Configuration Note

AudioCodes Professional Services – Interoperability Lab

Connecting AudioCodes' SBC to TransNexus® STIR/SHAKEN Service

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: August-1-2019

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 website at https://www.audiocodes.com/services-support/maintenance-and-support.

Stay in the Loop with AudioCodes

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used.

Related Documentation

Document Name
Mediant 500 E-SBC User's Manual
Mediant 500L E-SBC User's Manual
Mediant 800B E-SBC User's Manual
Mediant 2600 E-SBC User's Manual
Mediant 4000 SBC User's Manual
Mediant 9000 SBC User's Manual
Mediant Software SBC User's Manual
Gateway and SBC CLI Reference Guide
SIP Message Manipulation Reference Guide
AudioCodes Configuration Notes

Document Revision Record

LTRT	Description
13250	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 website at https://online.audiocodes.com/documentation-feedback.

1 Introduction

This document provides the recommended guidelines for setting up the AudioCodes Session Border Controller (hereafter, referred to as *SBC*) for interworking with TransNexus ClearIP software platform that provides STIR/SHAKEN certificate management, authentication and verification,

Note: The scope of this document does not fully cover all aspects for deploying the AudioCodes SBC in your environment. For detailed configuration, refer to the device's *User's Manual*. If you have any questions regarding required configuration, please contact your AudioCodes sales representative.

1.1 STIR/SHAKEN overview

STIR/SHAKEN is defined by the Federal Communications Commission (FCC) as a framework of interconnected standards. Based on common public key cryptography techniques, it essentially provides the basis to ensure the authenticity of a phone call. The framework is thought of as an important first step to combating illegal and unwanted robocalls.

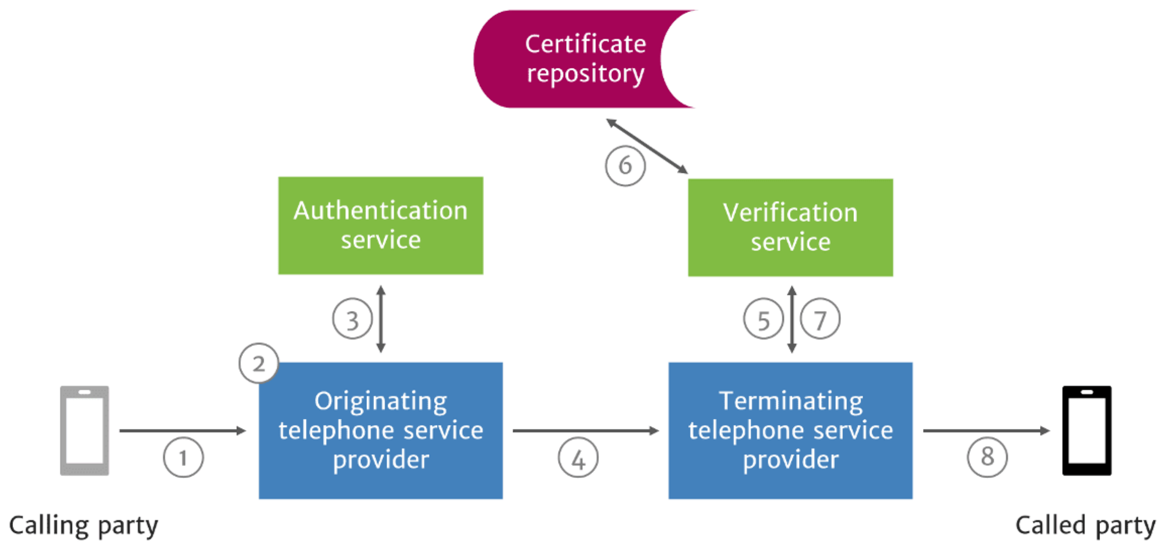
The process underlying STIR/SHAKEN has been in use on the Internet for years, providing token authentication for secure websites, minimizing the spoofing of Internet addresses by bad actors. Recent government, service provider, and enterprise security experts have deemed authentication and validation as a necessary process for reducing the impact of bad actors on the telephone network.

STIR, short for **S**ecure **T**elephony **I**dentity **R**evisited, is the protocol for providing calling party info within a digital signature. This focuses on the end devices and allows for the digital signature to be produced and verified in numerous locations.

SHAKEN stands for **S**ecure **H**andling of **A**sserted information using To**ken**s and focuses on how STIR can be implemented within carrier's networks. Where STIR emphasizes the end devices, SHAKEN addresses deploy ability.

1.1.1 How does STIR/SHAKEN work?

Figure 1-1: STIR/SHAKEN Work Flow



1. A SIP INVITE is received by the originating telephone service provider.
2. The originating telephone service provider checks the call source and calling number to determine how to attest for the validity of the calling number:
   - **Full Attestation (A):** The service provider authenticates the calling party AND confirms they are authorized to use this number. An example of this case is a subscriber registered with the originating telephone service provider’s softswitch.
   - **Partial Attestation (B):** The service provider verifies the call origination but cannot confirm that the call source is authorized to use the calling number. An example of this use case is a telephone number behind an enterprise PBX.
   - **Gateway Attestation (C):** The service provider authenticates the call’s origin but cannot verify the source. An example of this case would be a call received from an international gateway.
3. The originating telephone service provider uses the authentication service to create a SIP Identity header, that contains information on the calling number, called number, date and time, attestation level, and call origination, along with the certificate.
4. The SIP INVITE with the SIP Identity header is sent to the terminating telephone service provider.
5. The SIP INVITE with Identity header is passed to the verification service.
6. The verification service obtains the digital certificate of the originating telephone service provider from the public certificate repository.
7. The verification service returns the results to the terminating service provider’s softswitch or SBC.
8. The verification service returns the results to the terminating service provider’s softswitch or SBC.

1.2 About AudioCodes SBC Product Series

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

The 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 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 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.

2 Interoperability Topology

The interoperability topology contains deployment of AudioCodes SBC at the Originating Service Provider (for authentication) and at the Terminating Service Provider (for verification).

The figures below illustrate this interoperability topology:

Figure 2-1: Originating Service Provider Authenticates via SBC

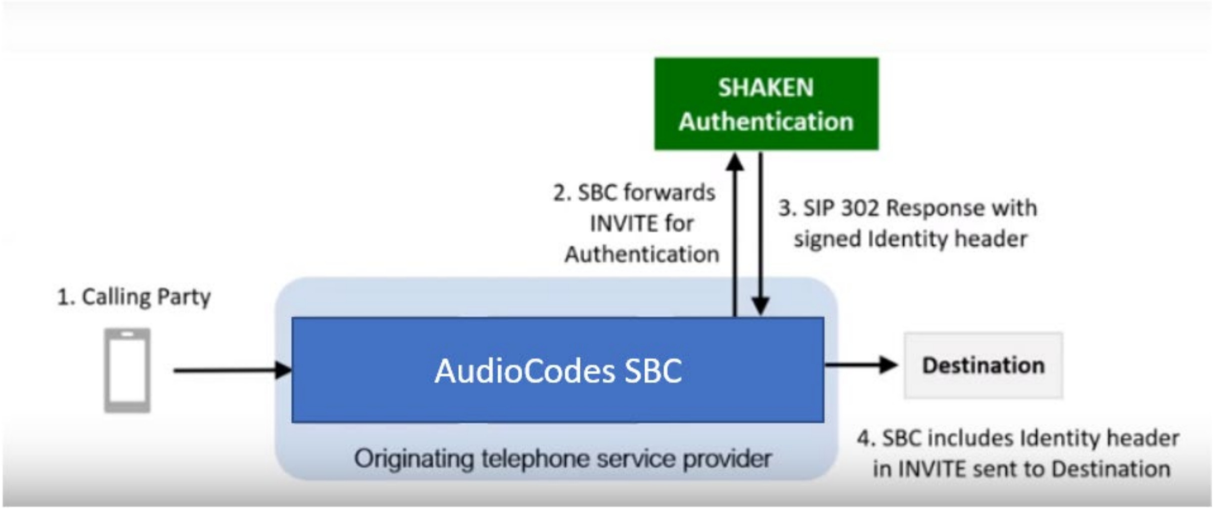
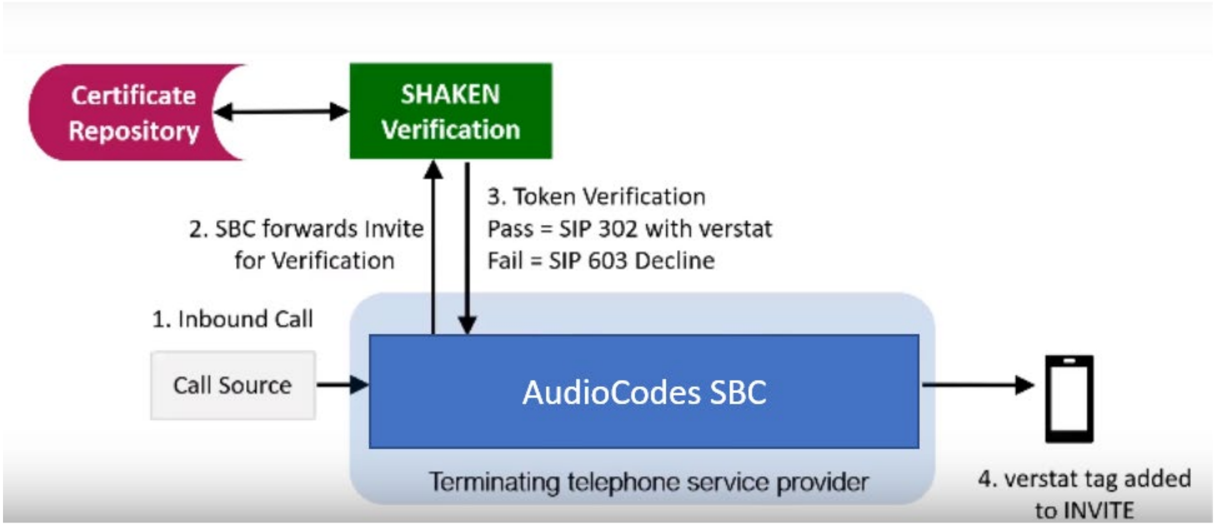


