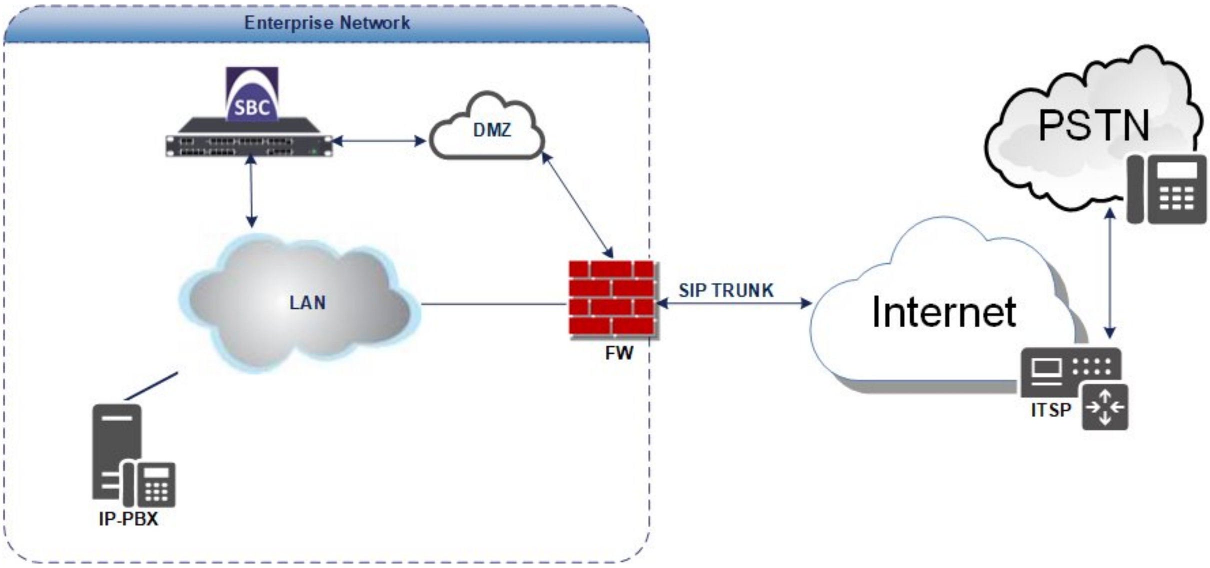
2.4 Interoperability Test Topology

The interoperability testing between AudioCodes E-SBC and Telia Entry SIP Trunk with Generic IP-PBX was done using the following topology setup:

- Enterprise deployed with IP-PBX in its private network for enhanced communication within the Enterprise.
- Enterprise wishes to offer its employees enterprise-voice capabilities and to connect the Enterprise to the PSTN network using Telia Entry's SIP Trunking service.
- AudioCodes E-SBC is implemented to interconnect between the Enterprise LAN and the SIP Trunk.
  - **Session:** Real-time voice session using the IP-based Session Initiation Protocol (SIP).
  - **Border:** IP-to-IP network border between IP-PBX network in the Enterprise LAN and Telia Entry's SIP Trunk located in the public network.

The figure below illustrates this interoperability test topology:

Figure 2-1: Interoperability Test Topology between E-SBC and IP-PBX with Telia Entry SIP Trunk



2.4.1 Environment Setup

The interoperability test topology includes the following environment setup:

Table 2-4: Environment Setup

Area	Setup
Network	▪ IP-PBX environment is located on the Enterprise's LAN ▪ Telia Entry SIP Trunk is located on the WAN
Signaling Transcoding	▪ Both IP-PBX and Telia Entry SIP Trunk, operate with SIP-over-UDP or SIP-over-TCP transport types
Codecs Transcoding	▪ IP-PBX supports G.711A-law, G.711U-law and G.722 coders ▪ Telia Entry SIP Trunk supports G.711A-law coder
Media Transcoding	▪ Both IP-PBX and Telia Entry SIP Trunk, operate with RTP media type

2.4.2 Known Limitations

There were no limitations observed in the interoperability tests done for the AudioCodes E-SBC interworking between Generic IP-PBX and Telia Entry 's SIP Trunk.

This page is intentionally left blank.

3 Configuring IP-PBX

Due to the constraint that interoperability tests were performed remotely, only X-Lite, Ekiga and Linphone softphones were used for IP-PBX simulation.

This page is intentionally left blank.

4 Configuring AudioCodes E-SBC

This section provides step-by-step procedures on how to configure AudioCodes E-SBC for interworking between IP-PBX and the Telia Entry SIP Trunk. These configuration procedures are based on the interoperability test topology described in Section 2.4 on page 10, and includes the following main areas:

- E-SBC WAN interface -   Telia Entry SIP Trunking environment
- E-SBC LAN interface – IP-PBX environment

This configuration is done using the E-SBC's embedded Web server (hereafter, referred to as *Web interface*).

Notes:

- For implementing IP-PBX and Telia Entry SIP Trunk based on the configuration described in this section, AudioCodes E-SBC must be installed with a License Key that includes the following software features:
  - √ **SBC**
  - √ **DSP**
  - √ **RTP**
  - √ **SIP**

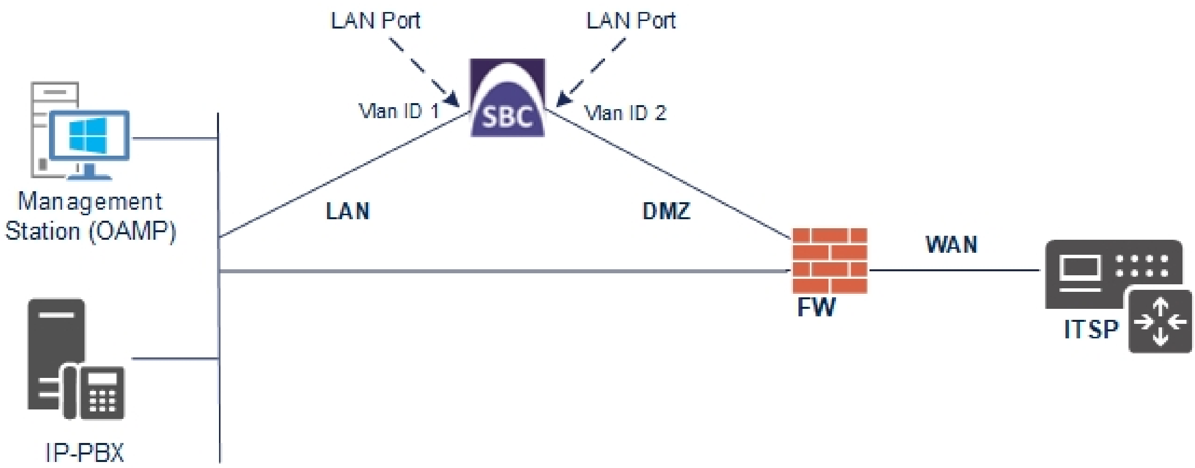
  For more information about the License Key, contact your AudioCodes sales representative.
- The scope of this interoperability test and document does **not** cover all security aspects for configuring this topology. Comprehensive security measures should be implemented per your organization's security policies. For security recommendations on AudioCodes' products, refer to the *Recommended Security Guidelines* document.

4.1 Step 1: IP Network Interfaces Configuration

This step describes how to configure the E-SBC's IP network interfaces. There are several ways to deploy the E-SBC; however, this interoperability test topology employs the following deployment method:

- E-SBC interfaces with the following IP entities:
  - IP-PBX, located on the LAN
  - Telia Entry SIP Trunk, located on the WAN
- E-SBC connects to the WAN through a DMZ network
- Physical connection: The type of physical connection to the LAN depends on the method used to connect to the Enterprise's network. In the interoperability test topology, E-SBC connects to the LAN and DMZ using dedicated LAN ports (i.e., two ports and two network cables are used).
- E-SBC also uses two logical network interfaces:
  - LAN (VLAN ID 1)
  - DMZ (VLAN ID 2)

Figure 4-1: Network Interfaces in Interoperability Test Topology



4.1.1 Step 1a: Configure VLANs

This step describes how to define VLANs for each of the following interfaces:

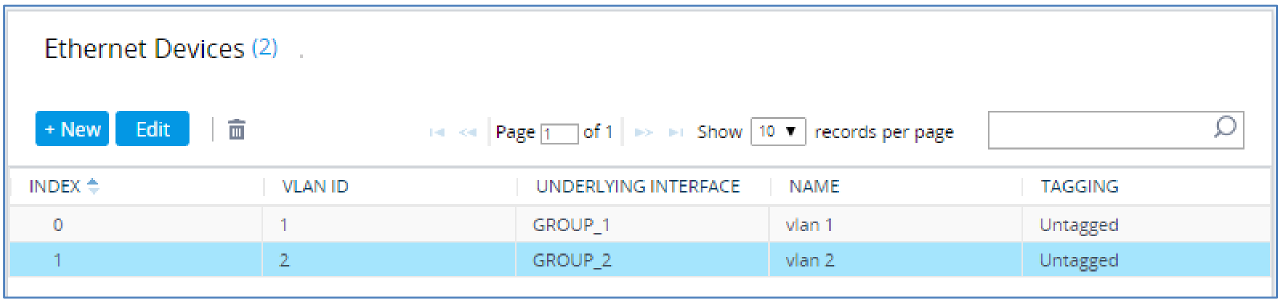
- LAN VoIP (assigned the name "LAN_IF")
- WAN VoIP (assigned the name "WAN_IF")

➢ To configure the VLANs:

1. Open the Ethernet Device table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **Ethernet Devices**).
2. There will be one existing row for VLAN ID 1 and underlying interface GROUP_1.
3. Add another VLAN ID 2 for the WAN side as follows:

Parameter	Value
Index	**1**
VLAN ID	**2**
Underlying Interface	**GROUP_2** (Ethernet port group)
Name	**vlan 2**
Tagging	**Untagged**

Figure 4-2: Configured VLAN IDs in Ethernet Device


Ethernet Devices (2)

+ New Edit Page 1 of 1 Show 10 records per page

INDEX	VLAN ID	UNDERLYING INTERFACE	NAME	TAGGING
0	1	GROUP_1	vlan 1	Untagged
1	2	GROUP_2	vlan 2	Untagged

4.1.2 Step 1b: Configure Network Interfaces

This step describes how to configure the IP network interfaces for each of the following interfaces:

- LAN VoIP (assigned the name "LAN_IF")
- WAN VoIP (assigned the name "WAN_IF")

➢ To configure the IP network interfaces:

1. Open the IP Interfaces table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **IP Interfaces**).
2. Modify the existing LAN network interface:
   a. Select the 'Index' radio button of the **OAMP + Media + Control** table row, and then click **Edit**.
   b. Configure the interface as follows:

Parameter	Value
Name	**LAN_IF** (arbitrary descriptive name)
Ethernet Device	**vlan 1**
IP Address	**10.15.77.55** (LAN IP address of E-SBC)
Prefix Length	**16** (subnet mask in bits for 255.255.0.0)
Default Gateway	**10.15.0.1**
Primary DNS	**10.15.27.1**

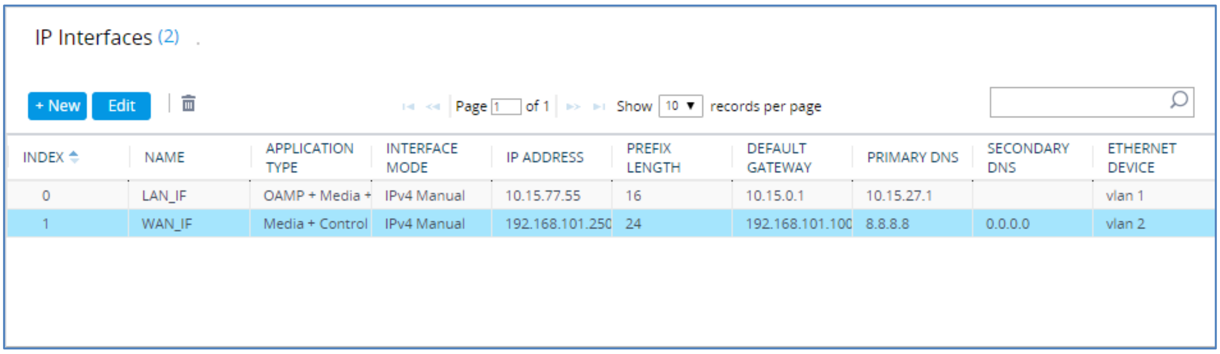
3. Add a network interface for the WAN side:
   a. Click **New**.
   b. Configure the interface as follows:

Parameter	Value
Name	**WAN_IF**
Application Type	**Media + Control**
Ethernet Device	**vlan 2**
IP Address	**192.168.101.250** (DMZ IP address of E-SBC)
Prefix Length	**24** (subnet mask in bits for 255.255.255.0)
Default Gateway	**192.168.101.100** (router's IP address)
Primary DNS	**8.8.8.8**
Secondary DNS	**0.0.0.0**

4. Click **Apply**.

The configured IP network interfaces are shown below:

Figure 4-3: Configured Network Interfaces in IP Interfaces Table


IP Interfaces (2)

+ New | Edit | Page 1 of 1 | Show 10 records per page

INDEX	NAME	APPLICATION TYPE	INTERFACE MODE	IP ADDRESS	PREFIX LENGTH	DEFAULT GATEWAY	PRIMARY DNS	SECONDARY DNS	ETHERNET DEVICE
0	LAN_IF	OAMP + Media +	IPv4 Manual	10.15.77.55	16	10.15.0.1	10.15.27.1		vlan 1
1	WAN_IF	Media + Control	IPv4 Manual	192.168.101.250	24	192.168.101.100	8.8.8.8	0.0.0.0	vlan 2

4.2 Step 2: Enable the SBC Application

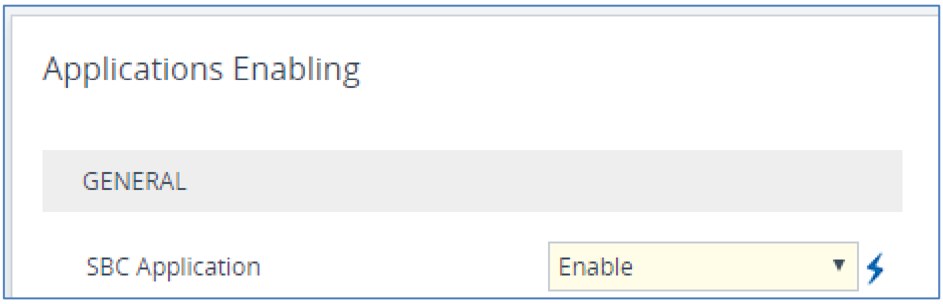
This step describes how to enable the SBC application.

Note: The SBC application is enabled by default. Sometimes it can be disabled manually. This step is relevant only if the SBC application was disabled.

➢ **To enable the SBC application:**

1. Open the Applications Enabling page (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Applications Enabling**).

Figure 4-4: Enabling SBC Application



2. From the 'SBC Application' drop-down list, select **Enable**.
3. Click **Apply**.
4. Reset the E-SBC with a burn to flash for this setting to take effect (see Section 4.13 on page 51).

4.3 Step 3: Configure Media Realms

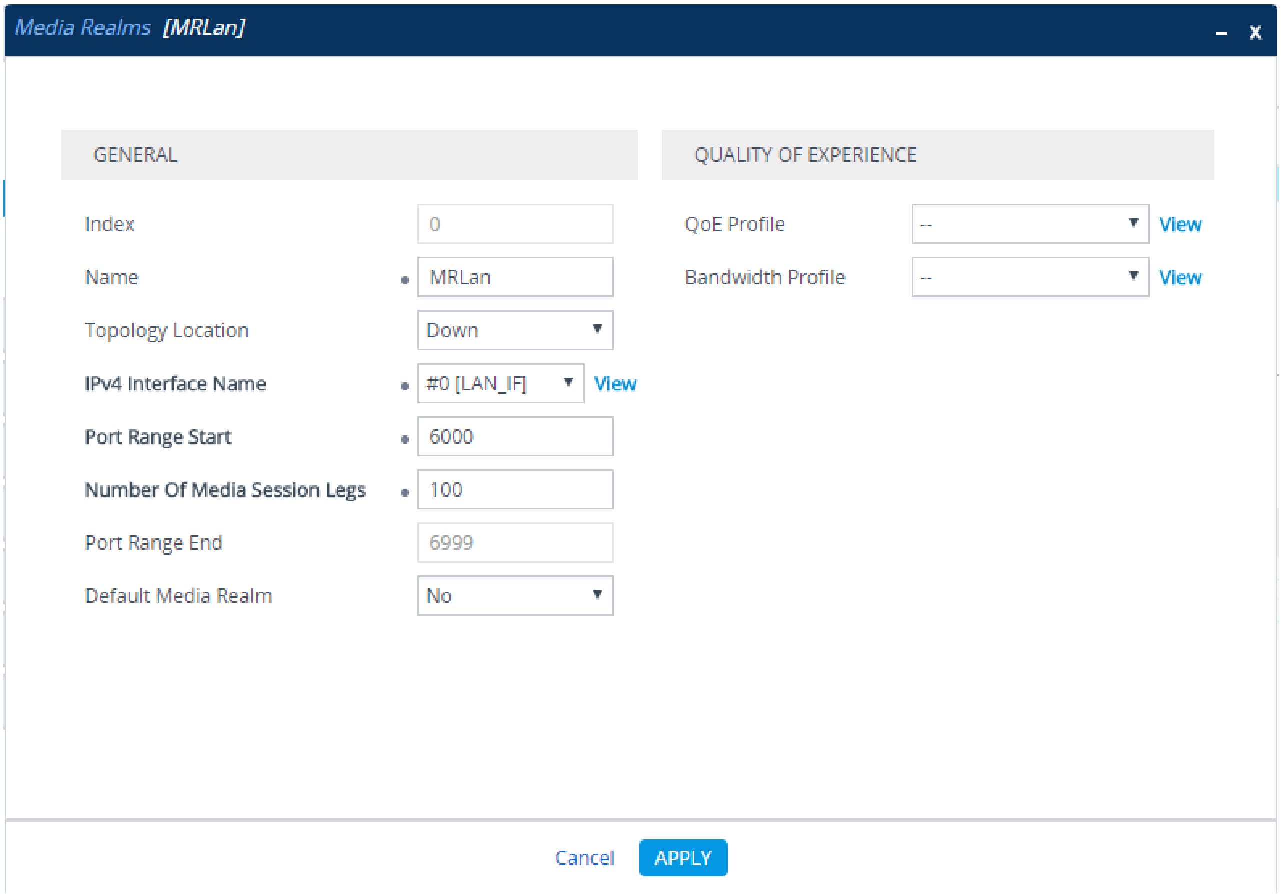
This step describes how to configure Media Realms. The simplest configuration is to create two Media Realms - one for internal (LAN) traffic and one for external (WAN) traffic.