Figure 2-2: Terminating Service Provider Verifies via SBC



This page is intentionally left blank.

3 Configuring AudioCodes SBC

This chapter provides step-by-step procedures on how to configure AudioCodes SBC for interworking with TransNexus ClearIP software platform for the SHAKEN Services. These configuration procedures are based on the interoperability test topology described in Section 2 on page 9, and includes the following main areas:

- For SBC, located at Originating Service Provider:
    - SBC LAN interface – IP-PBX, originating calls
    - SBC WAN interface – TransNexus SHAKEN Services and SIP Trunking
- For SBC, located at Terminating Service Provider:
    - SBC LAN interface – IP-PBX, terminating calls
    - SBC WAN interface – TransNexus SHAKEN Services and SIP Trunking

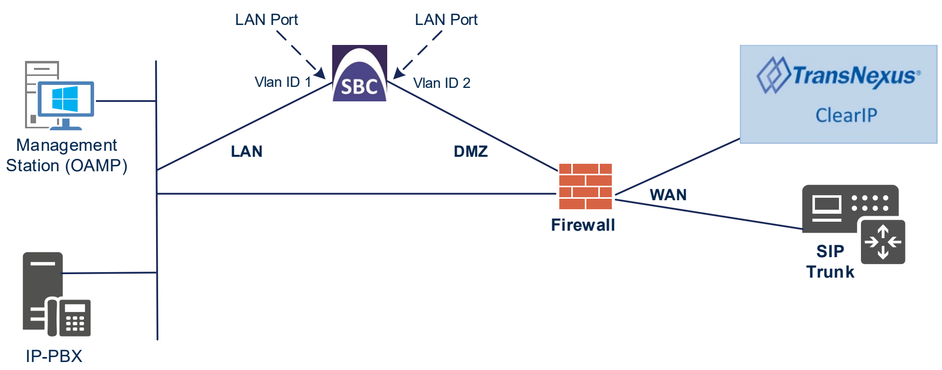
> **Note:** This document describes partial configuration. Your implementation can be different. So, for detailed configuration of other entities in the deployment such as the SIP Trunk Provider and the local IP-PBX, refer to the device's *User's Manual*.

3.1 IP Network Interfaces Configuration

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

- SBC interfaces with the following IP entities:
  - IP-PBX, located on the LAN
  - TransNexus ClearIP software platform, located on the WAN
- 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, SBC connects to the LAN and DMZ using dedicated LAN ports (i.e., two ports and two network cables are used).
- SBC also uses two logical network interfaces:
  - LAN (VLAN ID 1)
  - DMZ (VLAN ID 2)

Figure 3-1: Network Interfaces in Interoperability Test Topology



3.1.1 Configure VLANs

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

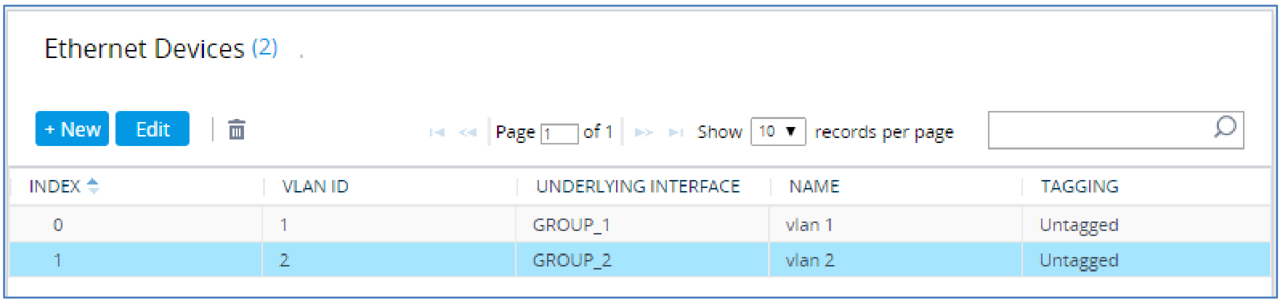
- LAN VoIP (assigned the name "LAN_IF")
- WAN VoIP (assigned the name "WAN_IF")

➢ **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 3-2: Configured VLAN IDs in Ethernet Device



3.1.2 Configure Network Interfaces

This section 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	**10.15.17.77** (LAN IP address of 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**

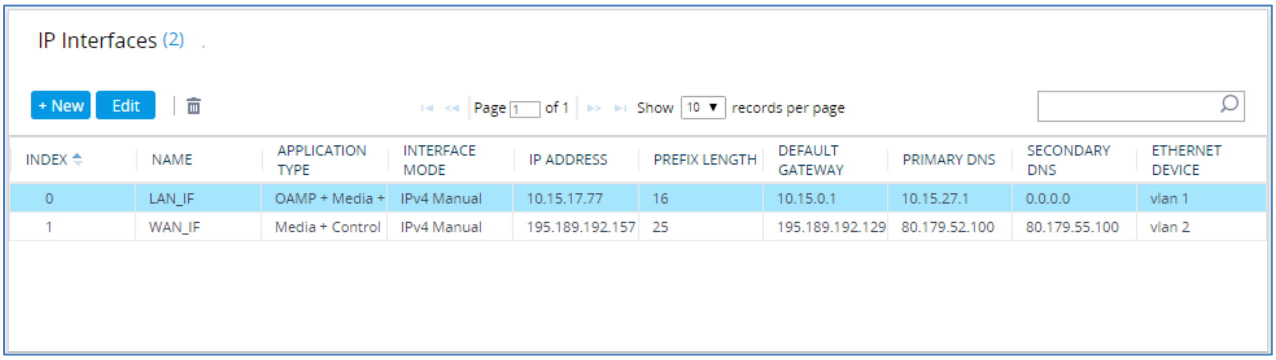
3. Add a network interface for the WAN side:
   a. Click **New**.
   a. Configure the interface as follows:

Parameter	Value
Name	**WAN_IF**
Application Type	**Media + Control**
Ethernet Device	**vlan 2**
IP Address	**195.189.192.157** (DMZ IP address of SBC)
Prefix Length	**25** (subnet mask in bits for 255.255.255.128)
Default Gateway	**195.189.192.129** (router's IP address)
Primary DNS	**80.179.52.100**
Secondary DNS	**80.179.55.100**

4. Click **Apply**.

The configured IP network interfaces are shown below:

Figure 3-3: 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	10.15.17.77	16	10.15.0.1	10.15.27.1	0.0.0.0	vlan 1
1	WAN_IF	Media + Control	IPv4 Manual	195.189.192.157	25	195.189.192.129	80.179.52.100	80.179.55.100	vlan 2

3.2 Configure Media Realms

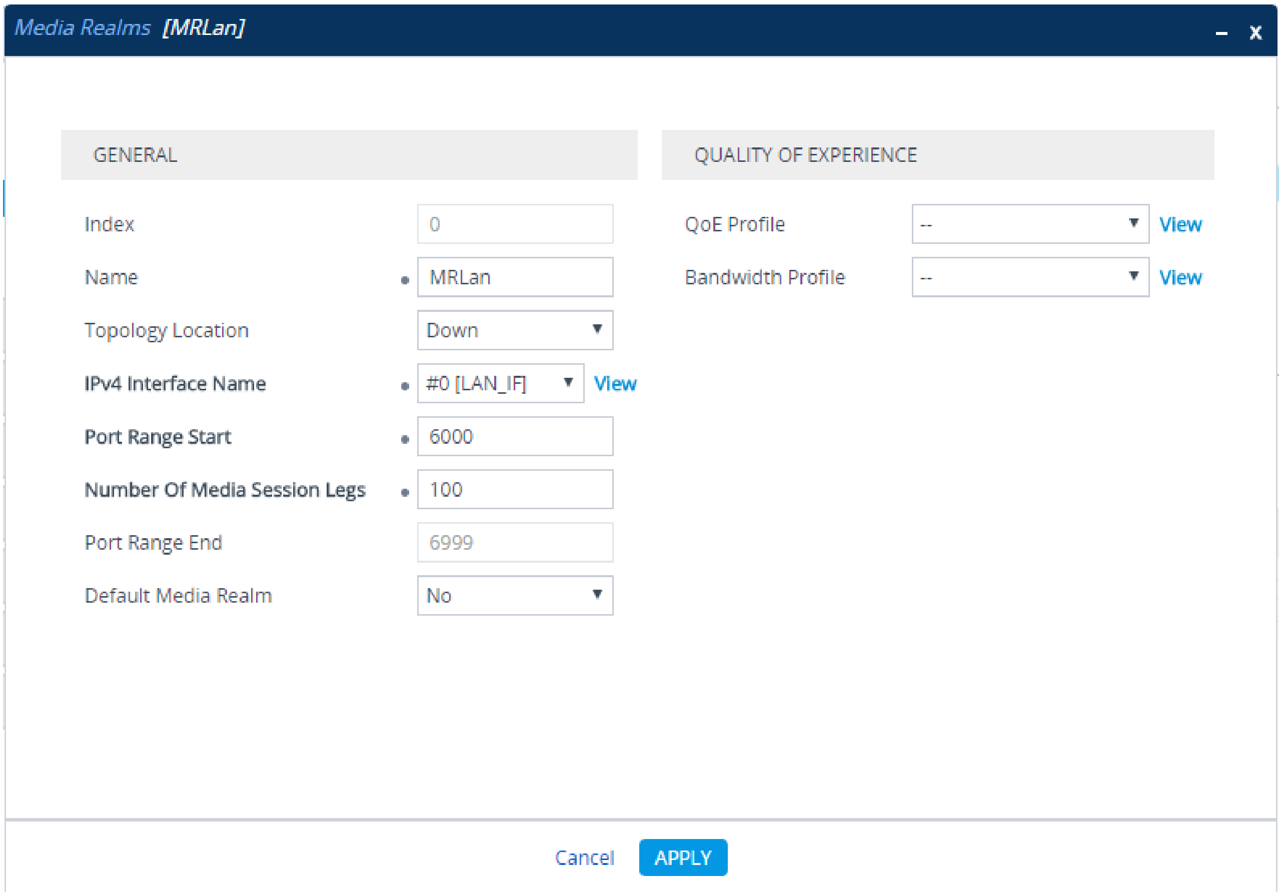
This section describes how to configure Media Realms. The simplest configuration is to create two Media Realms - one for internal (LAN) traffic and one for external (WAN) traffic.

➢ **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)

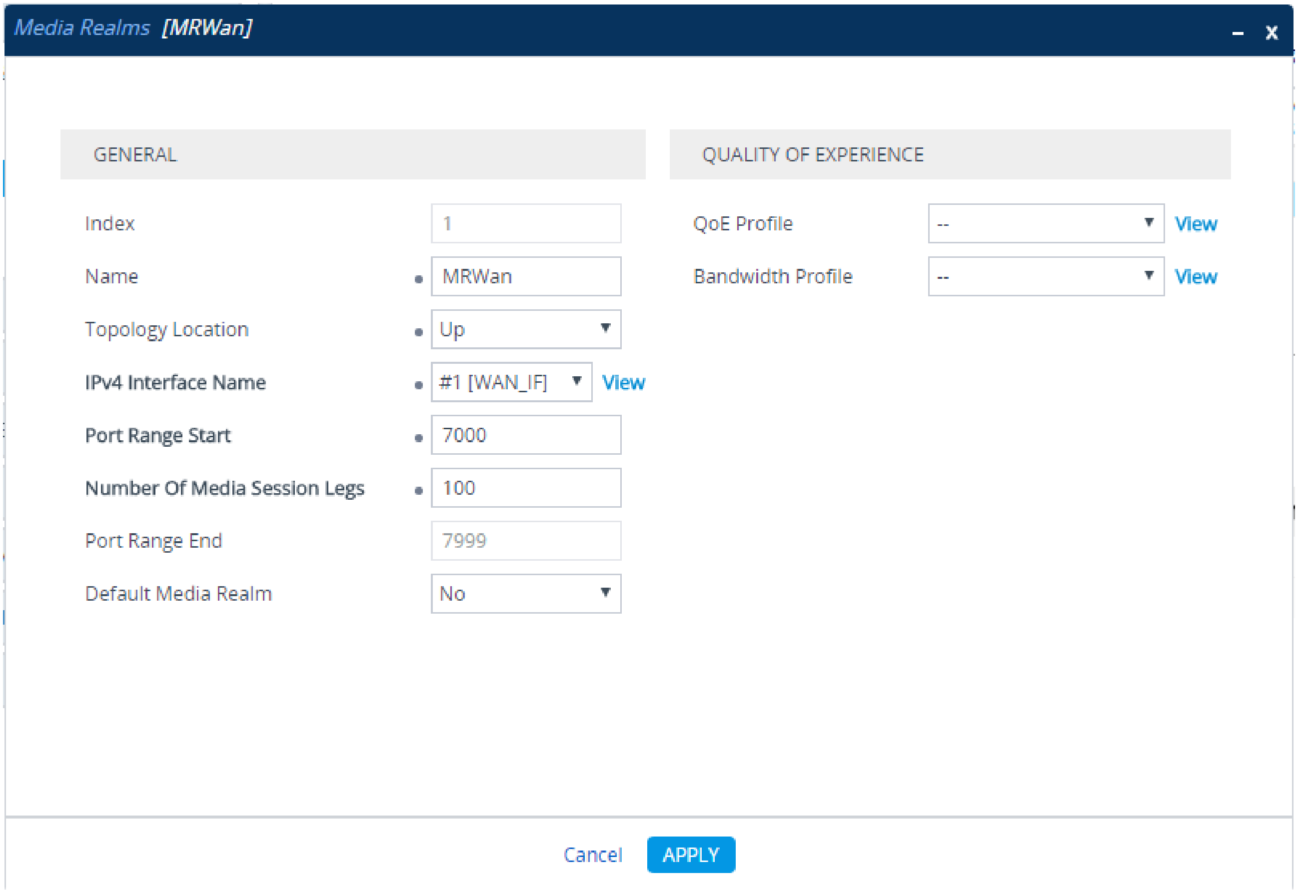
Figure 3-4: Configuring Media Realm for LAN



3. Configure a Media Realm for WAN traffic:

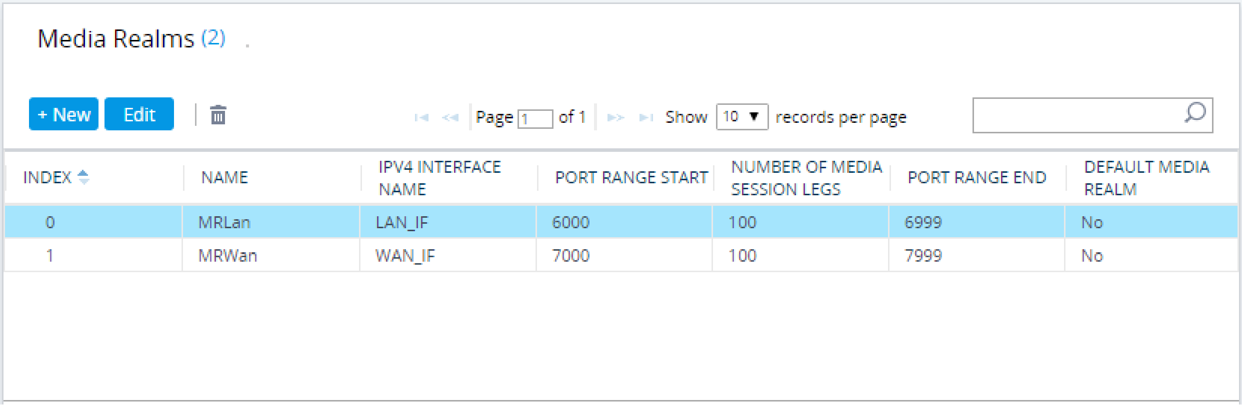
Parameter	Value
Index	**1**
Name	**MRWan** (arbitrary name)
Topology Location	**Up**
IPv4 Interface Name	**WAN_IF**
Port Range Start	**7000** (represents lowest UDP port number used for media on WAN)
Number of Media Session Legs	**100** (media sessions assigned with port range)