➢ **To configure Media Realms:**

1. Open the Media Realms table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Media Realms**).
2. Add a Media Realm for the LAN interface. You can use the default Media Realm (Index 0), but modify it as shown below:

Parameter	Value
Index	**0**
Name	**MRLan** (descriptive name)
IPv4 Interface Name	**LAN_IF**
Port Range Start	**6000** (represents lowest UDP port number used for media on LAN)
Number of Media Session Legs	**100** (media sessions assigned with port range)

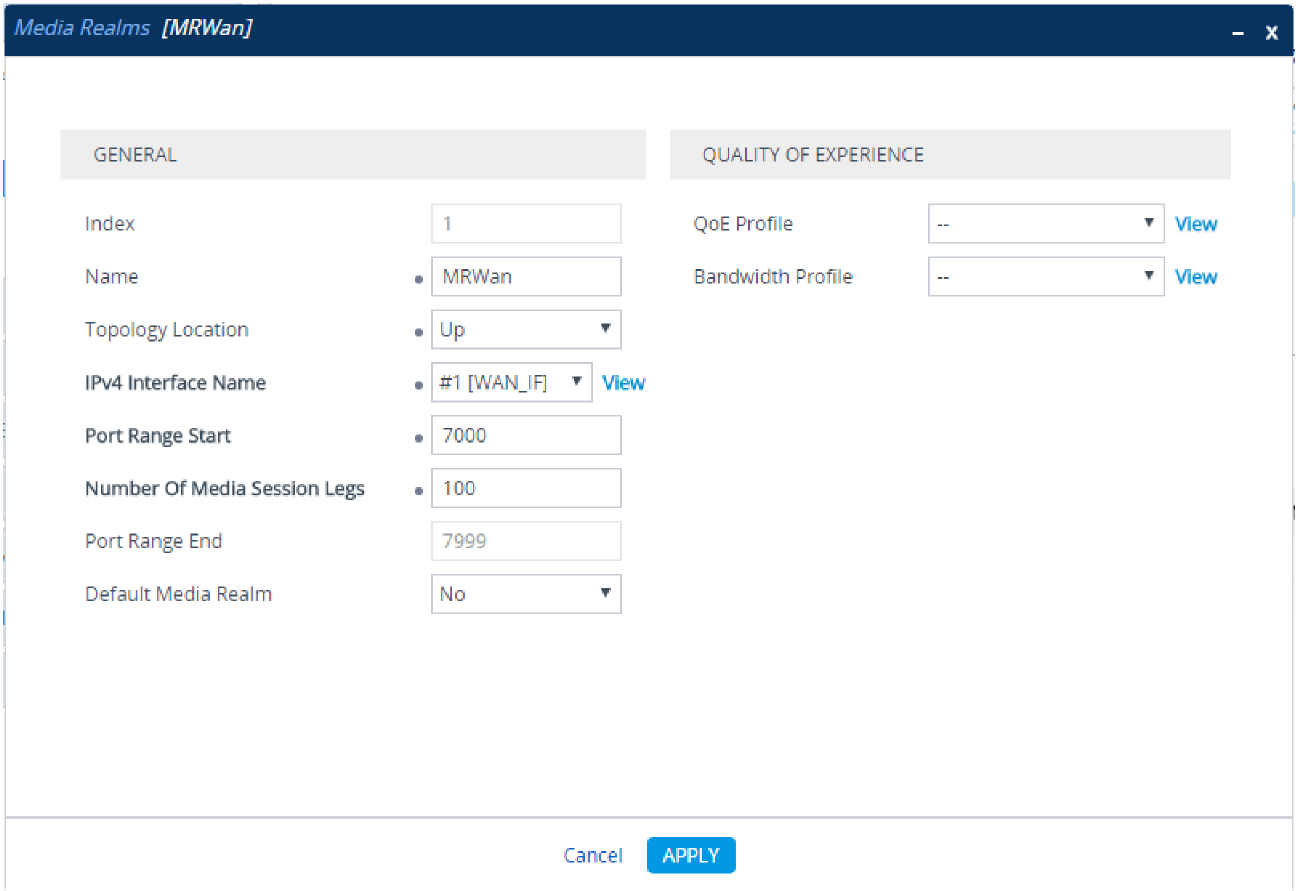
Figure 4-5: Configuring Media Realm for LAN



3. Configure a Media Realm for WAN traffic:

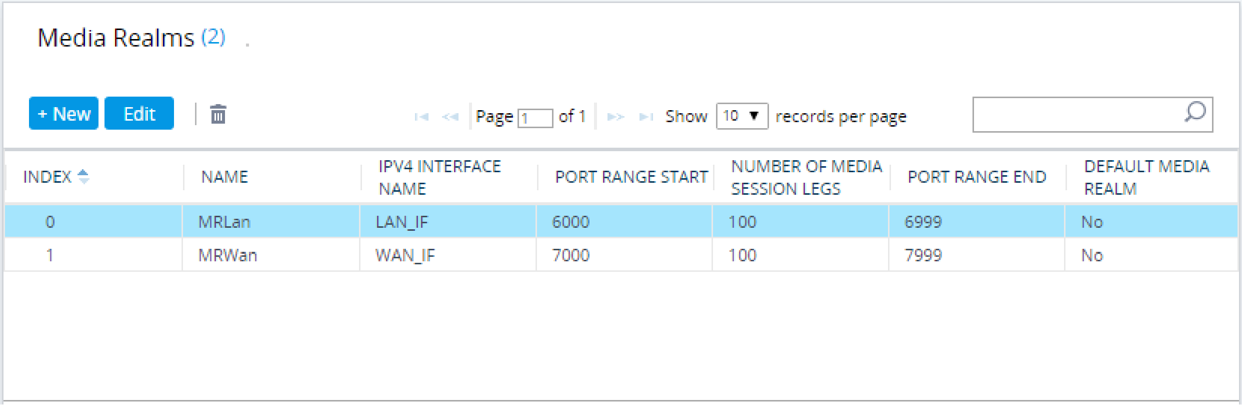
Parameter	Value
Index	**1**
Name	**MRWan** (arbitrary name)
Topology Location	**Up**
IPv4 Interface Name	**WAN_IF**
Port Range Start	**7000** (represents lowest UDP port number used for media on WAN)
Number of Media Session Legs	**100** (media sessions assigned with port range)

Figure 4-6: Configuring Media Realm for WAN



The configured Media Realms are shown in the figure below:

Figure 4-7: Configured Media Realms in Media Realm Table



INDEX	NAME	IPV4 INTERFACE NAME	PORT RANGE START	NUMBER OF MEDIA SESSION LEGS	PORT RANGE END	DEFAULT MEDIA REALM
0	MRLan	LAN_IF	6000	100	6999	No
1	MRWan	WAN_IF	7000	100	7999	No

4.4 Step 4: Configure SIP Signaling Interfaces

This step describes how to configure SIP Interfaces. For the interoperability test topology, an internal and external SIP Interface must be configured for the E-SBC.

➢ **To configure SIP Interfaces:**

1. Open the SIP Interfaces table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **SIP Interfaces**).
2. Add a SIP Interface for the LAN interface. You can use the default SIP Interface (Index 0), but modify it as shown below:

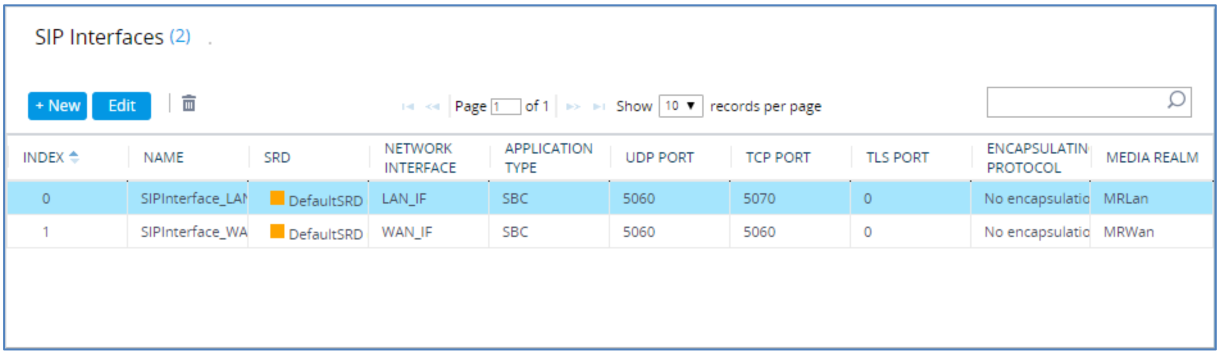
Parameter	Value
Index	**0**
Name	**SIPInterface_LAN** (see note at the end of this section)
Network Interface	**LAN_IF**
Application Type	**SBC**
UDP Port	**5060** (according to IP-PBX configuration)
TCP Port	**5070** (according to IP-PBX configuration)
TLS Port	**0**
Media Realm	**MRLan**

3. Configure a SIP Interface for the WAN:

Parameter	Value
Index	**1**
Name	**SIPInterface_WAN**
Network Interface	**WAN_IF**
Application Type	**SBC**
UDP Port	**5060**
TCP Port	**5060**
TLS Port	**0**
Media Realm	**MRWan**

The configured SIP Interfaces are shown in the figure below:

Figure 4-8: Configured SIP Interfaces in SIP Interface Table


SIP Interfaces (2)

+ New Edit

Page 1 of 1 Show 10 records per page

INDEX	NAME	SRD	NETWORK INTERFACE	APPLICATION TYPE	UDP PORT	TCP PORT	TLS PORT	ENCAPSULATIN PROTOCOL	MEDIA REALM
0	SIPInterface_LAN	DefaultSRD	LAN_IF	SBC	5060	5070	0	No encapsulatio	MRLan
1	SIPInterface_WA	DefaultSRD	WAN_IF	SBC	5060	5060	0	No encapsulatio	MRWan

Note: Current software releases uses the string **names** of the configuration entities (e.g., SIP Interface, Proxy Sets, and IP Groups). Therefore, it is recommended to configure each configuration entity with meaningful names for easy identification.

4.5 Step 5: Configure Proxy Sets

This step describes how to configure Proxy Sets. The Proxy Set defines the destination address (IP address or FQDN) of the IP entity server. Proxy Sets can also be used to configure load balancing between multiple servers.

For the interoperability test topology, two Proxy Sets need to be configured for the following IP entities:

- IP-PBX
- Telia Entry SIP Trunk

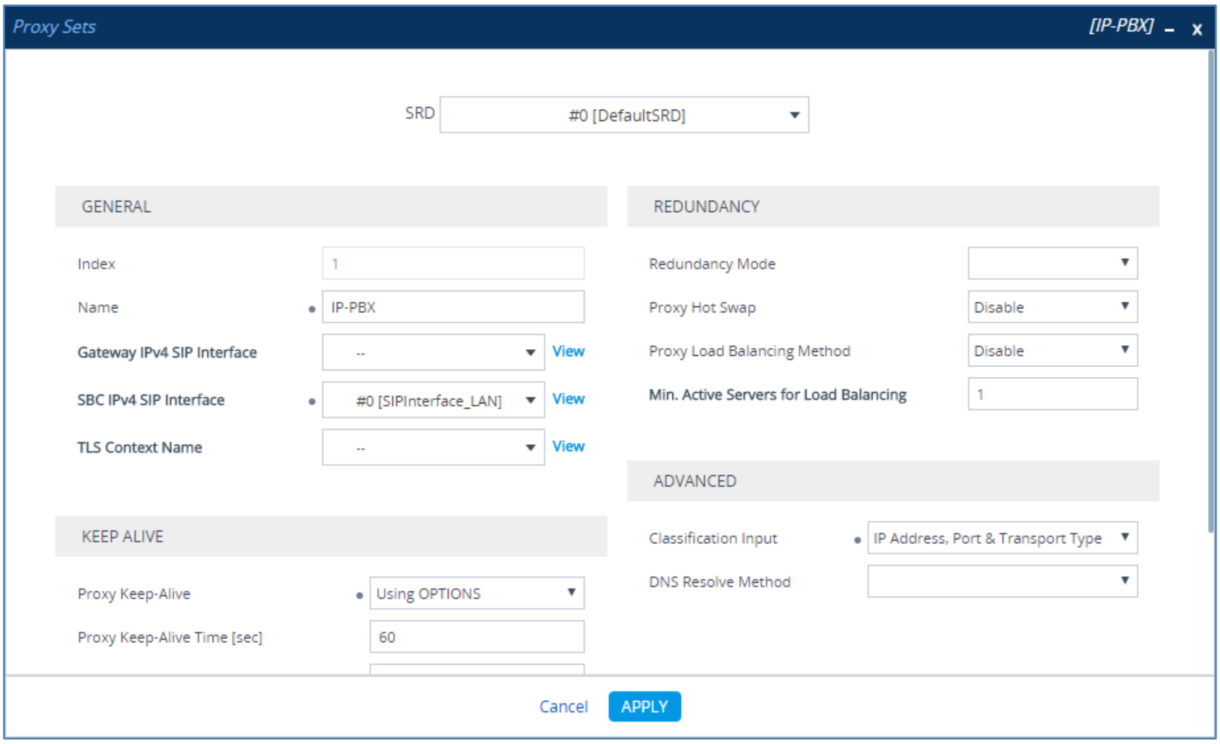
The Proxy Sets will be later applying to the VoIP network by assigning them to IP Groups.

➢ **To configure Proxy Sets:**

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder >**Proxy Sets**).
2. Add a Proxy Set for the IP-PBX as shown below:

Parameter	Value
Index	**1**
Name	**S4B**
SBC IPv4 SIP Interface	**SIPInterface_LAN**
Proxy Keep-Alive	**Using Options**

Figure 4-9: Configuring Proxy Set IP-PBX



a. Select the index row of the Proxy Set that you added, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.

b. Click **New**; the following dialog box appears:

Figure 4-10: Configuring Proxy Address for IP-PBX

c. Configure the address of the Proxy Set according to the parameters described in the table below.