Figure 3-5: Configuring Media Realm for WAN



The configured Media Realms are shown in the figure below:

Figure 3-6: 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

3.3 Configure SIP Signaling Interfaces

This section describes how to configure SIP Interfaces. For the interoperability test topology, an internal and external SIP interface must be configured for the 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:

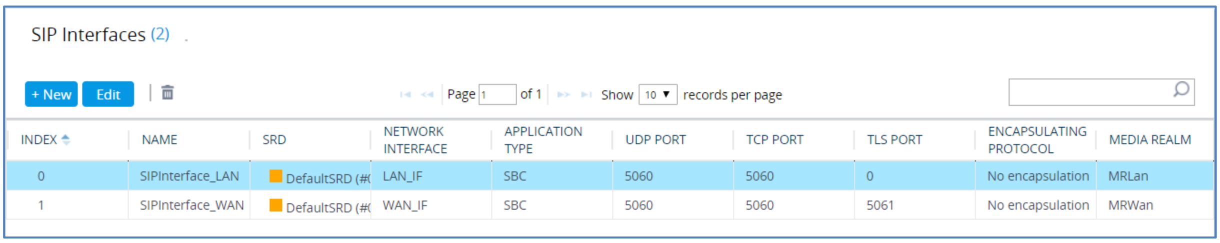
Parameter	Value
Index	**0**
Name	**SIPInterface_LAN** (arbitrary name)
Network Interface	**LAN_IF**
Application Type	**SBC**
UDP Port	**5060** (according to IP-PBX requirement)
TCP and TLS Port	**0**
Media Realm	**MRLan**

3. Configure a SIP Interface for the WAN:

Parameter	Value
Index	**1**
Name	**SIPInterface_WAN** (arbitrary name)
Network Interface	**WAN_IF**
Application Type	**SBC**
UDP Port	**5060** (according to SIP Trunk requirement)
TCP Port	**5060**
TLS Port	**5061** (according to TransNexus configuration)
Media Realm	**MRWan**

The configured SIP Interfaces are shown in the figure below:

Figure 3-7: 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	ENCAPSULATING PROTOCOL	MEDIA REALM
0	SIPInterface_LAN	DefaultSRD (#(	LAN_IF	SBC	5060	5060	0	No encapsulation	MRLan
1	SIPInterface_WAN	DefaultSRD (#(	WAN_IF	SBC	5060	5060	5061	No encapsulation	MRWan

3.4 Configure Proxy Sets

This section 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, following Proxy Sets need to be configured for the following IP entities:

- IP-PBX
- SIP Trunk
- TransNexus ClearIP software platform

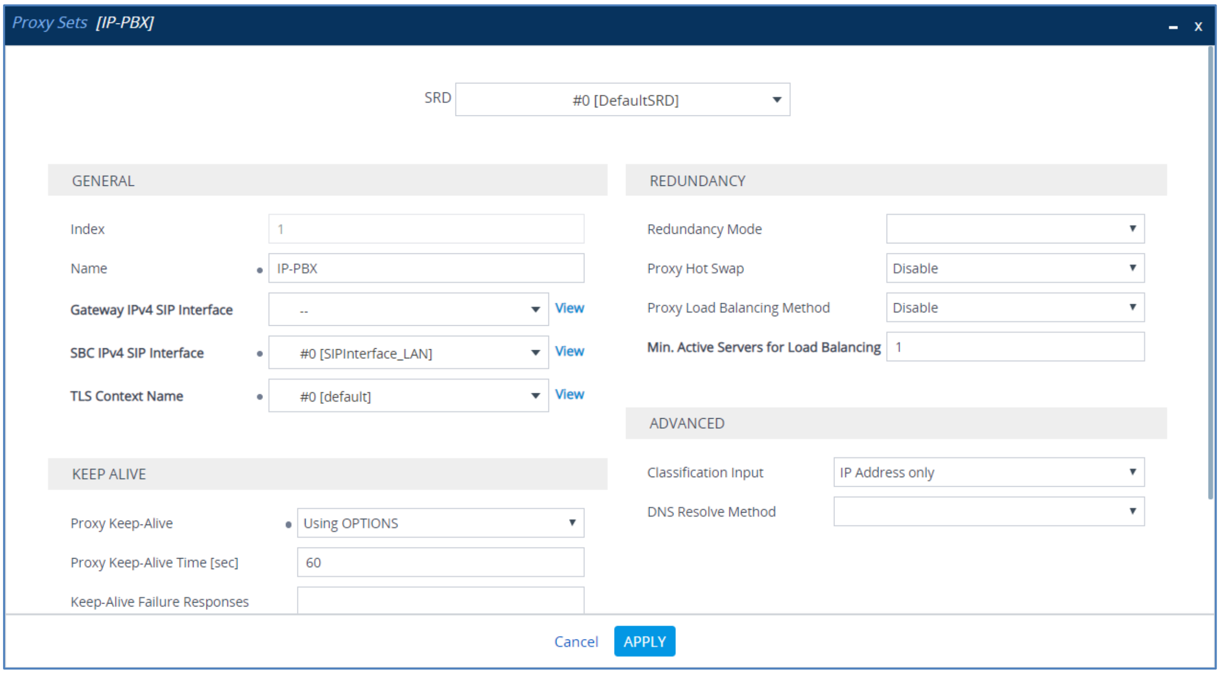
The Proxy Sets will be later applying to the VoIP network by assigning them to IP Groups.

➢ **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 Skype for Business Server as shown below:

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

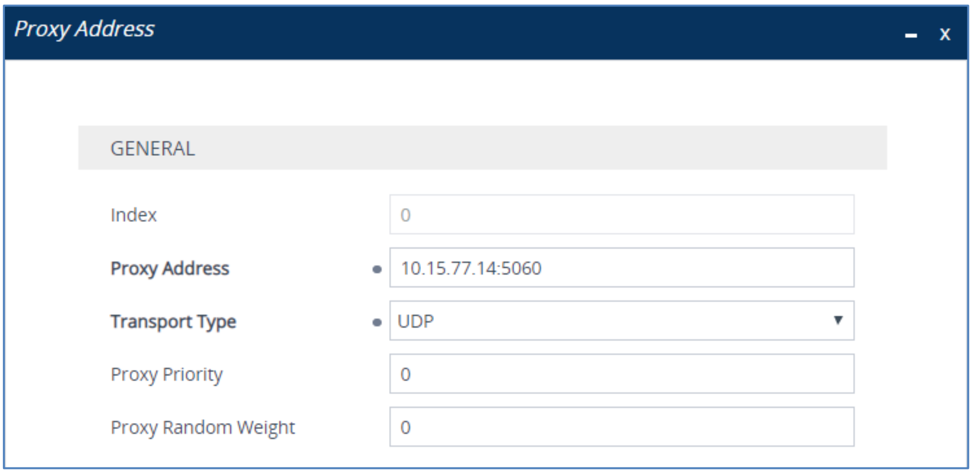
Figure 3-8: Configuring Proxy Set for IP-PBX



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 3-9: Configuring Proxy Address for IP-PBX