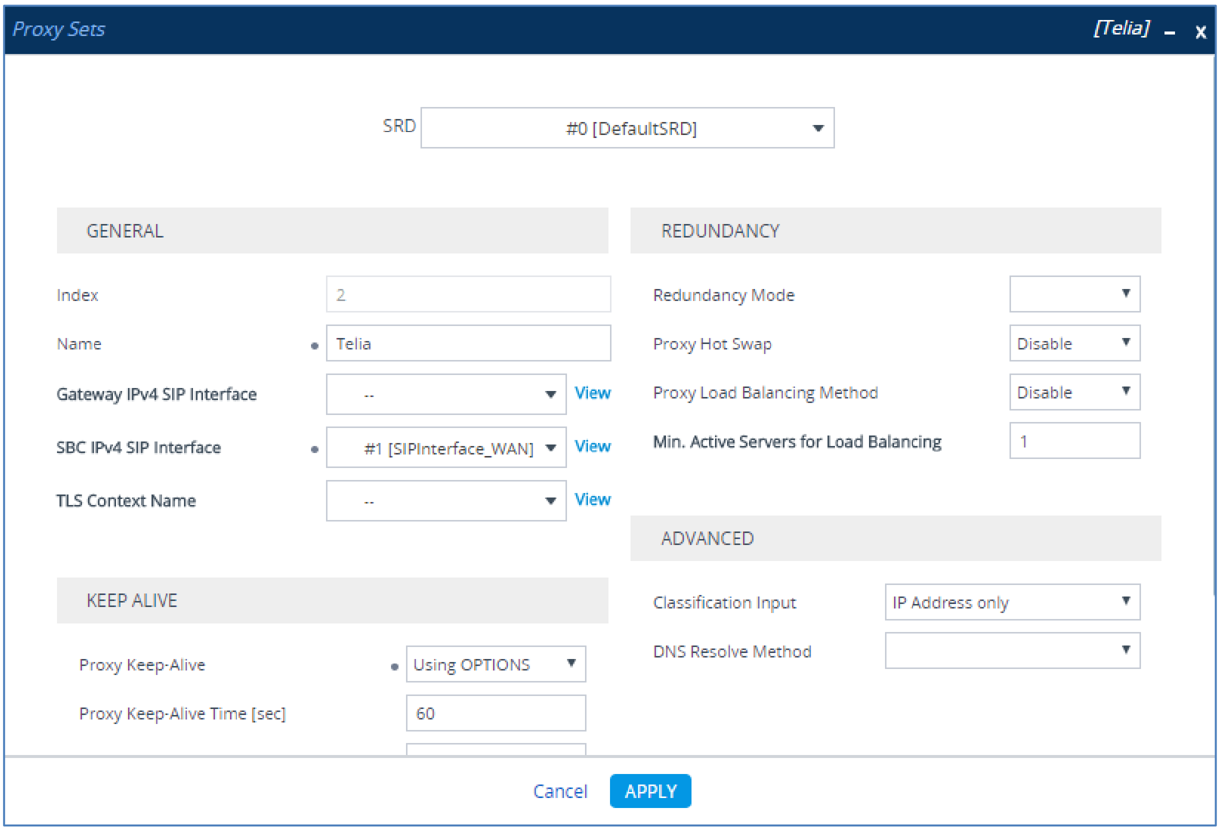
d. Click **Apply**.

Parameter	Value
Index	**0**
Proxy Address	**192.168.7.43:5060** (IP-PBX IP address / FQDN and destination port)
Transport Type	**UDP** (according to IP-PBX configuration)

3. Configure a Proxy Set for the Telia Entry SIP Trunk:

Parameter	Value
Index	**2**
Name	**ITSP**
SBC IPv4 SIP Interface	**SIPInterface_WAN**
Proxy Keep-Alive	**Using Options**

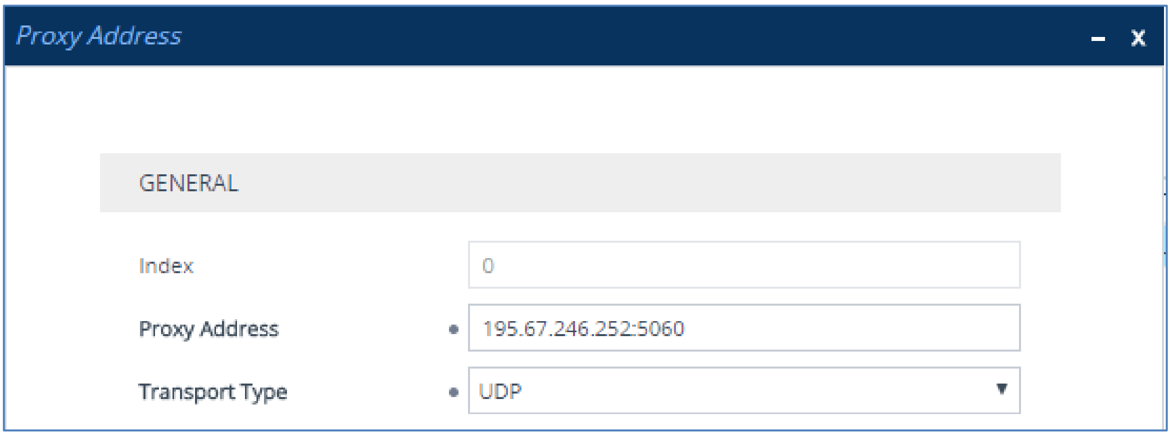
Figure 4-11: Configuring Proxy Set for Telia Entry SIP Trunk



a. Select the index row of the Proxy Set that you added, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.

b. Click **New**; the following dialog box appears:

Figure 4-12: Configuring Proxy Address for Telia Entry SIP Trunk



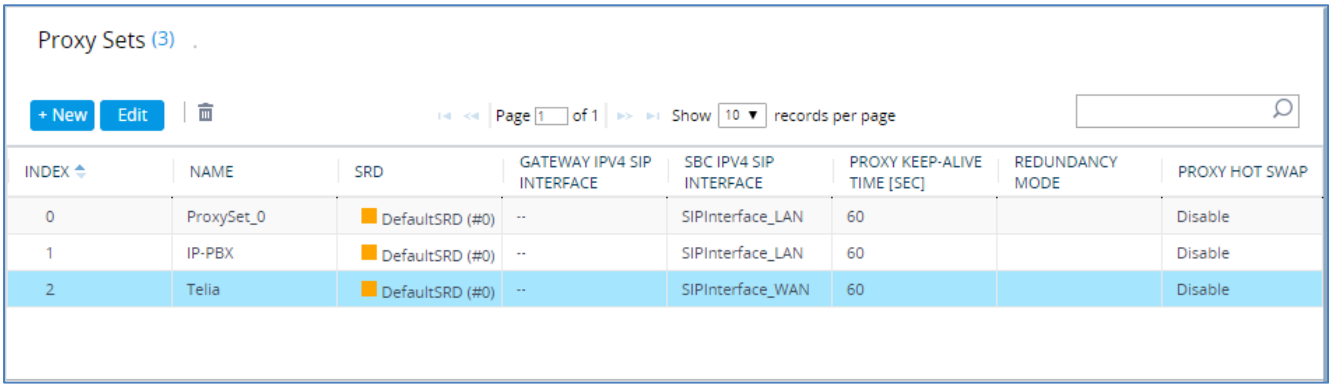
c. Configure the address of the Proxy Set according to the parameters described in the table below.

d. Click **Apply**.

Parameter	Value
Index	**0**
Proxy Address	**195.67.246.252:5060** (IP address / FQDN and destination port)
Transport Type	**UDP**

The configured Proxy Sets are shown in the figure below:

Figure 4-13: Configured Proxy Sets in Proxy Sets Table



4.6 Step 6: Configure IP Profiles

This step describes how to configure IP Profiles. The IP Profile defines a set of call capabilities relating to signaling (e.g., SIP message terminations such as REFER) and media (e.g., coder and transcoding method).

In this interoperability test topology, IP Profiles need to be configured for the following IP entities:

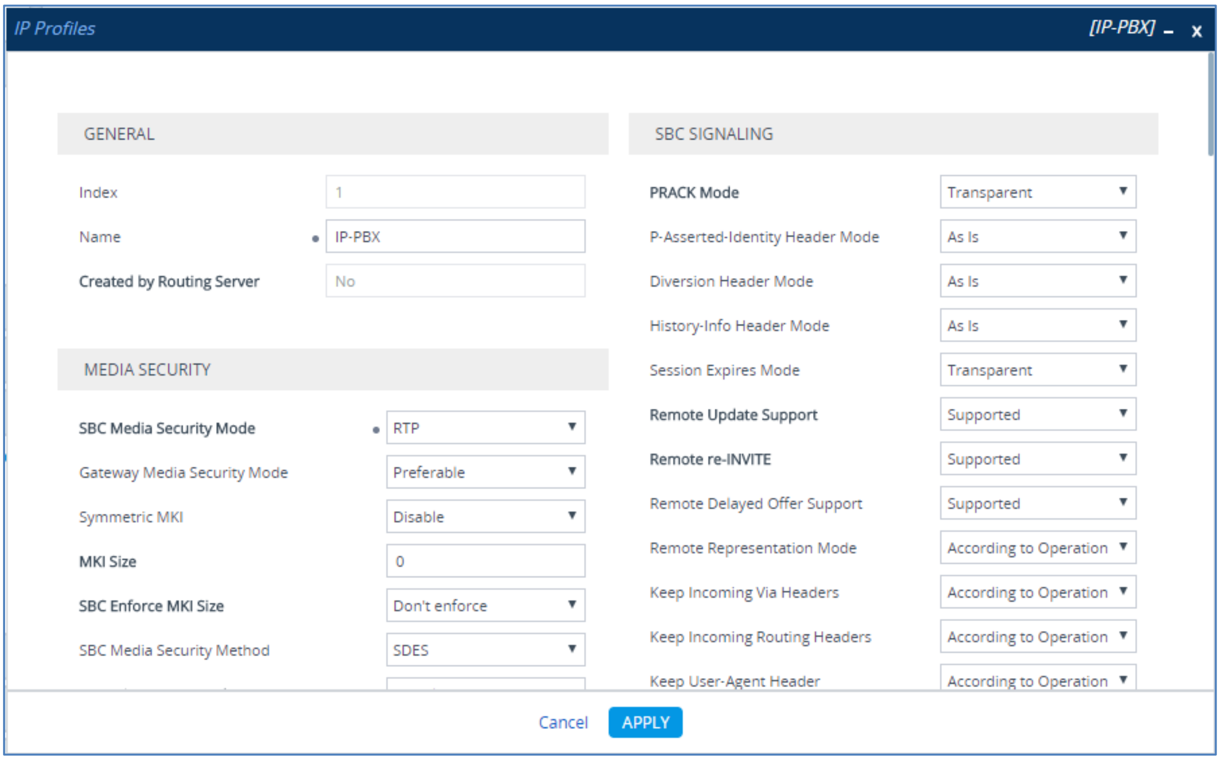
- IP-PBX – to operate in non-secure mode using RTP and SIP over UDP
- Telia Entry SIP trunk – to operate in non-secure mode using RTP and SIP over UDP

➢ **To configure IP Profile for the IP-PBX:**

1. Open the IP Profiles table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **IP Profiles**).
2. Click **New**, and then configure the parameters as follows:

Parameter	Value
General	
Index	**1**
Name	**IP-PBX**
Media Security	
SBC Media Security Mode	**RTP**
SBC Forward and Transfer	
Remote REFER Mode	**Handle Locally**
Remote 3xx Mode	**Handle Locally**
Media	
Broken Connection Mode	**Ignore**

Figure 4-14: Configuring IP Profile for IP-PBX



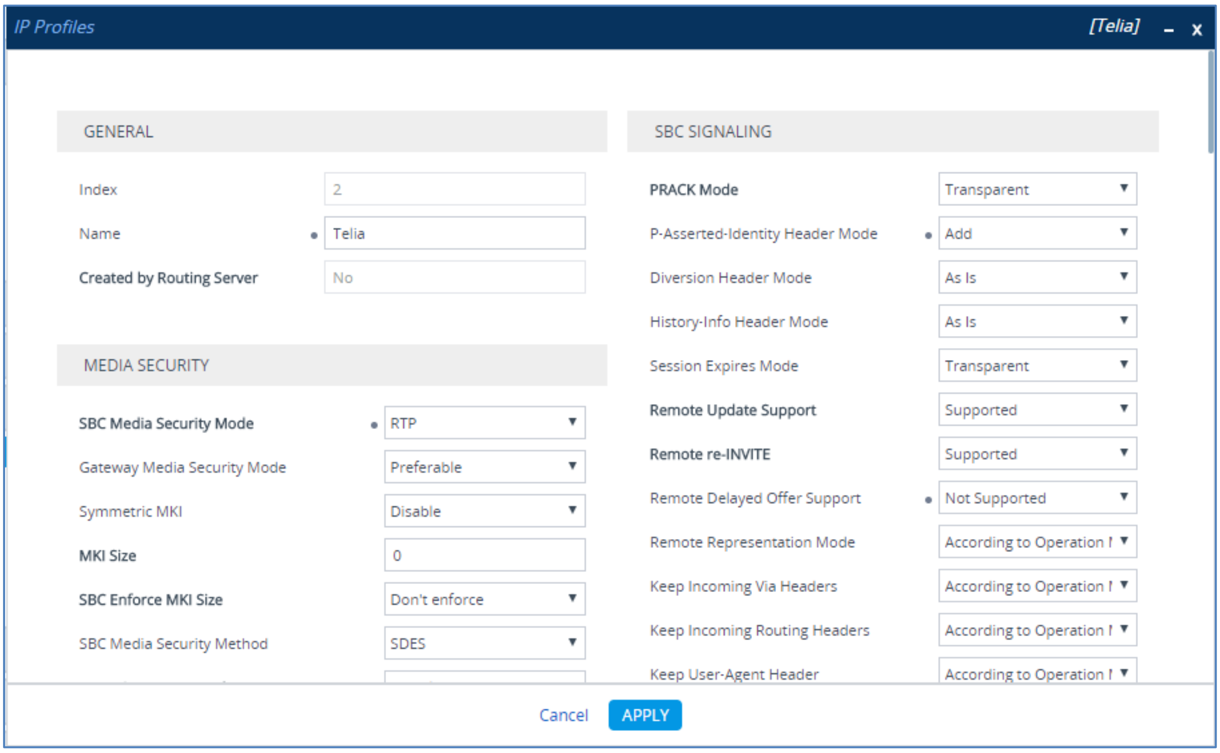
3. Click **Apply**.

➢ To configure an IP Profile for the Telia Entry SIP Trunk:

1. Click **New**, and then configure the parameters as follows:

Parameter	Value
General	
Index	**2**
Name	**Telia**
Media Security	
SBC Media Security Mode	**RTP**
SBC Early Media	
Remote Can Play Ringback	**No** (required if the IP-PBX does not provide a ringback tone for incoming calls)
SBC Signaling	
P-Asserted-Identity Header Mode	**Add** (required for anonymous calls)
Remote Delayed Offer Support	**Not Supported**
SBC Forward and Transfer	
Remote REFER Mode	**Handle Locally** (required, as ITSP does not support receipt of SIP REFER)
Play RBT To Transferee	**Yes**
Remote 3xx Mode	**Handle Locally**
Media	
Broken Connection Mode	**Ignore**

Figure 4-15: Configuring IP Profile for Telia Entry SIP Trunk



2. Click **Apply**.

4.7 Step 7: Configure IP Groups

This step describes how to configure IP Groups. The IP Group represents an IP entity on the network with which the E-SBC communicates. This can be a server (e.g., IP-PBX or ITSP) or it can be a group of users (e.g., LAN IP phones). For servers, the IP Group is typically used to define the server's IP address by associating it with a Proxy Set. Once IP Groups are configured, they are used to configure IP-to-IP routing rules for denoting source and destination of the call.

In this interoperability test topology, IP Groups must be configured for the following IP entities:

- IP-PBX located on LAN
- Telia Entry SIP Trunk located on WAN

➢ **To configure IP Groups:**

1. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
2. Add an IP Group for the IP-PBX:

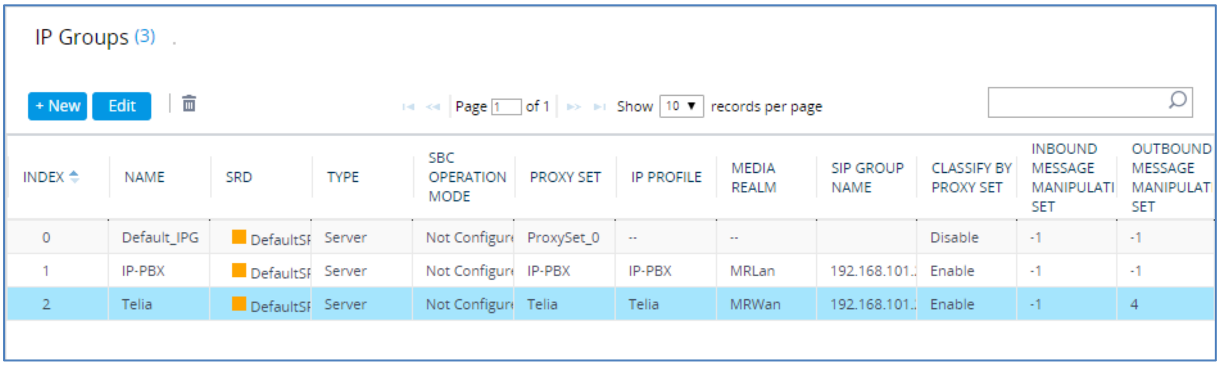
Parameter	Value
Index	**1**
Name	**IP-PBX**
Type	**Server**
Proxy Set	**IP-PBX**
IP Profile	**IP-PBX**
Media Realm	**MRLan**
SIP Group Name	(according to ITSP requirement)

3. Configure an IP Group for the Telia Entry SIP Trunk:

Parameter	Value
Index	**2**
Name	**Telia**
Topology Location	**Up**
Type	**Server**
Proxy Set	**Telia**
IP Profile	**Telia**
Media Realm	**MRWan**
SIP Group Name	(according to ITSP requirement)

The configured IP Groups are shown in the figure below:

Figure 4-16: Configured IP Groups in IP Group Table



IP Groups (3)

+ New Edit

Page 1 of 1 Show 10 records per page

INDEX	NAME	SRD	TYPE	SBC OPERATION MODE	PROXY SET	IP PROFILE	MEDIA REALM	SIP GROUP NAME	CLASSIFY BY PROXY SET	INBOUND MESSAGE MANIPULATI SET	OUTBOUND MESSAGE MANIPULAT SET
0	Default_IPG	DefaultSF	Server	Not Configur	ProxySet_0	--	--		Disable	-1	-1
1	IP-PBX	DefaultSF	Server	Not Configur	IP-PBX	IP-PBX	MRLan	192.168.101.	Enable	-1	-1
2	Telia	DefaultSF	Server	Not Configur	Telia	Telia	MRWan	192.168.101.	Enable	-1	4

4.8 Step 8: Configure Maximum IP Media Channels

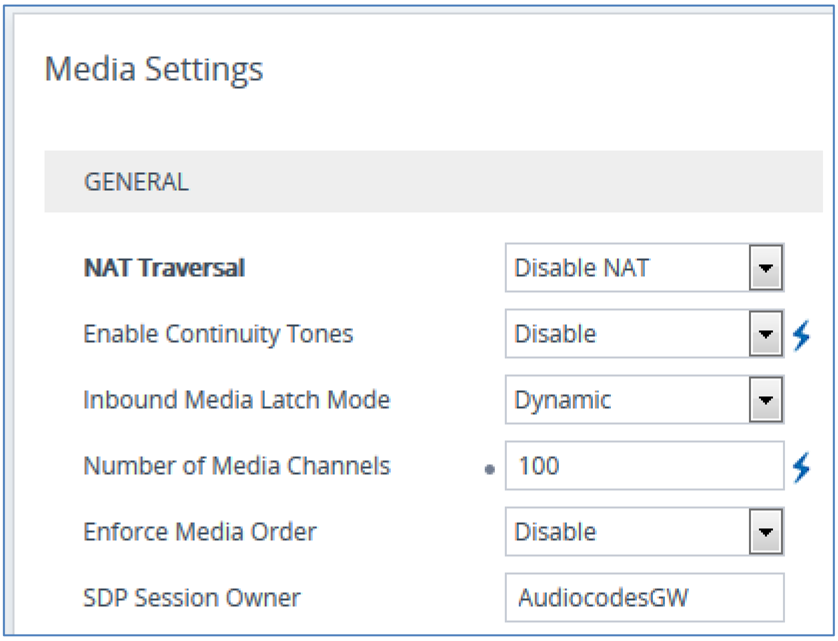
This step describes how to configure the maximum number of required IP media channels. The number of media channels represents the number of DSP channels that the E-SBC allocates to call sessions.

> **Note:** This step is required **only** if transcoding is required.

➢ **To configure the maximum number of IP media channels:**

1. Open the Media Settings page (**Setup** menu > **Signaling & Media** tab > **Media** folder > **Media Settings**).

Figure 4-17: Configuring Number of Media Channels



2. In the 'Number of Media Channels' field, enter the number of media channels according to your environments transcoding calls (e.g., **100**).
3. Click **Apply**.
4. Reset the E-SBC with a burn to flash for your settings to take effect (see Section 4.13 on page 51).

4.9 Step 9: Configure IP-to-IP Call Routing Rules

This step describes how to configure IP-to-IP call routing rules. These rules define the routes for forwarding SIP messages (e.g., INVITE) received from one IP entity to another. The E-SBC selects the rule whose configured input characteristics (e.g., IP Group) match those of the incoming SIP message. If the input characteristics do not match the first rule in the table, they are compared to the second rule, and so on, until a matching rule is located. If no rule is matched, the message is rejected. The routing rules use the configured IP Groups (as configured in Section 4.7 on page 28) to denote the source and destination of the call.

For the interoperability test topology, the following IP-to-IP routing rules need to be configured to route calls between IP-PBX (LAN) and Telia Entry SIP Trunk (DMZ):

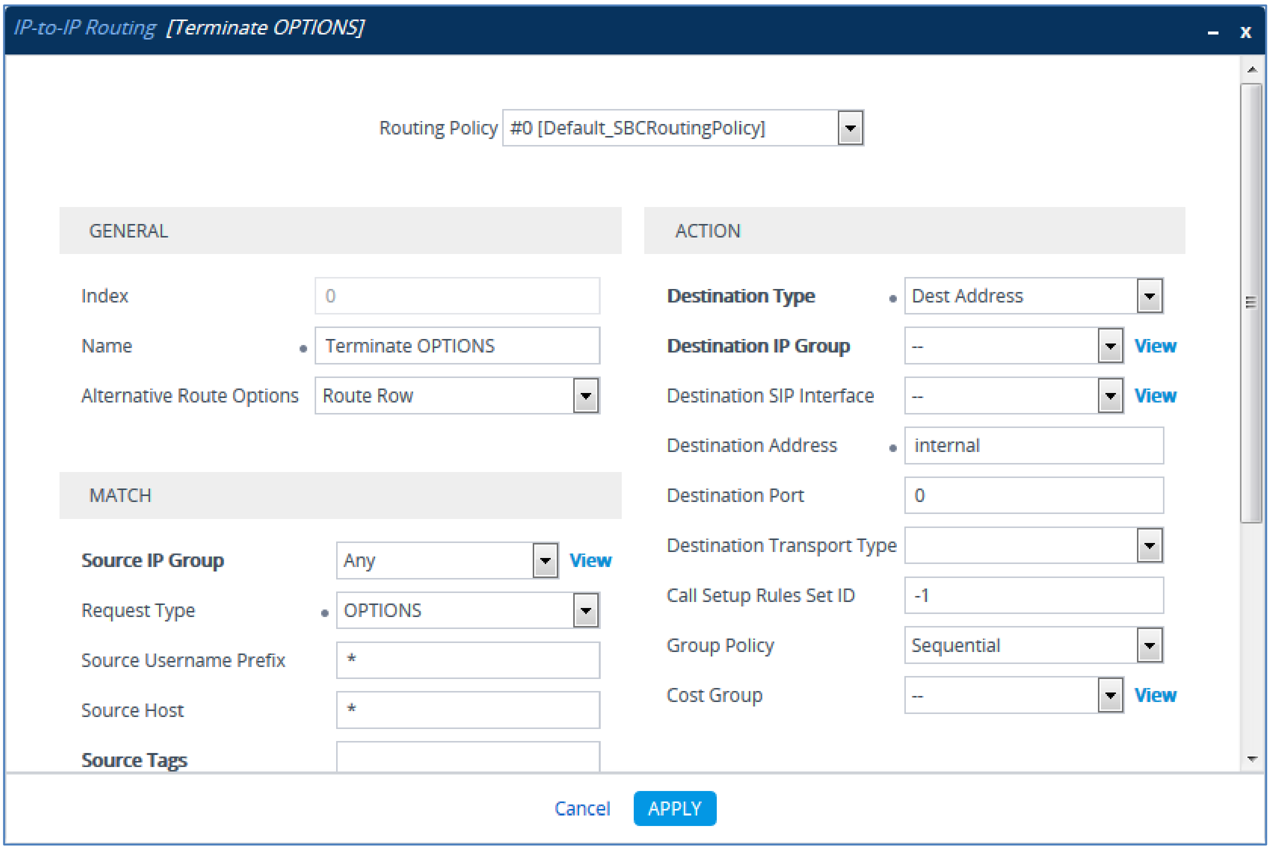
- Terminate SIP OPTIONS messages on the E-SBC that are received from the both LAN and DMZ
- Calls from IP-PBX to Telia Entry SIP Trunk
- Calls from Telia Entry SIP Trunk to IP-PBX

➢ **To configure IP-to-IP routing rules:**

1. Open the IP-to-IP Routing table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **IP-to-IP Routing**).
2. Configure a rule to terminate SIP OPTIONS messages received from the both LAN and DMZ:
   a. Click **New**, and then configure the parameters as follows:

Parameter	Value
Index	**0**
Name	**Terminate OPTIONS** (arbitrary descriptive name)
Source IP Group	**Any**
Request Type	**OPTIONS**
Destination Type	**Dest Address**
Destination Address	**internal**

Figure 4-18: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS

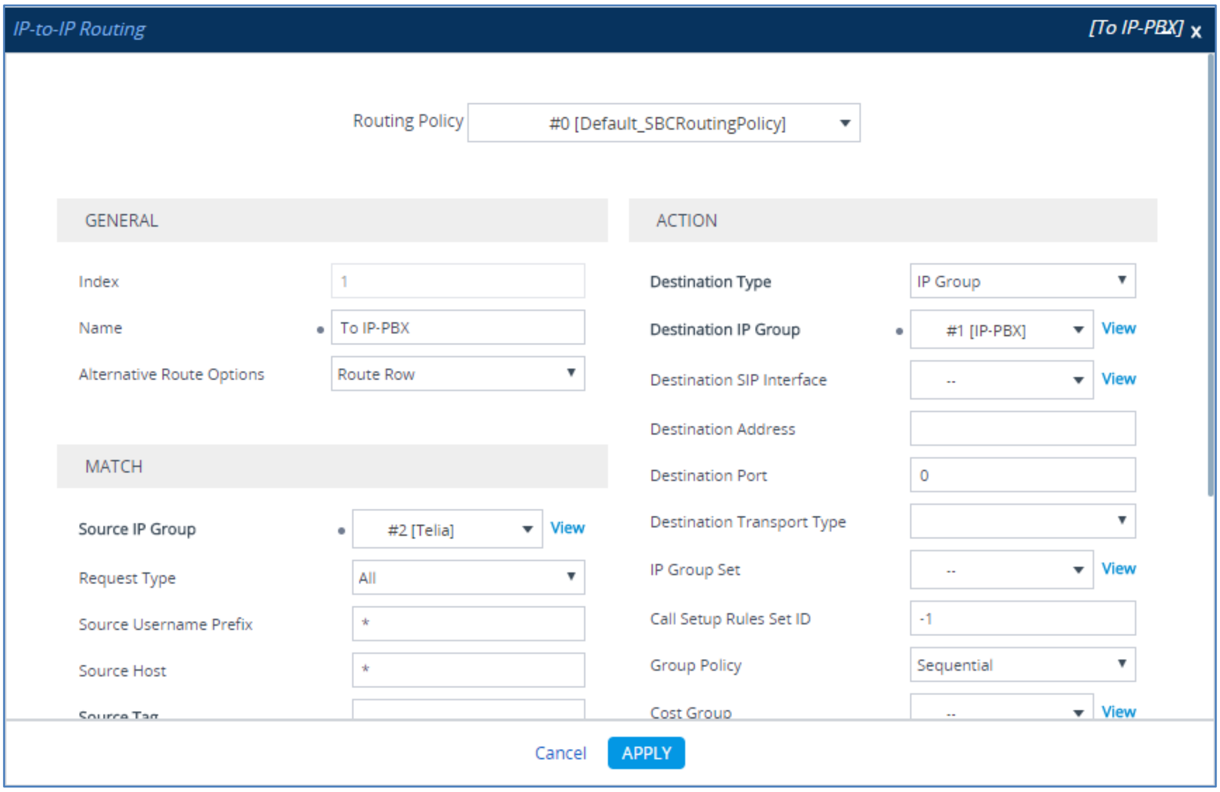


   b. Click **Apply**.

3. Configure rule to route calls from Telia Entry SIP Trunk to IP-PBX:
   a. Click **New**, and then configure the parameters as follows:

Parameter	Value
Index	**1**
Route Name	**To IP-PBX** (arbitrary descriptive name)
Source IP Group	**Telia**
Destination Type	**IP Group**
Destination IP Group	**IP-PBX**

Figure 4-19: Configuring IP-to-IP Routing Rule for ITSP to IP-PBX



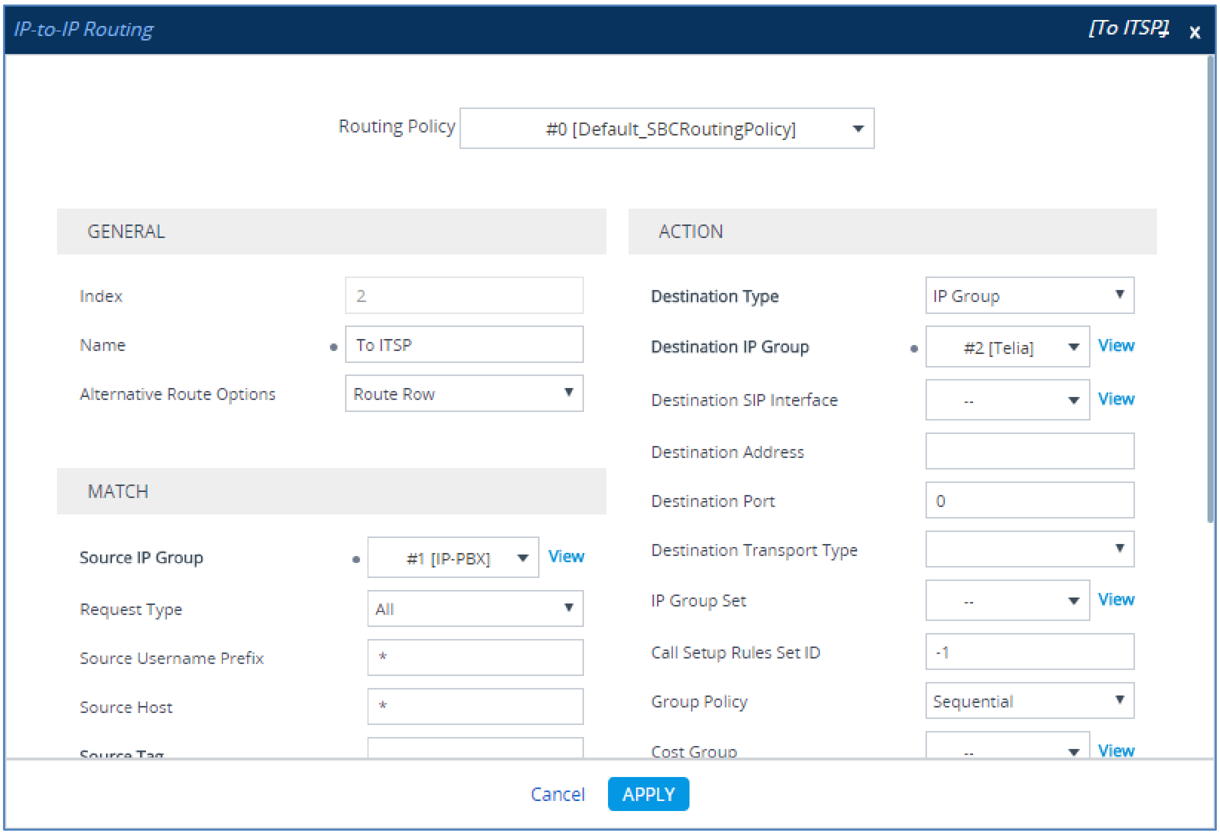
   b. Click **Apply**.

4. Configure a rule to route calls from IP-PBX to Telia Entry SIP Trunk:

a. Click **New**, and then configure the parameters as follows:

Parameter	Value
Index	**2**
Route Name	**To ITSP** (arbitrary descriptive name)
Source IP Group	**IP-PBX**
Destination Type	**IP Group**
Destination IP Group	**Telia**

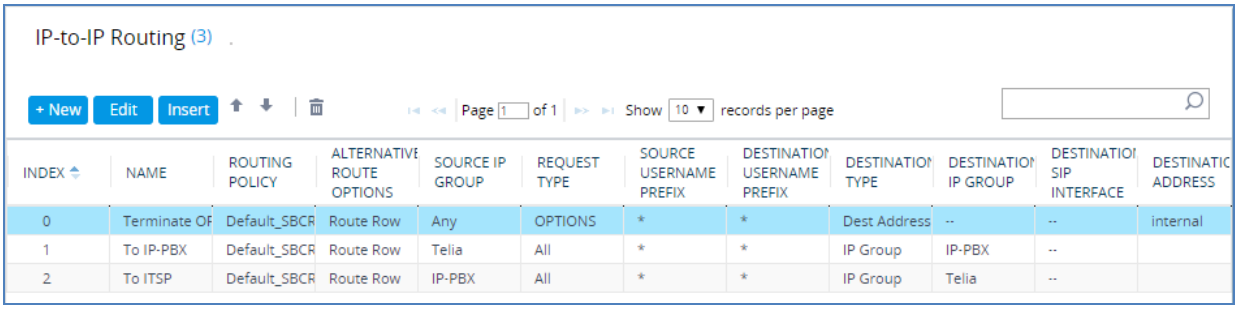
Figure 4-20: Configuring IP-to-IP Routing Rule for IP-PBX to ITSP



b. Click **Apply**.