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

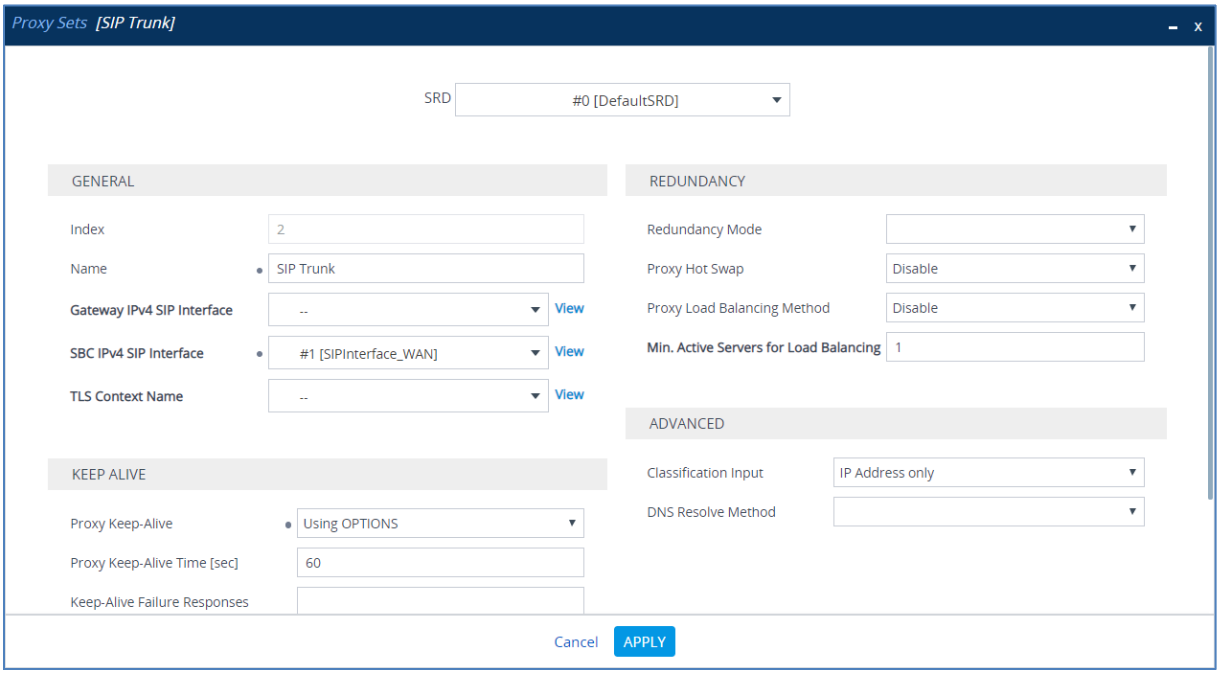
Parameter	Value
Index	**0**
Proxy Address	**10.15.77.14:5060** (IP-PBX IP address / FQDN and destination port)
Transport Type	**UDP** (according to IP-PBX configuration)

d. Click **Apply**.

3. Configure a Proxy Set for the SIP Trunk:

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

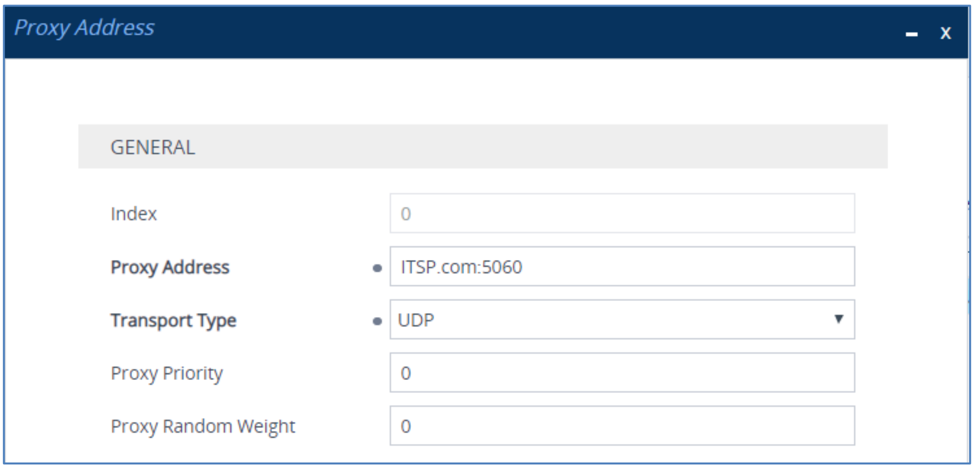
Figure 3-10: Configuring Proxy Set for SIP Trunk



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 3-11: Configuring Proxy Address for SIP Trunk



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

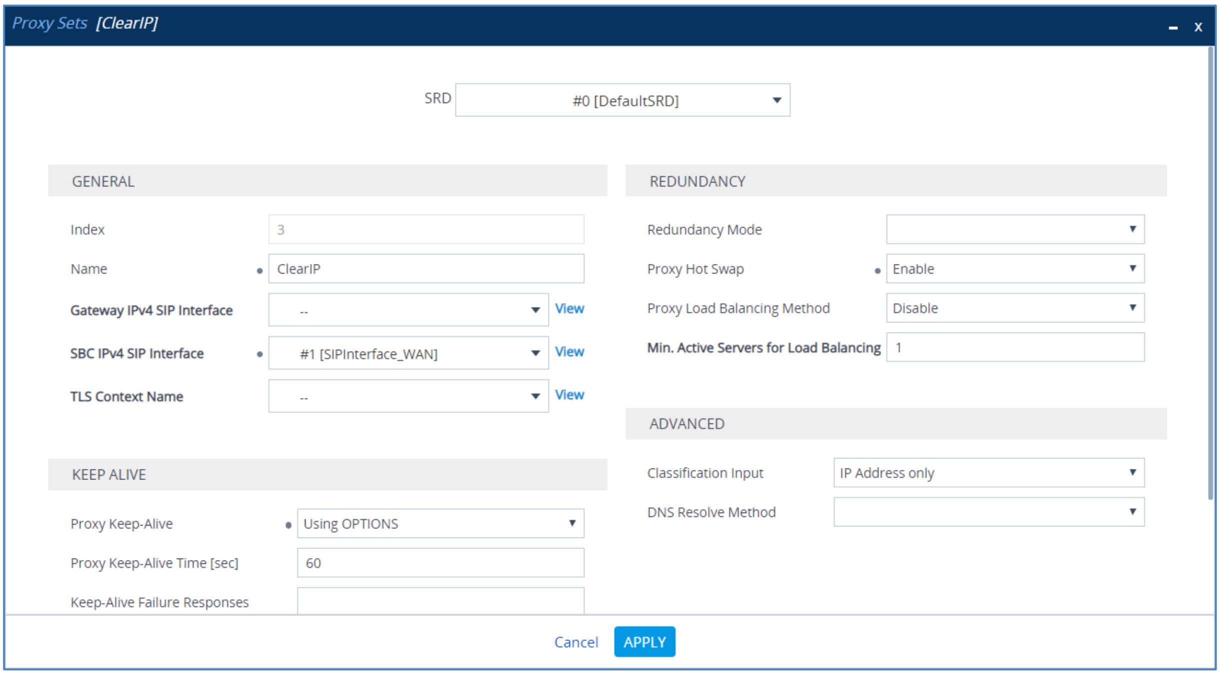
Parameter	Value
Index	**0**
Proxy Address	**SP.com:5060** (IP address / FQDN and destination port)
Transport Type	**UDP**

d. Click **Apply**.

4. Configure a Proxy Set for TransNexus ClearIP software platform:

Parameter	Value
Index	**3**
Name	**ClearIP**
SBC IPv4 SIP Interface	**SIPInterface_WAN**
Proxy Keep-Alive	**Using Options**
Proxy Hot Swap	**Enable**

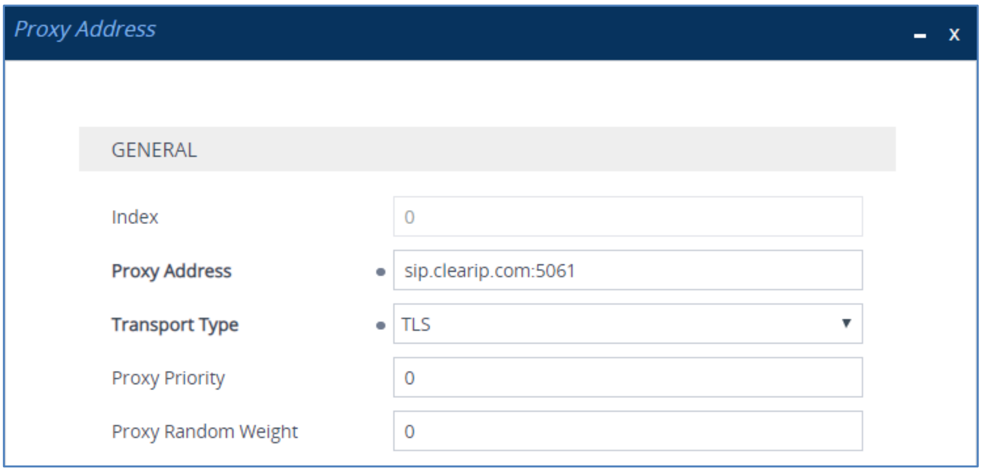
Figure 3-12: Configuring Proxy Set for ClearIP



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.