The configured routing rules are shown in the figure below:

Figure 4-21: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table



INDEX	NAME	ROUTING POLICY	ALTERNATIVE ROUTE OPTIONS	SOURCE IP GROUP	REQUEST TYPE	SOURCE USERNAME PREFIX	DESTINATION USERNAME PREFIX	DESTINATION TYPE	DESTINATION IP GROUP	DESTINATION SIP INTERFACE	DESTINATION ADDRESS
0	Terminate OP	Default_SBCR	Route Row	Any	OPTIONS	*	*	Dest Address	--	--	internal
1	To IP-PBX	Default_SBCR	Route Row	Telia	All	*	*	IP Group	IP-PBX	--	
2	To ITSP	Default_SBCR	Route Row	IP-PBX	All	*	*	IP Group	Telia	--	

Note: The routing configuration may change according to your specific deployment topology.

4.10 Step 10: Configure IP-to-IP Manipulation Rules

This step describes how to configure IP-to-IP manipulation rules. These rules manipulate the SIP Request-URI user part (source or destination number). The manipulation rules use the configured IP Groups (as configured in Section 4.7 on page 28) to denote the source and destination of the call.

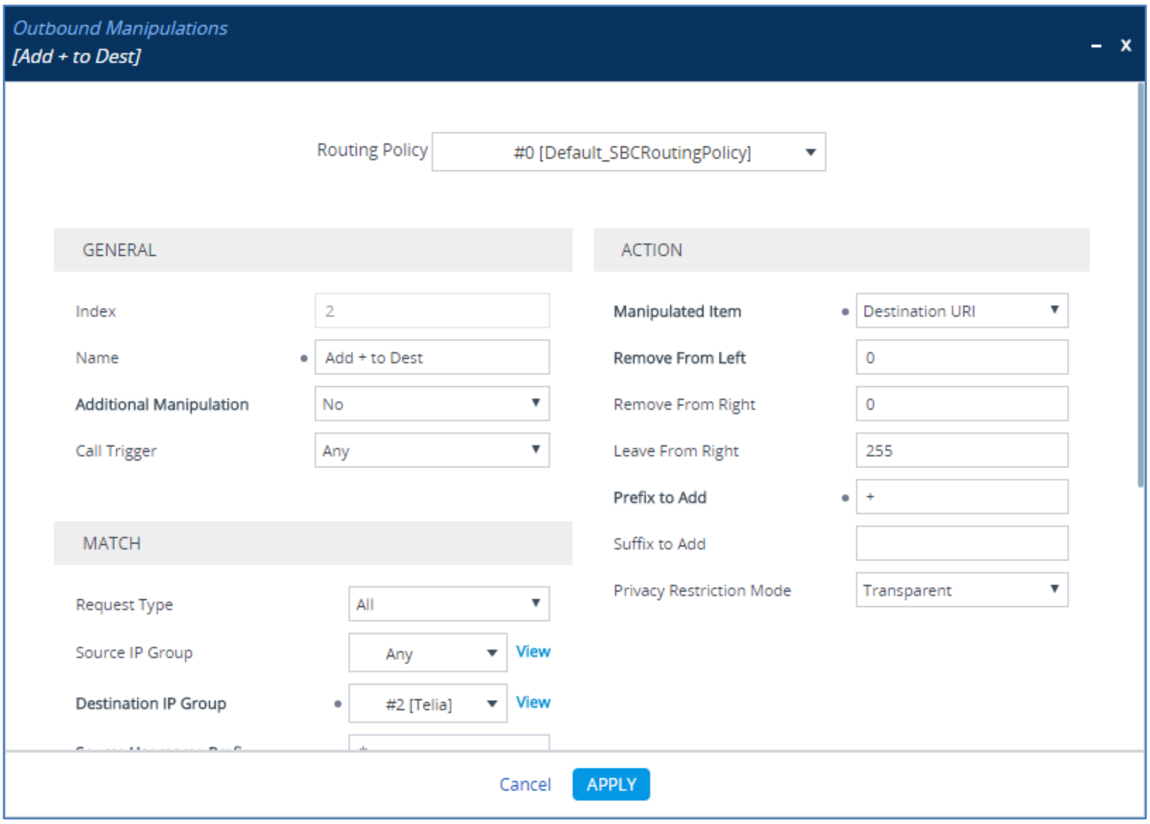
Note: Adapt the manipulation table according to your environment dial plan.

➢ **To configure a number manipulation rule:**

1. Open the Outbound Manipulations table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Manipulation** > **Outbound Manipulations**).
2. Click **New**, and then configure the parameters as follows:

Parameter	Value
Index	**2**
Name	**Add + to Dest**
Source IP Group	**Telia**
Destination IP Group	**IP-PBX**
Destination Username Prefix	***** (asterisk sign)
Manipulated Item	**Destination URI**
Prefix to Add	**+** (plus sign)

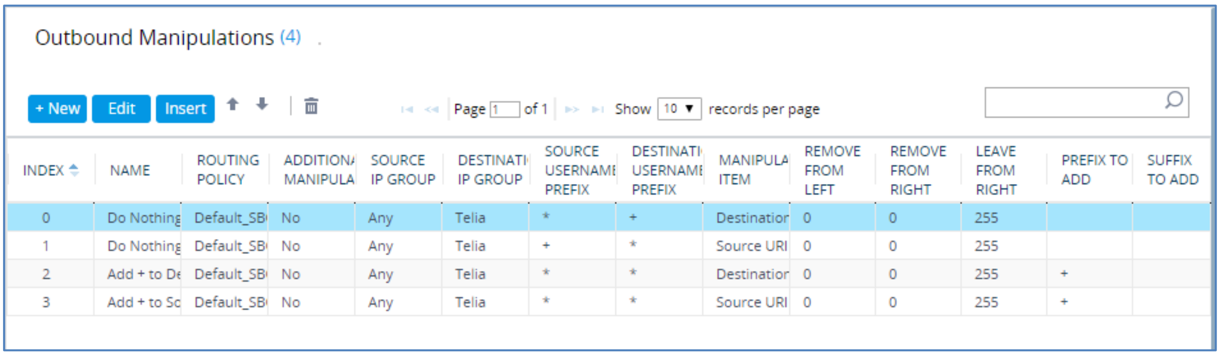
Figure 4-22: Configuring IP-to-IP Outbound Manipulation Rule



3. Click **Apply**.

The figure below shows an example of configured IP-to-IP outbound manipulation rules for calls between IP-PBX IP Group and Telia Entry SIP Trunk IP Group:

Figure 4-23: Example of Configured IP-to-IP Outbound Manipulation Rules



Rule Index	Description
0	Calls from any IP Group to ITSP IP Group with destination number prefix "+"; do nothing to the destination number.
1	Calls from any IP Group to ITSP IP Group with source number prefix "+"; do nothing to the source number.
2	For all other calls to ITSP IP Group, add the prefix "+" to the destination number.
3	For all other calls to ITSP IP Group, add the prefix "+" to the source number.

4.11 Step 11: Configure Message Manipulation Rules

This step describes how to configure SIP message manipulation rules. SIP message manipulation rules can include insertion, removal, and/or modification of SIP headers. Manipulation rules are grouped into Manipulation Sets, enabling you to apply multiple rules to the same SIP message (IP entity).

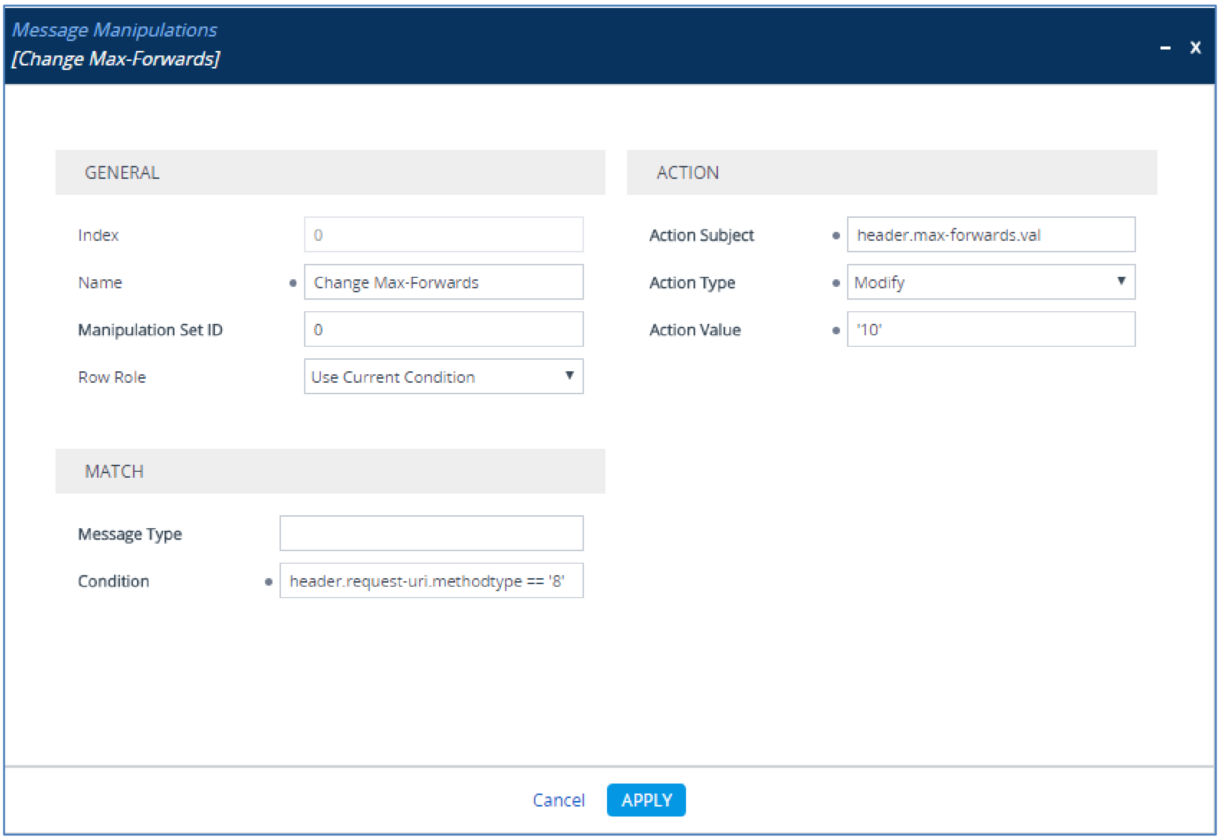
Once you have configured the SIP message manipulation rules, you need to assign them to the relevant IP Group (in the IP Group table) and determine whether they must be applied to inbound or outbound messages.

➢ **To configure SIP message manipulation rule:**

1. Open the Message Manipulations page (**Setup** menu > **Signaling & Media** tab > **Message Manipulation** folder > **Message Manipulations**).
2. Configure a new manipulation rule (Manipulation Set 0). This rule applies to OPTIONS messages received from the Telia Entry SIP Trunk IP Group. The Telia Entry SIP Trunk send OPTIONS messages with Max-Forwards=0, which cause error in the E-SBC. This rule replaces the value of the SIP Max-Forwards Header with the value '10'.

Parameter	Value
Index	**0**
Name	**Change Max-Forwards**
Manipulation Set ID	**0**
Condition	**header.request-uri.methodtype == '8'**
Action Subject	**header.max-forwards.val**
Action Type	**Modify**
Action Value	**'10'**

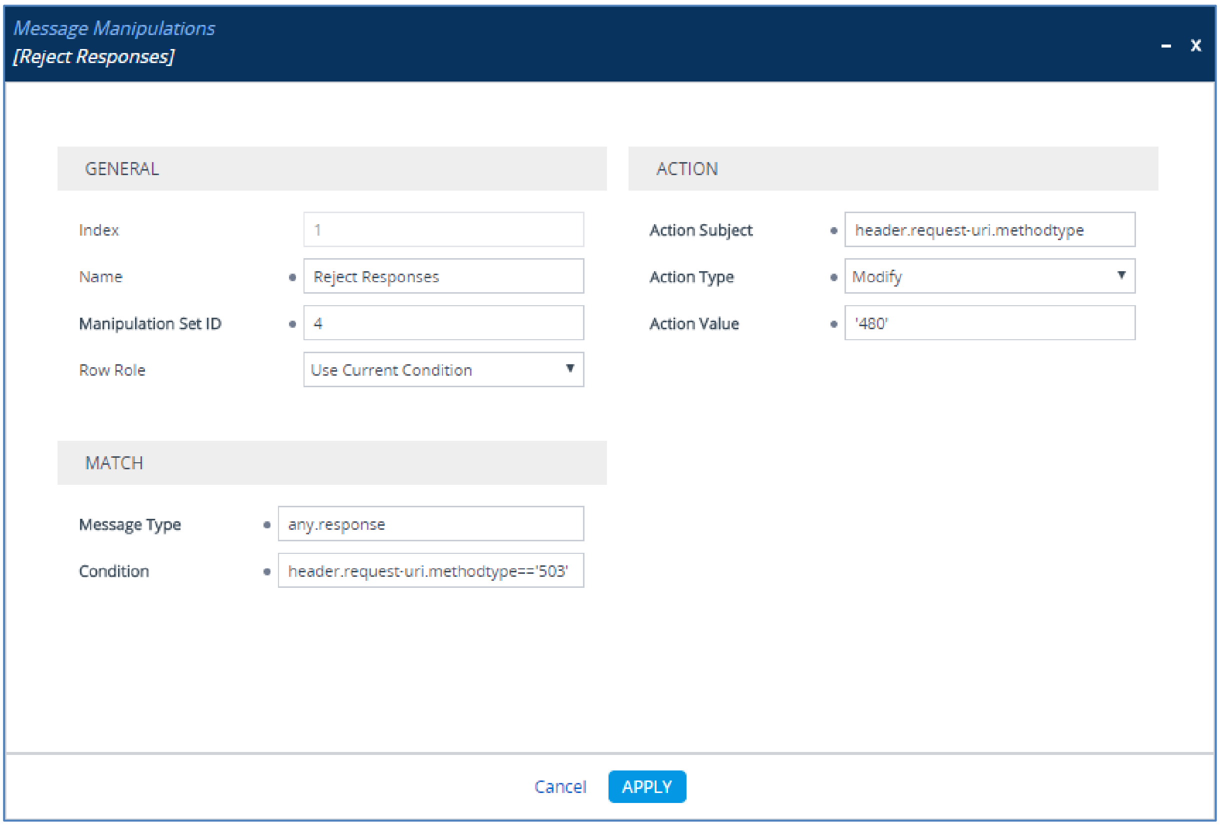
Figure 4-24: Configuring SIP Message Manipulation Rule 0 (from Telia Entry SIP Trunk)



3. Configure another manipulation rule (Manipulation Set 4) for Telia Entry SIP Trunk. This rule is applied to response messages sent to the Telia Entry SIP Trunk IP Group for Rejected Calls initiated by the IP-PBX IP Group. This replaces the method type ‘503’ with the value ‘480’, because Telia Entry SIP Trunk not recognizes ‘503’ method type.

Parameter	Value
Index	**1**
Name	**Reject Cause**
Manipulation Set ID	**4**
Message Type	**any.response**
Condition	**header.request-uri.methodtype=='503'**
Action Subject	**header.request-uri.methodtype**
Action Type	**Modify**
Action Value	**'480'**

Figure 4-25: Configuring SIP Message Manipulation Rule 1 (for Telia Entry SIP Trunk)



4. Configure another manipulation rule (Manipulation Set 4) for Telia Entry SIP Trunk. This rule applies to messages sent to the Telia Entry SIP Trunk IP Group in a call transfer scenario. This replaces the user part of the SIP P-Asserted-Identity Header with the value from the SIP Referred-By Header.

Parameter	Value
Index	**2**
Name	**Call Transfer**
Manipulation Set ID	**4**
Message Type	**any.request**
Condition	**header.referred-by exists**
Action Subject	**header.p-asserted-identity.url.user**
Action Type	**Modify**
Action Value	**header.referred-by.url.user**

Figure 4-26: Configuring SIP Message Manipulation Rule 2 (for Telia Entry SIP Trunk)

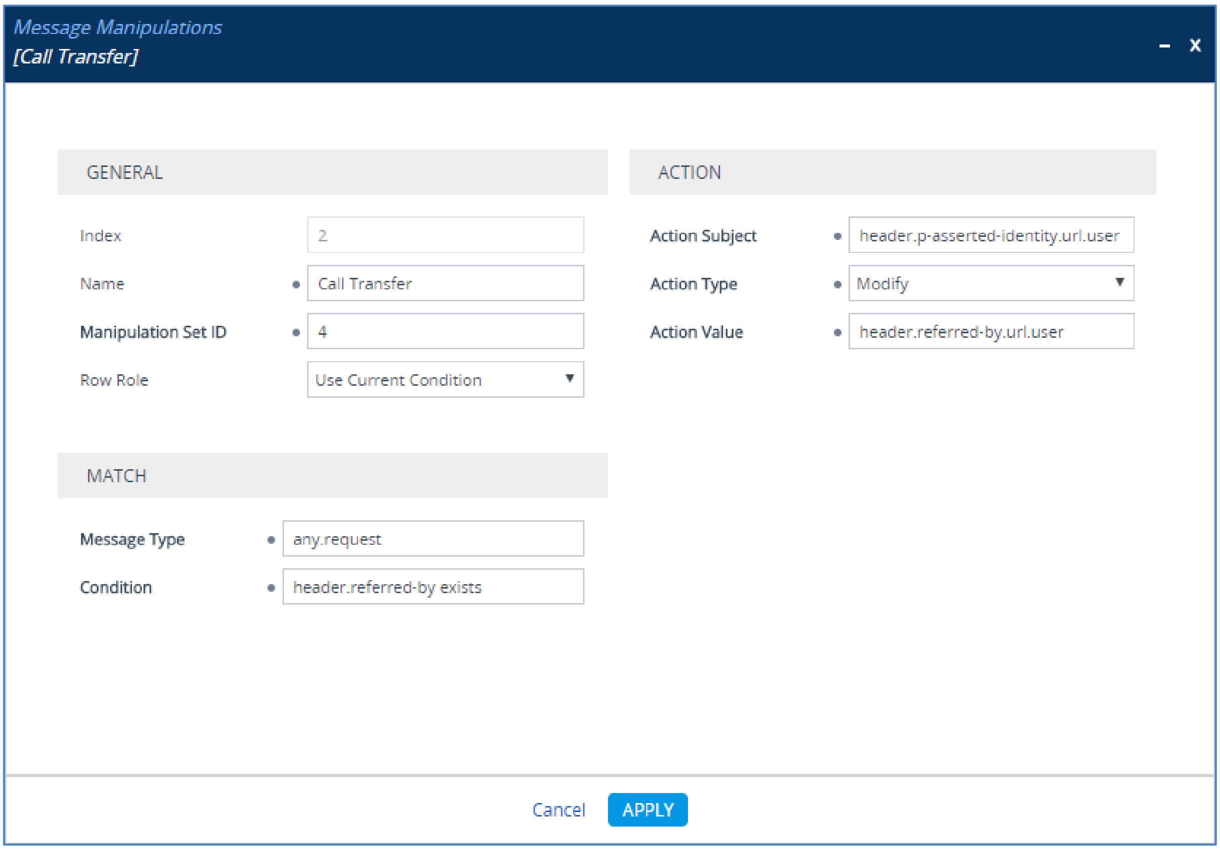
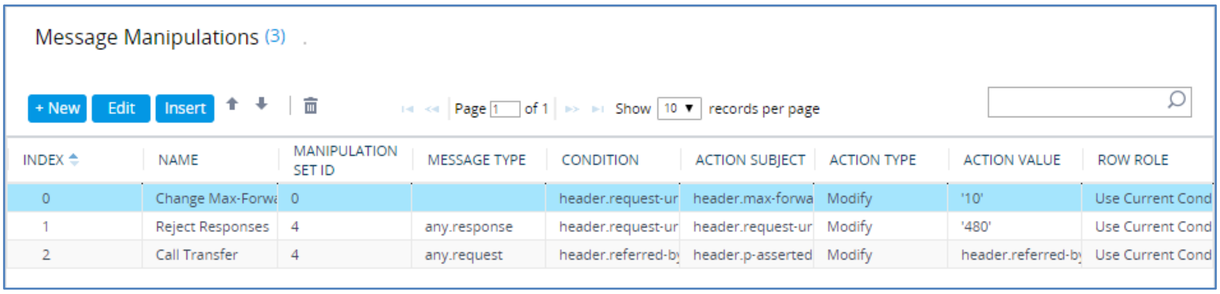


Figure 4-27: Example of Configured SIP Message Manipulation Rules

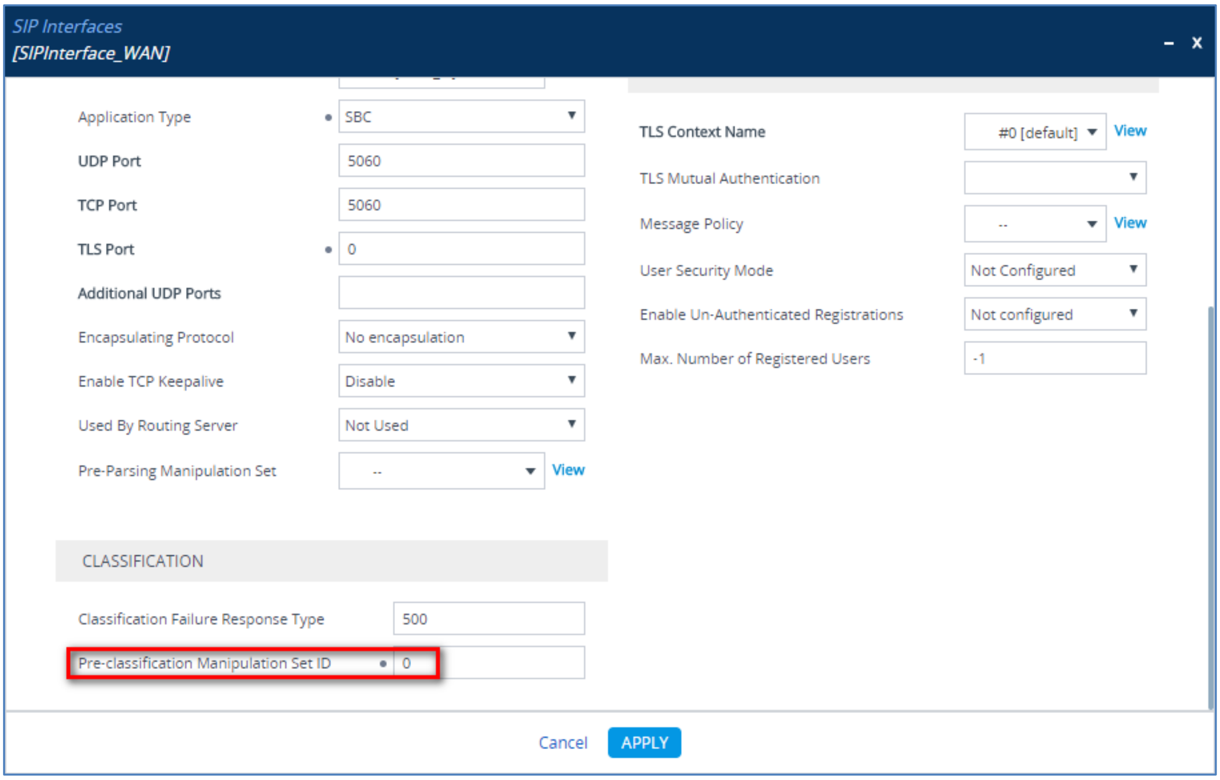


The table displayed below includes SIP message manipulation rules which are grouped together under Manipulation Set IDs (Manipulation Set IDs 0 and 4) and which are executed for messages sent to and from the Telia Entry SIP Trunk IP Group. These rules are specifically required to enable proper interworking between Telia Entry SIP Trunk and IP-PBX. Refer to the *User's Manual* for further details concerning the full capabilities of header manipulation.

Rule Index	Rule Description	Reason for Introducing Rule
0	This rule is applied to OPTIONS messages received from the Telia Entry SIP Trunk IP Group. This rule replaces the value of the SIP Max-Forwards Header with the value '10'.	The Telia Entry SIP Trunk sends OPTIONS messages with Max-Forwards=0, which causes errors in the E-SBC.
1	This rule is applied to response messages sent to the Telia Entry SIP Trunk IP Group for Rejected Calls initiated by the IP-PBX IP Group. This replaces the Method Type '503' with the value '480', because the Telia Entry SIP Trunk does not recognize the '503' Method Type.	
2	This rule is applied to messages sent to the Telia Entry SIP Trunk IP Group in a Call Transfer scenario. This replaces the **user** part of the SIP P-Asserted-Identity Header with the value from the SIP Referred-By Header.	Telia Entry SIP Trunk allows calls only from known numbers.

5. Assign Manipulation Set ID 0 to the WAN SIP Interface:
   a. Open the SIP Interface table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **SIP Interfaces**).
   b. Select the row of the WAN SIP Interface, and then click **Edit**.
   c. Set the 'Pre-classification Manipulation Set ID' field to **0**.

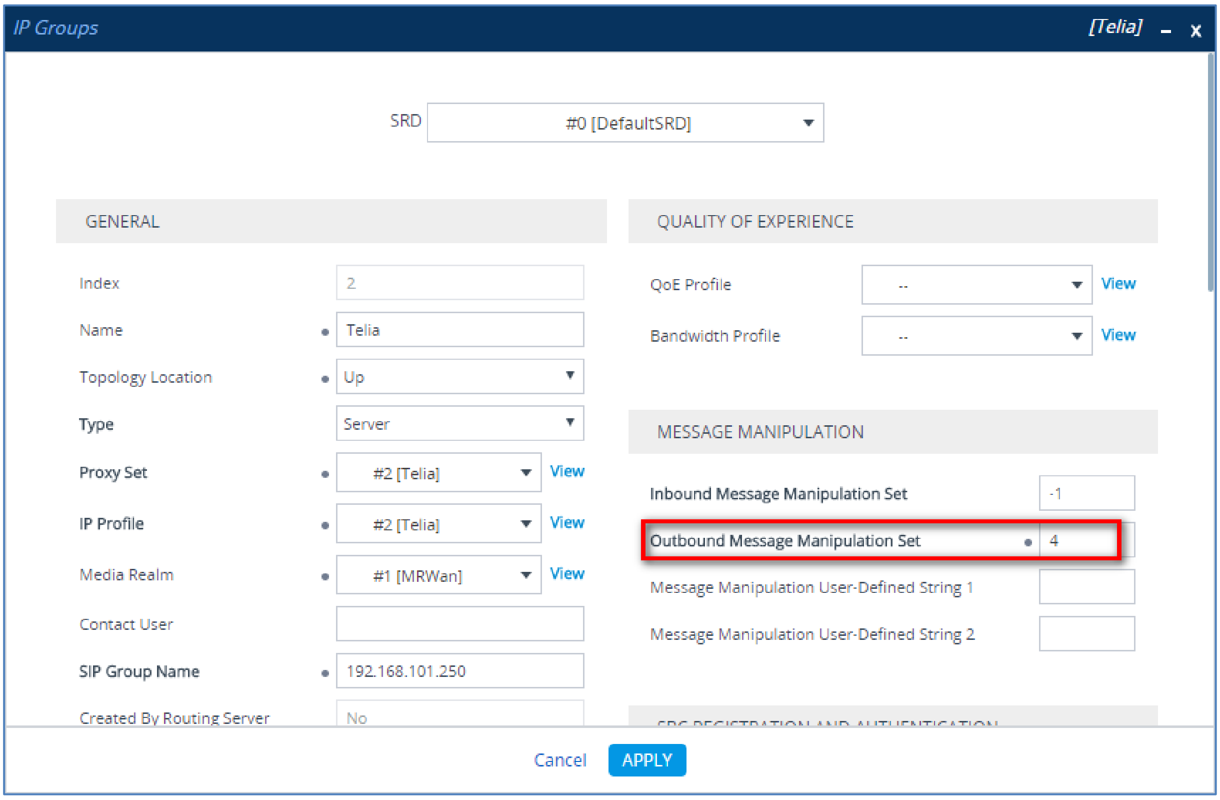
Figure 4-28: Assigning Manipulation Set to the WAN SIP Interface



   d. Click **Apply**.

6. Assign Manipulation Set ID 4 to the Telia Entry SIP trunk IP Group:
   a. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
   b. Select the row of the Telia Entry SIP trunk IP Group, and then click **Edit**.
   c. Set the 'Outbound Message Manipulation Set' field to **4**.

Figure 4-29: Assigning Manipulation Set 4 to the Telia Entry SIP Trunk IP Group



   d. Click **Apply**.

4.12 Step 12: Miscellaneous Configuration

This section describes miscellaneous E-SBC configuration.

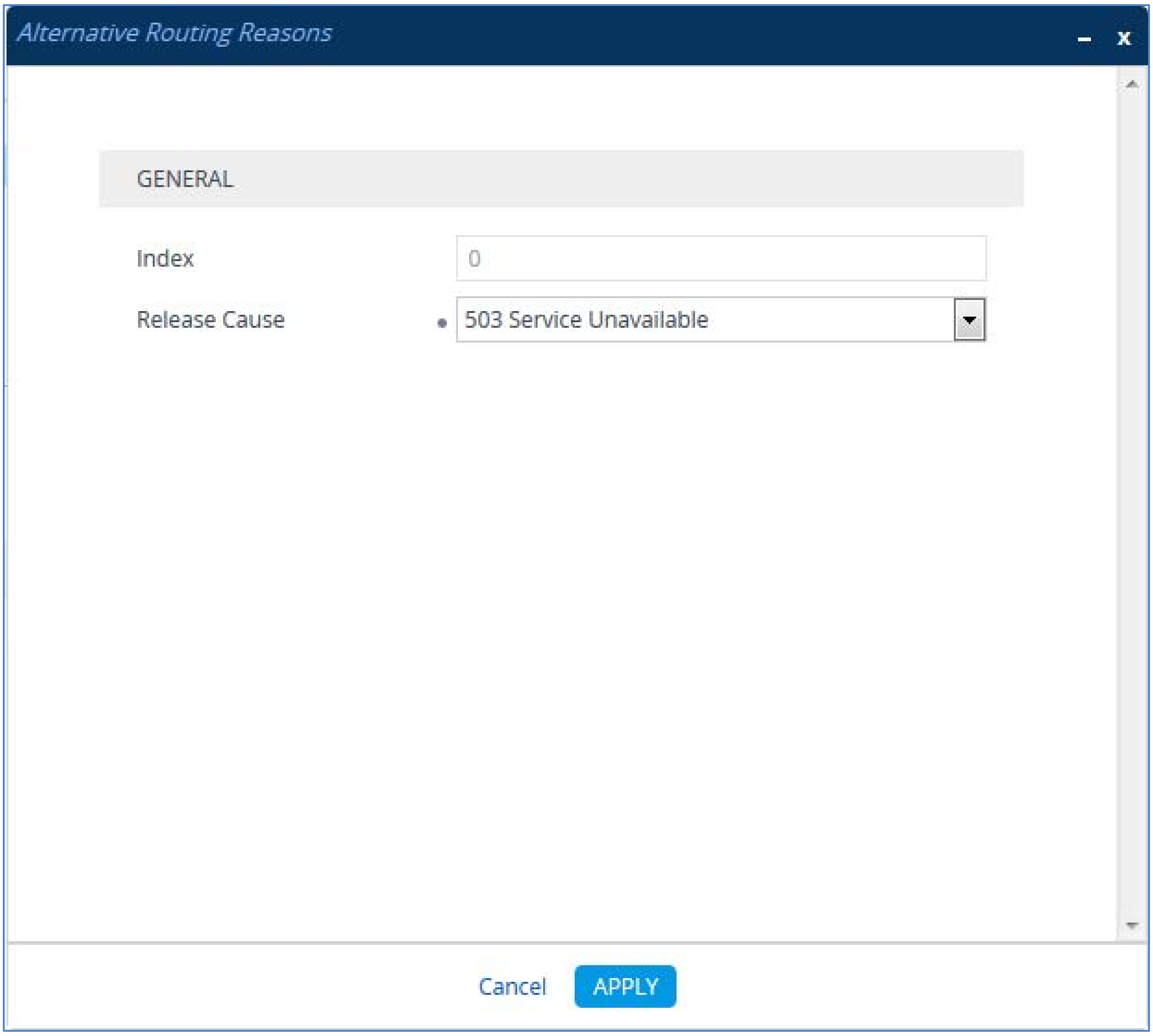
4.12.1 Step 12a: Configure SBC Alternative Routing Reasons

This step describes how to configure the E-SBC's handling of SIP 503 responses received for outgoing SIP dialog-initiating methods, e.g., INVITE, OPTIONS, and SUBSCRIBE messages. In this case E-SBC attempts to locate an alternative route for the call.

➢ **To configure SIP reason codes for alternative IP routing:**

1. Open the Alternative Routing Reasons table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **Alternative Reasons**).
2. Click **New**.
3. From the 'Release Cause' drop-down list, select **503 Service Unavailable**.