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

Figure 3-13: Configuring Proxy Address ClearIP



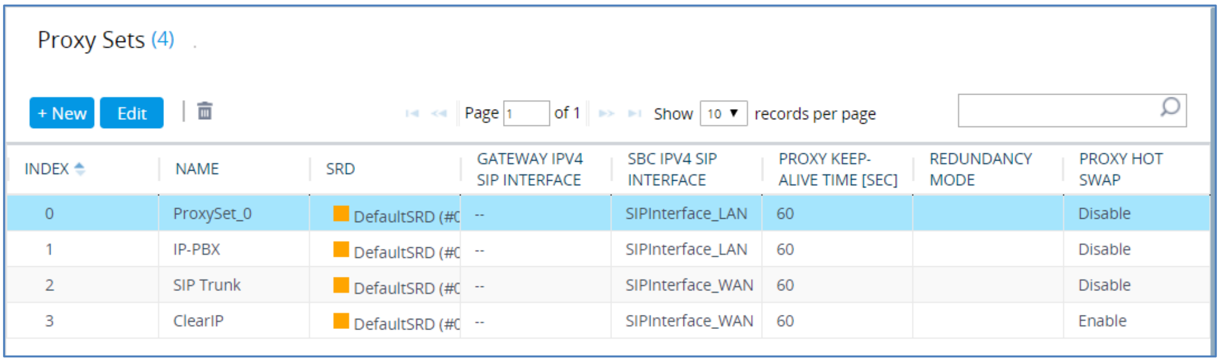
f. Configure the address of the Proxy Set according to the parameters described in the table below.

Parameter	Value
Index	**0**
Proxy Address	**sip.clearip.com:5061** (ClearIP FQDN and destination port)
Transport Type	**TLS**

g. Click **Apply**.

The configured Proxy Sets are shown in the figure below:

Figure 3-14: Configured Proxy Sets in Proxy Sets Table



INDEX	NAME	SRD	GATEWAY IPV4 SIP INTERFACE	SBC IPV4 SIP INTERFACE	PROXY KEEP-ALIVE TIME [SEC]	REDUNDANCY MODE	PROXY HOT SWAP
0	ProxySet_0	DefaultSRD (#0	--	SIPInterface_LAN	60		Disable
1	IP-PBX	DefaultSRD (#0	--	SIPInterface_LAN	60		Disable
2	SIP Trunk	DefaultSRD (#0	--	SIPInterface_WAN	60		Disable
3	ClearIP	DefaultSRD (#0	--	SIPInterface_WAN	60		Enable

3.5 Configure IP Profiles

This section 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 3xx) and media (e.g., coder and transcoding method).

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

- For SBC, located at Originating Service Provider:
  - IP-PBX
  - SIP Trunk
- For SBC, located at Terminating Service Provider:
  - SIP Trunk

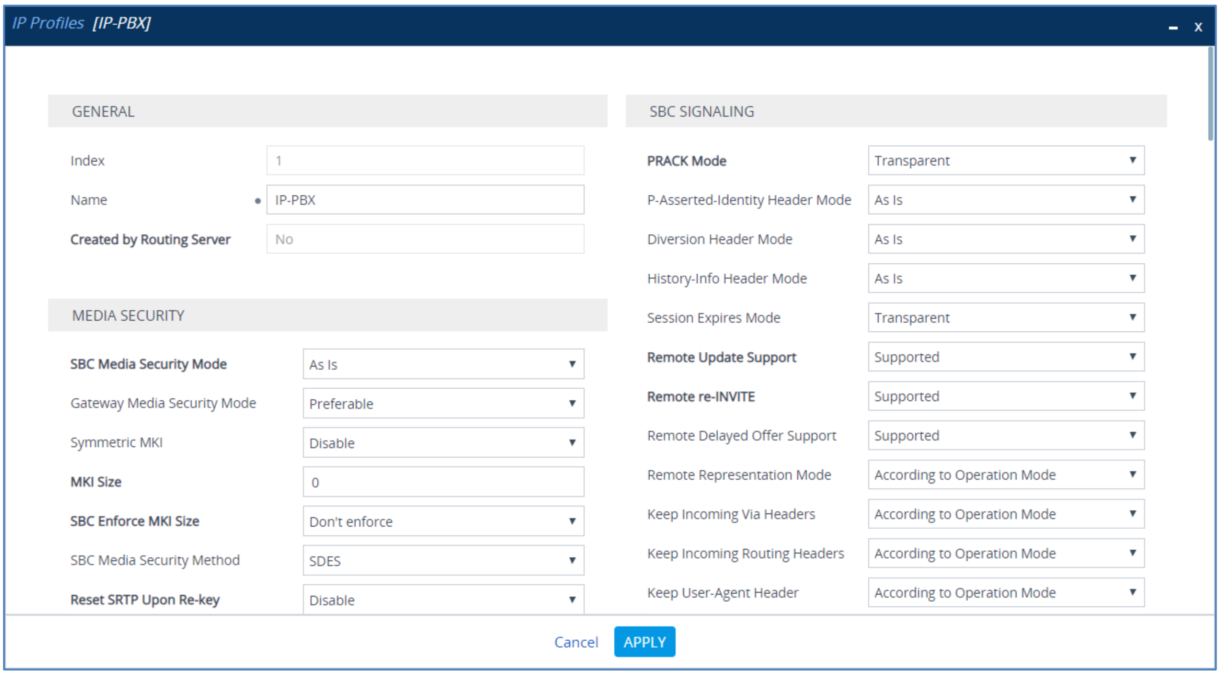
Note: This section shows only partial configuration. Your implementation can be different and additional parameters maybe needed to be configured for each entity. For detailed configuration, refer to the device's *User's Manual*.

➢ **To configure IP Profile for the IP-PBX in the Originating SBC:**

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**
SBC Forward and Transfer	
Remote 3xx Mode	**Handle Locally** (required, for terminating SIP 3xx responses from ClearIP software platform)

Figure 3-15: Configuring IP Profile for IP-PBX in the Originating SBC



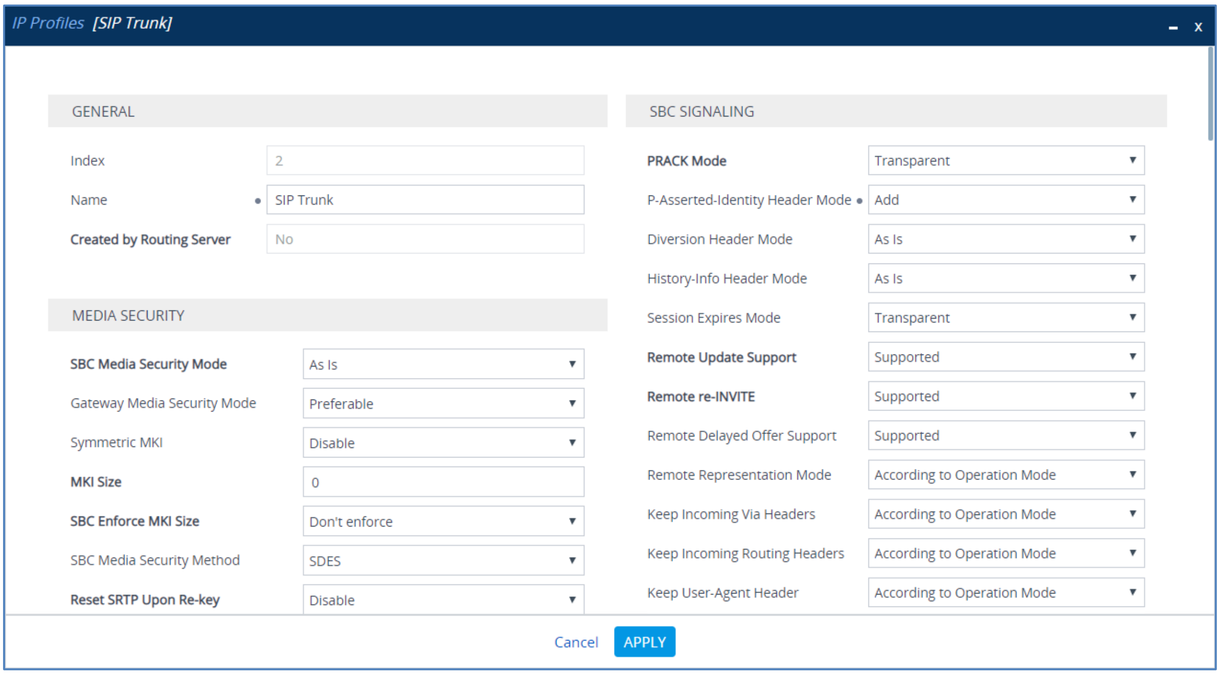
3. Click **Apply**.

➢ **To configure an IP Profile for the SIP Trunk in the Originating SBC:**

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

Parameter	Value
General	
Index	**2**
Name	**SIP Trunk**
SBC Signaling	
P-Asserted-Identity Header Mode	**Add**

Figure 3-16: Configuring IP Profile for SIP Trunk in the Originating SBC



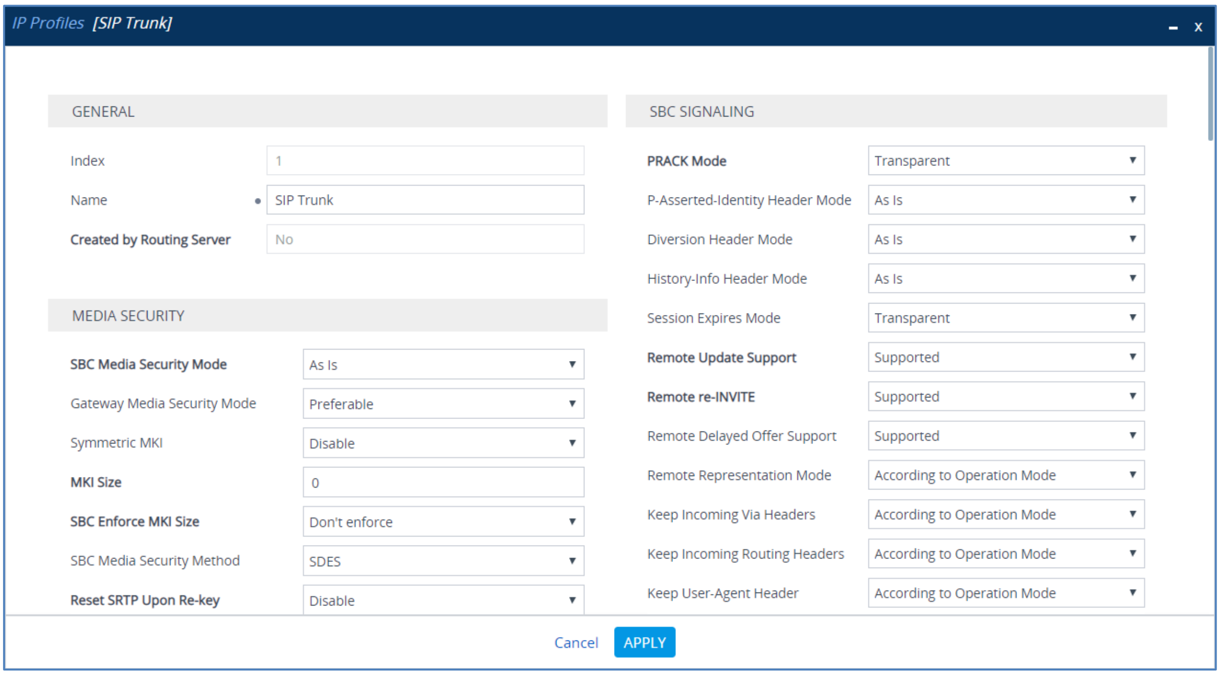
2. Click **Apply**.

➤ To configure an IP Profile for the SIP Trunk in the Terminating SBC:

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

Parameter	Value
General	
Index	**1**
Name	**SIP Trunk**
SBC Forward and Transfer	
Remote 3xx Mode	**Handle Locally** (required, for terminating SIP 3xx responses from ClearIP software platform)

Figure 3-17: Configuring IP Profile for SIP Trunk in the Terminating SBC



2. Click **Apply**.

3.6 Configure IP Groups

This section describes how to configure IP Groups. The IP Group represents an IP entity on the network with which the SBC communicates. This can be a server (e.g., IP-PBX or SIP Trunk) 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
- SIP Trunk
- TransNexus ClearIP software platform

➢ **To configure IP Groups in the Originating SBC:**

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 SIP Trunk:

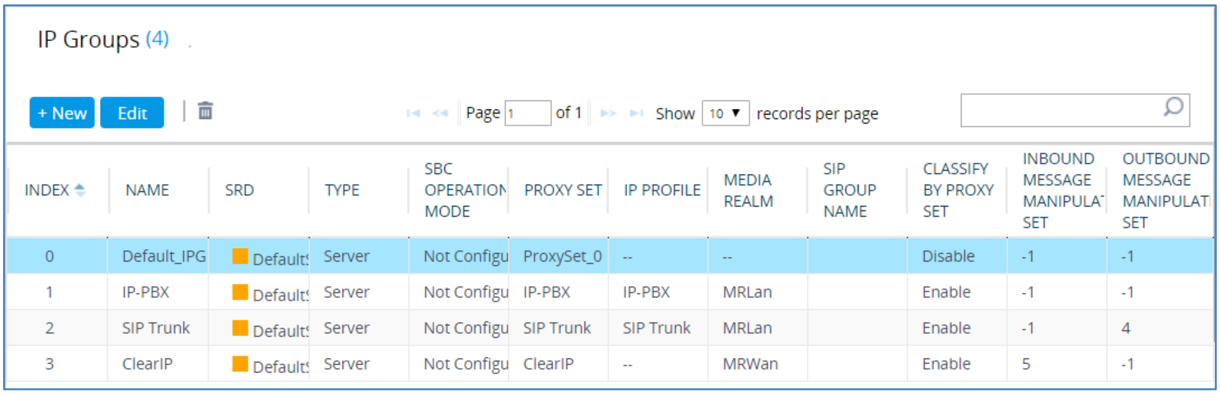
Parameter	Value
Index	**2**
Name	**SIP Trunk**
Topology Location	**Up**
Type	**Server**
Proxy Set	**SIP Trunk**
IP Profile	**SIP Trunk**
Media Realm	**MRWan**
SIP Group Name	(according to ITSP requirement)

4. Configure an IP Group for the ClearIP software platform :

Parameter	Value
Index	**3**
Name	**ClearIP**
Topology Location	**Up**
Type	**Server**
Proxy Set	**ClearIP**
Media Realm	**MRWan**
SIP Group Name	(according to ITSP requirement)

The configured IP Groups are shown in the figure below:

Figure 3-18: Configured IP Groups in IP Group Table for Originating SBC


IP Groups (4)

+ 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 MANIPULAT SET	OUTBOUND MESSAGE MANIPULAT SET
0	Default_IPG	DefaultS	Server	Not Configu	ProxySet_0	--	--		Disable	-1	-1
1	IP-PBX	DefaultS	Server	Not Configu	IP-PBX	IP-PBX	MRLan		Enable	-1	-1
2	SIP Trunk	DefaultS	Server	Not Configu	SIP Trunk	SIP Trunk	MRLan		Enable	-1	4
3	ClearIP	DefaultS	Server	Not Configu	ClearIP	--	MRWan		Enable	5	-1

➢ **To configure IP Groups in the Terminating SBC:**

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**
Media Realm	**MRLan**
SIP Group Name	(according to ITSP requirement)

3. Configure an IP Group for the SIP Trunk:

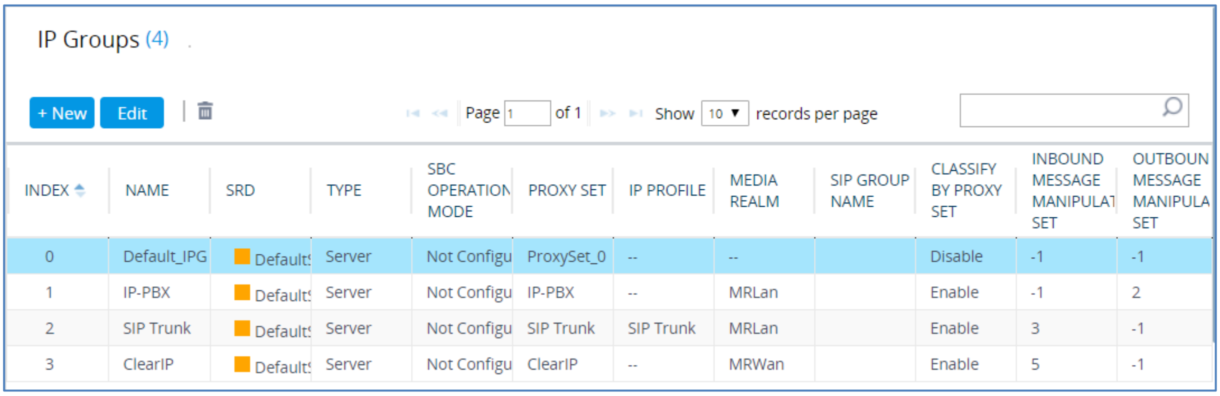
Parameter	Value
Index	**2**
Name	**SIP Trunk**
Topology Location	**Up**
Type	**Server**
Proxy Set	**SIP Trunk**
IP Profile	**SIP Trunk**
Media Realm	**MRWan**
SIP Group Name	(according to ITSP requirement)