Figure 4-30: SBC Alternative Routing Reasons Table



4. Click **Apply**.

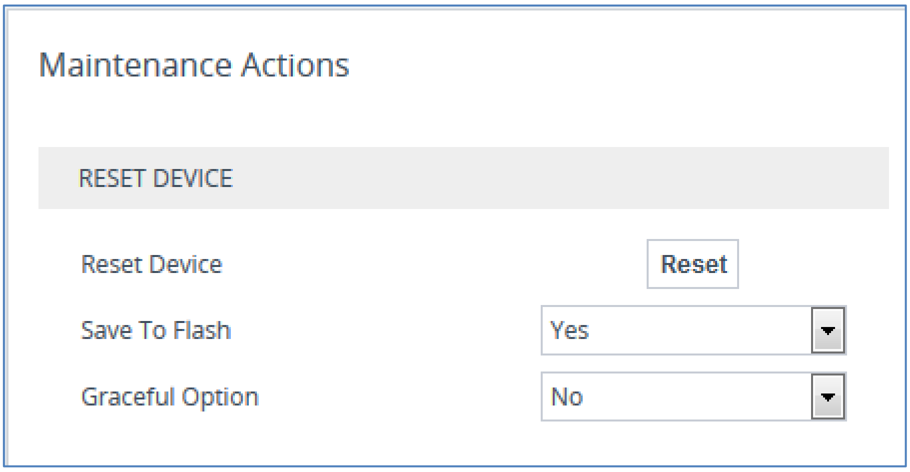
4.13 Step 13: Reset the E-SBC

After you have completed the configuration of the E-SBC described in this chapter, save ("burn") the configuration to the E-SBC's flash memory with a reset for the settings to take effect.

➢ **To reset the device through Web interface:**

1. Open the Maintenance Actions page (**Setup** menu > **Administration** tab > **Maintenance** folder > **Maintenance Actions**).

Figure 4-31: Resetting the E-SBC



2. Ensure that the ' Save To Flash' field is set to **Yes** (default).
3. Click the **Reset** button; a confirmation message box appears, requesting you to confirm.
4. Click **OK** to confirm device reset.

This page is intentionally left blank.

A AudioCodes INI File

The *ini* configuration file of the E-SBC, corresponding to the Web-based configuration as described in Section 4 on page 15, is shown below:

Note: To load or save an *ini* file, use the Configuration File page (**Setup** menu > **Administration** tab > **Maintenance** folder > **Configuration File**).

```
;**************
;** Ini File **
;**************

;Board: M800B
;HW Board Type: 69  FK Board Type: 72
;Serial Number: 8836505
;Slot Number: 1
;Software Version: 7.20A.158.009
;DSP Software Version: 5014AE3_R => 721.09
;Board IP Address: 192.168.7.100
;Board Subnet Mask: 255.255.255.0
;Board Default Gateway: 192.168.7.1
;Ram size: 512M   Flash size: 64M   Core speed: 500Mhz
;Num of DSP Cores: 3  Num DSP Channels: 150
;Num of physical LAN ports: 4
;Profile: NONE
;;;Key features:;Board Type: M800B ;DSP Voice features: IpmDetector RTCP-
XR ;PSTN Protocols: IUA=1 ;System features: HighPrecisionClock ;Security:
IPSEC MediaEncryption StrongEncryption EncryptControlProtocol ;IP Media:
VXML ;Coders: G723 G729 G728 NETCODER GSM-FR GSM-EFR AMR EVRC-QCELP G727
ILBC EVRC-B AMR-WB G722 EG711 MS_RTA_NB MS_RTA_WB SILK_NB SILK_WB
SPEEX_NB SPEEX_WB OPUS_NB OPUS_WB ;Channel Type: DspCh=150 ;E1Trunks=2
;T1Trunks=2 ;DATA features: ;Control Protocols: MGCP SIP SBC=150 MSFT
FEU=100 TestCall=100 ;Default features:;Coders: G711 G726;

;------  HW components------
;
; Slot # : Module type : # of ports
;----------------------------------------------
;      1 : FALC56      : 1
;      2 : FALC56      : 1
;      3 : Empty
;----------------------------------------------


[SYSTEM Params]

SyslogServerIP = 192.168.7.43
EnableSyslog = 1
;VpFileLastUpdateTime is hidden but has non-default value
TR069ACSPASSWORD = '$1$gQ=='
TR069CONNECTIONREQUESTPASSWORD = '$1$gQ=='
NTPServerIP = '0.0.0.0'
;LastConfigChangeTime is hidden but has non-default value
;BarrierFilename is hidden but has non-default value
```

```
;PM_gwINVITEDialogs is hidden but has non-default value
;PM_gwSUBSCRIBEDialogs is hidden but has non-default value
;PM_gwSBCRegisteredUsers is hidden but has non-default value
;PM_gwSBCMediaLegs is hidden but has non-default value
;PM_gwSBCTranscodingSessions is hidden but has non-default value

[BSP Params]

PCMLawSelect = 3
UdpPortSpacing = 10
EnterCpuOverloadPercent = 99
ExitCpuOverloadPercent = 95

[Analog Params]


[ControlProtocols Params]

AdminStateLockControl = 0

[MGCP Params]


[MEGACO Params]


[PSTN Params]


[SS7 Params]


[Voice Engine Params]

CallProgressTonesFilename = 'usa_tones_13.dat'

[WEB Params]

LogoWidth = '145'
HTTPSCipherString = 'RC4:EXP'
;HTTPSPkeyFileName is hidden but has non-default value
;HTTPSCertFileName is hidden but has non-default value

[SIP Params]

GWDEBUGLEVEL = 5
ENABLESBCAPPLICATION = 1
MSLDAPPRIMARYKEY = 'telephoneNumber'
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 10486144
;GWAPPCONFIGURATIONVERSION is hidden but has non-default value

[IPsec Params]


[SNMP Params]
```

```
[ PhysicalPortsTable ]

FORMAT PhysicalPortsTable_Index = PhysicalPortsTable_Port,
PhysicalPortsTable_Mode, PhysicalPortsTable_SpeedDuplex,
PhysicalPortsTable_PortDescription, PhysicalPortsTable_GroupMember,
PhysicalPortsTable_GroupStatus;
PhysicalPortsTable 0 = "GE_4_1", 1, 4, "User Port #0", "GROUP_1",
"Active";
PhysicalPortsTable 1 = "GE_4_2", 1, 4, "User Port #1", "GROUP_1",
"Redundant";
PhysicalPortsTable 2 = "GE_4_3", 1, 4, "User Port #2", "GROUP_2",
"Active";
PhysicalPortsTable 3 = "GE_4_4", 1, 4, "User Port #3", "GROUP_2",
"Redundant";

[ \PhysicalPortsTable ]


[ EtherGroupTable ]

FORMAT EtherGroupTable_Index = EtherGroupTable_Group,
EtherGroupTable_Mode, EtherGroupTable_Member1, EtherGroupTable_Member2;
EtherGroupTable 0 = "GROUP_1", 2, "GE_4_1", "GE_4_2";
EtherGroupTable 1 = "GROUP_2", 2, "GE_4_3", "GE_4_4";
EtherGroupTable 2 = "GROUP_3", 0, "", "";
EtherGroupTable 3 = "GROUP_4", 0, "", "";

[ \EtherGroupTable ]


[ DeviceTable ]

FORMAT DeviceTable_Index = DeviceTable_VlanID,
DeviceTable_UnderlyingInterface, DeviceTable_DeviceName,
DeviceTable_Tagging, DeviceTable_MTU;
DeviceTable 0 = 1, "GROUP_1", "vlan 1", 0, 1500;
DeviceTable 1 = 2, "GROUP_2", "vlan 2", 0, 1500;

[ \DeviceTable ]


[ InterfaceTable ]

FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_InterfaceName, InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress,
InterfaceTable_UnderlyingDevice;
InterfaceTable 0 = 6, 10, 10.15.77.55, 16, 10.15.0.1, "LAN_IF",
10.15.27.1, , "vlan 1";
InterfaceTable 1 = 5, 10, 192.168.101.250, 24, 192.168.101.100, "WAN_IF",
8.8.8.8, 0.0.0.0, "vlan 2";

[ \InterfaceTable ]
```

```
[ WebUsers ]

FORMAT WebUsers_Index = WebUsers_Username, WebUsers_Password,
WebUsers_Status, WebUsers_PwAgeInterval, WebUsers_SessionLimit,
WebUsers_CliSessionLimit, WebUsers_SessionTimeout, WebUsers_BlockTime,
WebUsers_UserLevel, WebUsers_PwNonce, WebUsers_SSHPublicKey;
WebUsers 0 = "Admin",
"$1$c0REQxAWThwcHkkZTR61uLGxtLLk5b6767zvurq99aLzp6ai8vb9qKqi/66mp8GYlJLHw
cKRzJ+Sk82Vz5rVhtQ=", 1, 0, 5, -1, 15, 60, 200,
"0967786edab8c9e919e3bc14bb8124f9", "";
WebUsers 1 = "User",
"$1$YldUBQYHUQpcWAgJCVwOE0dDEEcTRRJPT0oYHR4bSrXgsOK9t+K+ubm/u7zp6uyipqb29
/Hzpvqqqfio+/r5wZY=", 1, 0, 5, -1, 15, 60, 50,
"f859b36258b753dfed42049e58b68971", "";

[ \WebUsers ]


[ TLSContexts ]

FORMAT TLSContexts_Index = TLSContexts_Name, TLSContexts_TLSVersion,
TLSContexts_DTLSVersion, TLSContexts_ServerCipherString,
TLSContexts_ClientCipherString, TLSContexts_RequireStrictCert,
TLSContexts_OcspEnable, TLSContexts_OcspServerPrimary,
TLSContexts_OcspServerSecondary, TLSContexts_OcspServerPort,
TLSContexts_OcspDefaultResponse, TLSContexts_DHKeySize;
TLSContexts 0 = "default", 0, 0, "RC4:AES128", "DEFAULT", 0, 0, , , 2560,
0, 1024;

[ \TLSContexts ]


[ AudioCodersGroups ]

FORMAT AudioCodersGroups_Index = AudioCodersGroups_Name;
AudioCodersGroups 0 = "AudioCodersGroups_0";

[ \AudioCodersGroups ]


[ IpProfile ]

FORMAT IpProfile_Index = IpProfile_ProfileName, IpProfile_IpPreference,
IpProfile_CodersGroupName, IpProfile_IsFaxUsed,
IpProfile_JitterBufMinDelay, IpProfile_JitterBufOptFactor,
IpProfile_IPDiffServ, IpProfile_SigIPDiffServ,
IpProfile_RTPRedundancyDepth, IpProfile_CNGmode,
IpProfile_VxxTransportType, IpProfile_NSEMode, IpProfile_IsDTMFUsed,
IpProfile_PlayRBTone2IP, IpProfile_EnableEarlyMedia,
IpProfile_ProgressIndicator2IP, IpProfile_EnableEchoCanceller,
IpProfile_CopyDest2RedirectNumber, IpProfile_MediaSecurityBehaviour,
IpProfile_CallLimit, IpProfile_DisconnectOnBrokenConnection,
IpProfile_FirstTxDtmfOption, IpProfile_SecondTxDtmfOption,
IpProfile_RxDTMFOption, IpProfile_EnableHold, IpProfile_InputGain,
IpProfile_VoiceVolume, IpProfile_AddIEInSetup,
IpProfile_SBCExtensionCodersGroupName,
IpProfile_MediaIPVersionPreference, IpProfile_TranscodingMode,
IpProfile_SBCAllowedMediaTypes, IpProfile_SBCAllowedAudioCodersGroupName,
IpProfile_SBCAllowedVideoCodersGroupName, IpProfile_SBCAllowedCodersMode,
IpProfile_SBCMediaSecurityBehaviour, IpProfile_SBCRFC2833Behavior,
IpProfile_SBCAlternativeDTMFMethod, IpProfile_SBCSendMultipleDTMFMethods,
IpProfile_SBCAssertIdentity, IpProfile_AMDSensitivityParameterSuit,
```

```
IpProfile_AMDSensitivityLevel, IpProfile_AMDMaxGreetingTime,
IpProfile_AMDMaxPostSilenceGreetingTime, IpProfile_SBCDiversionMode,
IpProfile_SBCHistoryInfoMode, IpProfile_EnableQSIGTunneling,
IpProfile_SBCFaxCodersGroupName, IpProfile_SBCFaxBehavior,
IpProfile_SBCFaxOfferMode, IpProfile_SBCFaxAnswerMode,
IpProfile_SbcPrackMode, IpProfile_SBCSessionExpiresMode,
IpProfile_SBCRemoteUpdateSupport, IpProfile_SBCRemoteReinviteSupport,
IpProfile_SBCRemoteDelayedOfferSupport, IpProfile_SBCRemoteReferBehavior,
IpProfile_SBCRemote3xxBehavior, IpProfile_SBCRemoteMultiple18xSupport,
IpProfile_SBCRemoteEarlyMediaResponseType,
IpProfile_SBCRemoteEarlyMediaSupport, IpProfile_EnableSymmetricMKI,
IpProfile_MKISize, IpProfile_SBCEnforceMKISize,
IpProfile_SBCRemoteEarlyMediaRTP, IpProfile_SBCRemoteSupportsRFC3960,
IpProfile_SBCRemoteCanPlayRingback, IpProfile_EnableEarly183,
IpProfile_EarlyAnswerTimeout, IpProfile_SBC2833DTMFPayloadType,
IpProfile_SBCUserRegistrationTime, IpProfile_ResetSRTPStateUponRekey,
IpProfile_AmdMode, IpProfile_SBCReliableHeldToneSource,
IpProfile_GenerateSRTPKeys, IpProfile_SBCPlayHeldTone,
IpProfile_SBCRemoteHoldFormat, IpProfile_SBCRemoteReplacesBehavior,
IpProfile_SBCSDPPtimeAnswer, IpProfile_SBCPreferredPTime,
IpProfile_SBCUseSilenceSupp, IpProfile_SBCRTPRedundancyBehavior,
IpProfile_SBCPlayRBTToTransferee, IpProfile_SBCRTCPMode,
IpProfile_SBCJitterCompensation,
IpProfile_SBCRemoteRenegotiateOnFaxDetection,
IpProfile_JitterBufMaxDelay,
IpProfile_SBCUserBehindUdpNATRegistrationTime,
IpProfile_SBCUserBehindTcpNATRegistrationTime,
IpProfile_SBCSDPHandleRTCPAttribute,
IpProfile_SBCRemoveCryptoLifetimeInSDP, IpProfile_SBCIceMode,
IpProfile_SBCRTCPMux, IpProfile_SBCMediaSecurityMethod,
IpProfile_SBCHandleXDetect, IpProfile_SBCRTCPFeedback,
IpProfile_SBCRemoteRepresentationMode, IpProfile_SBCKeepVIAHeaders,
IpProfile_SBCKeepRoutingHeaders, IpProfile_SBCKeepUserAgentHeader,
IpProfile_SBCRemoteMultipleEarlyDialogs,
IpProfile_SBCRemoteMultipleAnswersMode, IpProfile_SBCDirectMediaTag,
IpProfile_SBCAdaptRFC2833BWToVoiceCoderBW,
IpProfile_CreatedByRoutingServer, IpProfile_SBCFaxReroutingMode,
IpProfile_SBCMaxCallDuration, IpProfile_SBCGenerateRTP,
IpProfile_SBCISUPBodyHandling, IpProfile_SBCISUPVariant,
IpProfile_SBCVoiceQualityEnhancement, IpProfile_SBCMaxOpusBW,
IpProfile_LocalRingbackTone, IpProfile_LocalHeldTone;
IpProfile 1 = "IP-PBX", 1, "AudioCodersGroups_0", 0, 10, 10, 46, 24, 0,
0, 0, 0, 0, 0, 0, -1, 1, 0, 0, -1, 0, 4, -1, 1, 1, 0, 0, "", "", 0, 0,
"", "", "", 0, 2, 0, 0, 0, 0, 0, 8, 300, 400, 0, 0, 0, "", 0, 0, 1, 3, 0,
2, 2, 1, 3, 2, 1, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0,
0, 0, 0, 0, 0, 0, 0, 0, 0, 300, -1, -1, 0, 0, 0, 0, 0, 0, 0, -1, -1, -1,
-1, -1, 0, "", 0, 0, 0, 0, 0, 0, 0, 0, 0, -1, -1;
IpProfile 2 = "Telia", 1, "AudioCodersGroups_0", 0, 10, 10, 46, 24, 0, 0,
0, 0, 0, 0, 0, -1, 1, 0, 0, -1, 0, 4, -1, 1, 1, 0, 0, "", "", 0, 0, "",
"", "", 0, 2, 0, 0, 0, 1, 0, 8, 300, 400, 0, 0, 0, "", 0, 0, 1, 3, 0, 2,
2, 0, 3, 2, 1, 0, 1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0,
0, 0, 0, 0, 1, 0, 0, 0, 300, -1, -1, 0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1,
-1, 0, "", 0, 0, 0, 0, 0, 0, 0, 0, 0, -1, -1;

[ \IpProfile ]


[ CpMediaRealm ]

FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName,
CpMediaRealm_IPv4IF, CpMediaRealm_IPv6IF, CpMediaRealm_PortRangeStart,
CpMediaRealm_MediaSessionLeg, CpMediaRealm_PortRangeEnd,
CpMediaRealm_IsDefault, CpMediaRealm_QoeProfile, CpMediaRealm_BWProfile,
CpMediaRealm_TopologyLocation;
CpMediaRealm 0 = "MRLan", "LAN_IF", "", 6000, 100, 6999, 0, "", "", 0;
```

```
CpMediaRealm 1 = "MRWan", "WAN_IF", "", 7000, 100, 7999, 0, "", "", 1;

[ \CpMediaRealm ]


[ SBCRoutingPolicy ]

FORMAT SBCRoutingPolicy_Index = SBCRoutingPolicy_Name,
SBCRoutingPolicy_LCREnable, SBCRoutingPolicy_LCRAverageCallLength,
SBCRoutingPolicy_LCRDefaultCost, SBCRoutingPolicy_LdapServerGroupName;
SBCRoutingPolicy 0 = "Default_SBCRoutingPolicy", 0, 1, 1, "";

[ \SBCRoutingPolicy ]


[ SRD ]

FORMAT SRD_Index = SRD_Name, SRD_BlockUnRegUsers, SRD_MaxNumOfRegUsers,
SRD_EnableUnAuthenticatedRegistrations, SRD_SharingPolicy,
SRD_UsedByRoutingServer, SRD_SBCOperationMode, SRD_SBCRoutingPolicyName,
SRD_SBCDialPlanName;
SRD 0 = "DefaultSRD", 0, -1, 1, 0, 0, 0, "Default_SBCRoutingPolicy", "";

[ \SRD ]


[ MessagePolicy ]

FORMAT MessagePolicy_Index = MessagePolicy_Name,
MessagePolicy_MaxMessageLength, MessagePolicy_MaxHeaderLength,
MessagePolicy_MaxBodyLength, MessagePolicy_MaxNumHeaders,
MessagePolicy_MaxNumBodies, MessagePolicy_SendRejection,
MessagePolicy_MethodList, MessagePolicy_MethodListType,
MessagePolicy_BodyList, MessagePolicy_BodyListType,
MessagePolicy_UseMaliciousSignatureDB;
MessagePolicy 0 = "Malicious Signature DB Protection", -1, -1, -1, -1, -
1, 1, "", 0, "", 0, 1;

[ \MessagePolicy ]


[ SIPInterface ]

FORMAT SIPInterface_Index = SIPInterface_InterfaceName,
SIPInterface_NetworkInterface, SIPInterface_ApplicationType,
SIPInterface_UDPPort, SIPInterface_TCPPort, SIPInterface_TLSPort,
SIPInterface_AdditionalUDPPorts, SIPInterface_SRDName,
SIPInterface_MessagePolicyName, SIPInterface_TLSContext,
SIPInterface_TLSMutualAuthentication, SIPInterface_TCPKeepaliveEnable,
SIPInterface_ClassificationFailureResponseType,
SIPInterface_PreClassificationManSet, SIPInterface_EncapsulatingProtocol,
SIPInterface_MediaRealm, SIPInterface_SBCDirectMedia,
SIPInterface_BlockUnRegUsers, SIPInterface_MaxNumOfRegUsers,
SIPInterface_EnableUnAuthenticatedRegistrations,
SIPInterface_UsedByRoutingServer, SIPInterface_TopologyLocation,
SIPInterface_PreParsingManSetName;
SIPInterface 0 = "SIPInterface_LAN", "LAN_IF", 2, 5060, 5070, 0, "",
"DefaultSRD", "", "default", -1, 0, 500, -1, 0, "MRLan", 0, -1, -1, -1,
0, 0, "";
```

```
SIPInterface 1 = "SIPInterface_WAN", "WAN_IF", 2, 5060, 5060, 0, "",
"DefaultSRD", "", "default", -1, 0, 500, 0, 0, "MRWan", 0, -1, -1, -1, 0,
1, "";

[ \SIPInterface ]


[ ProxySet ]

FORMAT ProxySet_Index = ProxySet_ProxyName,
ProxySet_EnableProxyKeepAlive, ProxySet_ProxyKeepAliveTime,
ProxySet_ProxyLoadBalancingMethod, ProxySet_IsProxyHotSwap,
ProxySet_SRDName, ProxySet_ClassificationInput, ProxySet_TLSContextName,
ProxySet_ProxyRedundancyMode, ProxySet_DNSResolveMethod,
ProxySet_KeepAliveFailureResp, ProxySet_GWIPv4SIPInterfaceName,
ProxySet_SBCIPv4SIPInterfaceName, ProxySet_GWIPv6SIPInterfaceName,
ProxySet_SBCIPv6SIPInterfaceName, ProxySet_MinActiveServersLB,
ProxySet_SuccessDetectionRetries, ProxySet_SuccessDetectionInterval,
ProxySet_FailureDetectionRetransmissions;
ProxySet 0 = "ProxySet_0", 0, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "",
"", "SIPInterface_LAN", "", "", 1, 1, 10, -1;
ProxySet 1 = "IP-PBX", 1, 60, 0, 0, "DefaultSRD", 1, "", -1, -1, "", "",
"SIPInterface_LAN", "", "", 1, 1, 10, -1;
ProxySet 2 = "Telia", 1, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "", "",
"SIPInterface_WAN", "", "", 1, 1, 10, -1;

[ \ProxySet ]


[ IPGroup ]

FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Name, IPGroup_ProxySetName,
IPGroup_SIPGroupName, IPGroup_ContactUser, IPGroup_SipReRoutingMode,
IPGroup_AlwaysUseRouteTable, IPGroup_SRDName, IPGroup_MediaRealm,
IPGroup_ClassifyByProxySet, IPGroup_ProfileName,
IPGroup_MaxNumOfRegUsers, IPGroup_InboundManSet, IPGroup_OutboundManSet,
IPGroup_RegistrationMode, IPGroup_AuthenticationMode, IPGroup_MethodList,
IPGroup_EnableSBCClientForking, IPGroup_SourceUriInput,
IPGroup_DestUriInput, IPGroup_ContactName, IPGroup_Username,
IPGroup_Password, IPGroup_UUIFormat, IPGroup_QOEProfile,
IPGroup_BWProfile, IPGroup_AlwaysUseSourceAddr, IPGroup_MsgManUserDef1,
IPGroup_MsgManUserDef2, IPGroup_SIPConnect, IPGroup_SBCPSAPMode,
IPGroup_DTLSContext, IPGroup_CreatedByRoutingServer,
IPGroup_UsedByRoutingServer, IPGroup_SBCOperationMode,
IPGroup_SBCRouteUsingRequestURIPort, IPGroup_SBCKeepOriginalCallID,
IPGroup_TopologyLocation, IPGroup_SBCDialPlanName,
IPGroup_CallSetupRulesSetId, IPGroup_Tags, IPGroup_SBCUserStickiness,
IPGroup_UserUDPPortAssignment;
IPGroup 0 = 0, "Default_IPG", "ProxySet_0", "", "", -1, 0, "DefaultSRD",
"", 0, "", -1, -1, -1, 0, 0, "", 0, -1, -1, "", "", "$1$gQ==", 0, "", "",
0, "", "", 0, 0, "default", 0, 0, -1, 0, 0, 0, "", -1, "", 0, 0;
IPGroup 1 = 0, "IP-PBX", "IP-PBX", "192.168.101.250", "", -1, 0,
"DefaultSRD", "MRLan", 1, "IP-PBX", -1, -1, -1, 0, 0, "", 0, -1, -1, "",
"", "$1$gQ==", 0, "", "", 0, "", "", 0, 0, "default", 0, 0, -1, 0, 0, 0,
"", -1, "", 0, 0;
IPGroup 2 = 0, "Telia", "Telia", "192.168.101.250", "", -1, 0,
"DefaultSRD", "MRWan", 1, "Telia", -1, -1, 4, 0, 0, "", 0, -1, -1, "",
"", "$1$gQ==", 0, "", "", 0, "", "", 0, 0, "default", 0, 0, -1, 0, 0, 1,
"", -1, "", 0, 0;

[ \IPGroup ]
```

```
[ SBCAlternativeRoutingReasons ]

FORMAT SBCAlternativeRoutingReasons_Index =
SBCAlternativeRoutingReasons_ReleaseCause;
SBCAlternativeRoutingReasons 0 = 503;

[ \SBCAlternativeRoutingReasons ]


[ ProxyIp ]

FORMAT ProxyIp_Index = ProxyIp_ProxySetId, ProxyIp_ProxyIpIndex,
ProxyIp_IpAddress, ProxyIp_TransportType;
ProxyIp 0 = "1", 0, "192.168.7.43:5060", 0;
ProxyIp 1 = "2", 0, "195.67.246.252:5060", 0;

[ \ProxyIp ]


[ IP2IPRouting ]

FORMAT IP2IPRouting_Index = IP2IPRouting_RouteName,
IP2IPRouting_RoutingPolicyName, IP2IPRouting_SrcIPGroupName,
IP2IPRouting_SrcUsernamePrefix, IP2IPRouting_SrcHost,
IP2IPRouting_DestUsernamePrefix, IP2IPRouting_DestHost,
IP2IPRouting_RequestType, IP2IPRouting_MessageConditionName,
IP2IPRouting_ReRouteIPGroupName, IP2IPRouting_Trigger,
IP2IPRouting_CallSetupRulesSetId, IP2IPRouting_DestType,
IP2IPRouting_DestIPGroupName, IP2IPRouting_DestSIPInterfaceName,
IP2IPRouting_DestAddress, IP2IPRouting_DestPort,
IP2IPRouting_DestTransportType, IP2IPRouting_AltRouteOptions,
IP2IPRouting_GroupPolicy, IP2IPRouting_CostGroup, IP2IPRouting_DestTags,
IP2IPRouting_SrcTags, IP2IPRouting_IPGroupSetName,
IP2IPRouting_RoutingTagName, IP2IPRouting_InternalAction;
IP2IPRouting 0 = "Terminate OPTIONS", "Default_SBCRoutingPolicy", "Any",
"*", "*", "*", "*", 6, "", "Any", 0, -1, 1, "", "", "internal", 0, -1, 0,
0, "", "", "", "", "default", "";
IP2IPRouting 1 = "To IP-PBX", "Default_SBCRoutingPolicy", "Telia", "*",
"*", "*", "*", 0, "", "Any", 0, -1, 0, "IP-PBX", "", "", 0, -1, 0, 0, "",
"", "", "", "default", "";
IP2IPRouting 2 = "To ITSP", "Default_SBCRoutingPolicy", "IP-PBX", "*",
"*", "*", "*", 0, "", "Any", 0, -1, 0, "Telia", "", "", 0, -1, 0, 0, "",
"", "", "", "default", "";

[ \IP2IPRouting ]


[ IPOutboundManipulation ]

FORMAT IPOutboundManipulation_Index =
IPOutboundManipulation_ManipulationName,
IPOutboundManipulation_RoutingPolicyName,
IPOutboundManipulation_IsAdditionalManipulation,
IPOutboundManipulation_SrcIPGroupName,
IPOutboundManipulation_DestIPGroupName,
IPOutboundManipulation_SrcUsernamePrefix, IPOutboundManipulation_SrcHost,
IPOutboundManipulation_DestUsernamePrefix,
IPOutboundManipulation_DestHost,
IPOutboundManipulation_CallingNamePrefix,
IPOutboundManipulation_MessageConditionName,
IPOutboundManipulation_RequestType,
```

```
IPOutboundManipulation_ReRouteIPGroupName,
IPOutboundManipulation_Trigger, IPOutboundManipulation_ManipulatedURI,
IPOutboundManipulation_RemoveFromLeft,
IPOutboundManipulation_RemoveFromRight,
IPOutboundManipulation_LeaveFromRight, IPOutboundManipulation_Prefix2Add,
IPOutboundManipulation_Suffix2Add,
IPOutboundManipulation_PrivacyRestrictionMode,
IPOutboundManipulation_DestTags, IPOutboundManipulation_SrcTags;
IPOutboundManipulation 0 = "Do Nothing", "Default_SBCRoutingPolicy", 0,
"Any", "Telia", "*", "*", "+", "*", "*", "", 0, "Any", 0, 1, 0, 0, 255,
"", "", 0, "", "";
IPOutboundManipulation 1 = "Do Nothing", "Default_SBCRoutingPolicy", 0,
"Any", "Telia", "+", "*", "*", "*", "*", "", 0, "Any", 0, 0, 0, 0, 255,
"", "", 0, "", "";
IPOutboundManipulation 2 = "Add + to Dest", "Default_SBCRoutingPolicy",
0, "Any", "Telia", "*", "*", "*", "*", "*", "", 0, "Any", 0, 1, 0, 0,
255, "+", "", 0, "", "";
IPOutboundManipulation 3 = "Add + to Source", "Default_SBCRoutingPolicy",
0, "Any", "Telia", "*", "*", "*", "*", "*", "", 0, "Any", 0, 0, 0, 0,
255, "+", "", 0, "", "";

[ \IPOutboundManipulation ]


[ MessageManipulations ]

FORMAT MessageManipulations_Index =
MessageManipulations_ManipulationName, MessageManipulations_ManSetID,
MessageManipulations_MessageType, MessageManipulations_Condition,
MessageManipulations_ActionSubject, MessageManipulations_ActionType,
MessageManipulations_ActionValue, MessageManipulations_RowRole;
MessageManipulations 0 = "Change Max-Forwards", 0, "", "header.request-
uri.methodtype == '8'", "header.max-forwards.val", 2, "'10'", 0;
MessageManipulations 1 = "Reject Responses", 4, "any.response",
"header.request-uri.methodtype=='503'", "header.request-uri.methodtype",
2, "'480'", 0;
MessageManipulations 2 = "Call Transfer", 4, "any.request",
"header.referred-by exists", "header.p-asserted-identity.url.user", 2,
"header.referred-by.url.user", 0;

[ \MessageManipulations ]


[ GwRoutingPolicy ]

FORMAT GwRoutingPolicy_Index = GwRoutingPolicy_Name,
GwRoutingPolicy_LCREnable, GwRoutingPolicy_LCRAverageCallLength,
GwRoutingPolicy_LCRDefaultCost, GwRoutingPolicy_LdapServerGroupName;
GwRoutingPolicy 0 = "GwRoutingPolicy", 0, 1, 1, "";

[ \GwRoutingPolicy ]


[ ResourcePriorityNetworkDomains ]

FORMAT ResourcePriorityNetworkDomains_Index =
ResourcePriorityNetworkDomains_Name,
ResourcePriorityNetworkDomains_Ip2TelInterworking;
ResourcePriorityNetworkDomains 1 = "dsn", 1;
ResourcePriorityNetworkDomains 2 = "dod", 1;
ResourcePriorityNetworkDomains 3 = "drsn", 1;
```

```
ResourcePriorityNetworkDomains 5 = "uc", 1;
ResourcePriorityNetworkDomains 7 = "cuc", 1;

[ \ResourcePriorityNetworkDomains ]


[ MaliciousSignatureDB ]

FORMAT MaliciousSignatureDB_Index = MaliciousSignatureDB_Name,
MaliciousSignatureDB_Pattern;
MaliciousSignatureDB 0 = "SIPVicious", "Header.User-Agent.content prefix
'friendly-scanner'";
MaliciousSignatureDB 1 = "SIPScan", "Header.User-Agent.content prefix
'sip-scan'";
MaliciousSignatureDB 2 = "Smap", "Header.User-Agent.content prefix
'smap'";
MaliciousSignatureDB 3 = "Sipsak", "Header.User-Agent.content prefix
'sipsak'";
MaliciousSignatureDB 4 = "Sipcli", "Header.User-Agent.content prefix
'sipcli'";
MaliciousSignatureDB 5 = "Sivus", "Header.User-Agent.content prefix
'SIVuS'";
MaliciousSignatureDB 6 = "Gulp", "Header.User-Agent.content prefix
'Gulp'";
MaliciousSignatureDB 7 = "Sipv", "Header.User-Agent.content prefix
'sipv'";
MaliciousSignatureDB 8 = "Sundayddr Worm", "Header.User-Agent.content
prefix 'sundayddr'";
MaliciousSignatureDB 9 = "VaxIPUserAgent", "Header.User-Agent.content
prefix 'VaxIPUserAgent'";
MaliciousSignatureDB 10 = "VaxSIPUserAgent", "Header.User-Agent.content
prefix 'VaxSIPUserAgent'";
MaliciousSignatureDB 11 = "SipArmyKnife", "Header.User-Agent.content
prefix 'siparmyknife'";

[ \MaliciousSignatureDB ]


[ AudioCoders ]

FORMAT AudioCoders_Index = AudioCoders_AudioCodersGroupId,
AudioCoders_AudioCodersIndex, AudioCoders_Name, AudioCoders_pTime,
AudioCoders_rate, AudioCoders_PayloadType, AudioCoders_Sce,
AudioCoders_CoderSpecific;
AudioCoders 0 = "AudioCodersGroups_0", 0, 1, 2, 90, -1, 0, "";

[ \AudioCoders ]
```

This page is intentionally left blank.

International Headquarters

1 Hayarden Street,

Airport City

Lod 7019900, Israel

Tel: +972-3-976-4000

Fax: +972-3-976-4040

AudioCodes Inc.

27 World's Fair Drive,

Somerset, NJ 08873

Tel: +1-732-469-0880

Fax: +1-732-469-2298

Contact us: https://www.audiocodes.com/corporate/offices-worldwide

Website: https://www.audiocodes.com/

Document #: LTRT-39275