4. Configure an IP Group for the ClearIP software platform:

Parameter	Value
Index	**3**
Name	**ClearIP**
Topology Location	**Up**
Type	**Server**
Proxy Set	**ClearIP**
Media Realm	**MRWan**
SIP Group Name	(according to ITSP requirement)

The configured IP Groups are shown in the figure below:

Figure 3-19: Configured IP Groups in IP Group Table for Terminating SBC



INDEX	NAME	SRD	TYPE	SBC OPERATION MODE	PROXY SET	IP PROFILE	MEDIA REALM	SIP GROUP NAME	CLASSIFY BY PROXY SET	INBOUND MESSAGE MANIPULAT SET	OUTBOUN MESSAGE MANIPULA SET
0	Default_IPG	Default!	Server	Not Configu	ProxySet_0	--	--		Disable	-1	-1
1	IP-PBX	Default!	Server	Not Configu	IP-PBX	--	MRLan		Enable	-1	2
2	SIP Trunk	Default!	Server	Not Configu	SIP Trunk	SIP Trunk	MRLan		Enable	3	-1
3	ClearIP	Default!	Server	Not Configu	ClearIP	--	MRWan		Enable	5	-1

3.7 Configure IP-to-IP Call Routing Rules

This section 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 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 3.6 on page 23,) to denote the source and destination of the call.

For the interoperability test topology, the following IP-to-IP routing rules need to be:

- For SBC, located at Originating Service Provider:
  - Terminate SIP OPTIONS messages on the SBC that are received from any entity
  - IP-PBX
  - SIP Trunk
- For SBC, located at Terminating Service Provider:
  - Terminate SIP OPTIONS messages on the SBC that are received from any entity
  - SIP Trunk

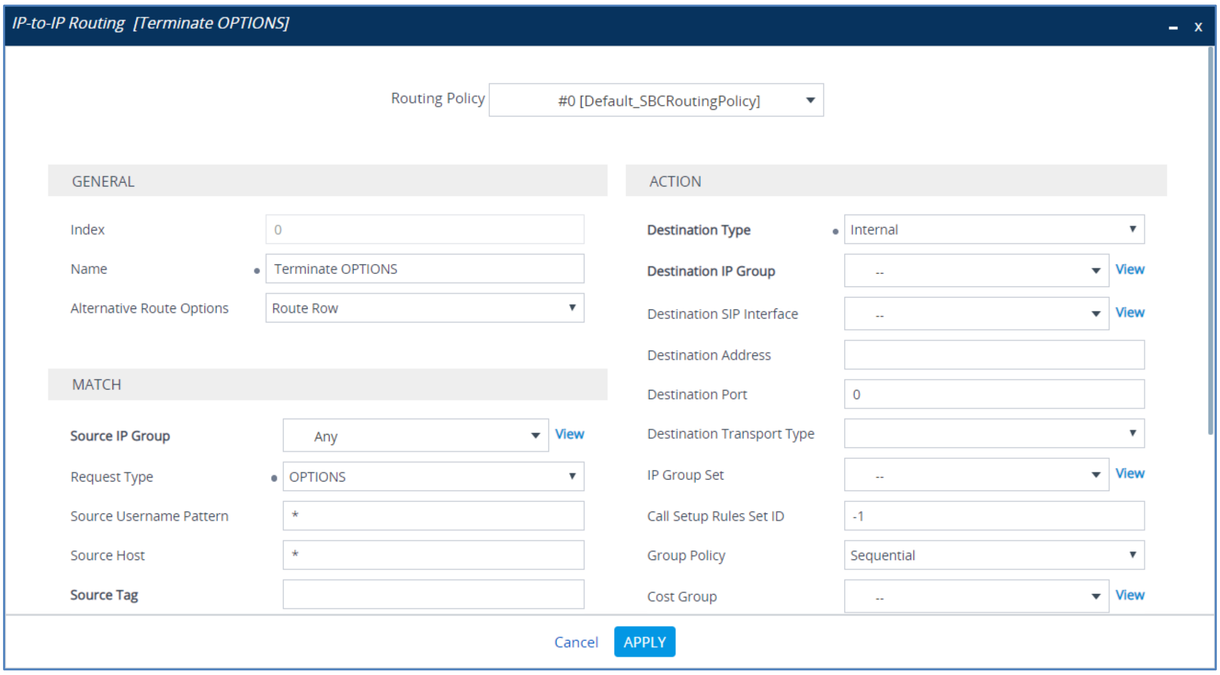
3.7.1 Configure IP-to-IP Call Routing Rules for Originating SBC

➢ **To configure IP-to-IP routing rules for Originating SBC:**

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 any entity:
   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	**Internal**
Internal Action	**Reply (Response='200')**

Figure 3-20: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS



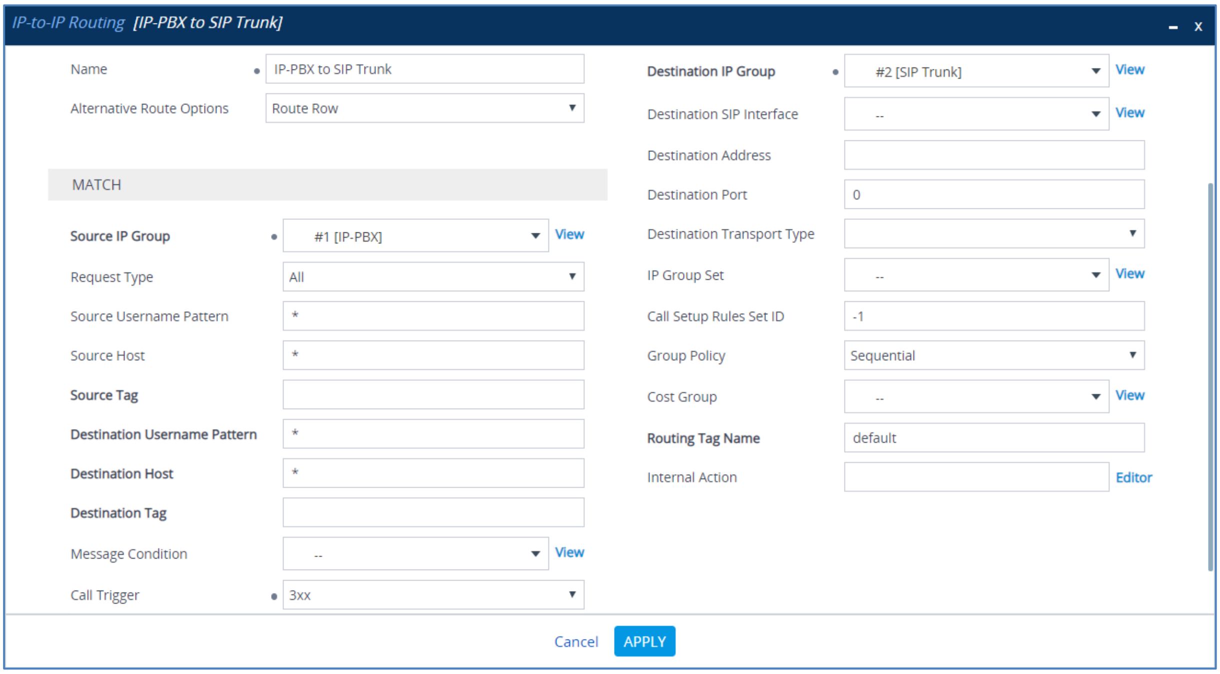
b. Click **Apply**.

3. Configure a rule to re-route messages from IP-PBX towards SIP Trunk after receiving SIP 3xx response from ClearIP software platform:

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

Parameter	Value
Index	**1**
Route Name	**IP-PBX to SIP Trunk** (arbitrary descriptive name)
Source IP Group	**IP-PBX**
Call Triger	**3xx**
Destination Type	**IP Group**
Destination IP Group	**SIP Trunk**

Figure 3-21: Configuring IP-to-IP Routing Rule for Re-Routing after receiving 3xx

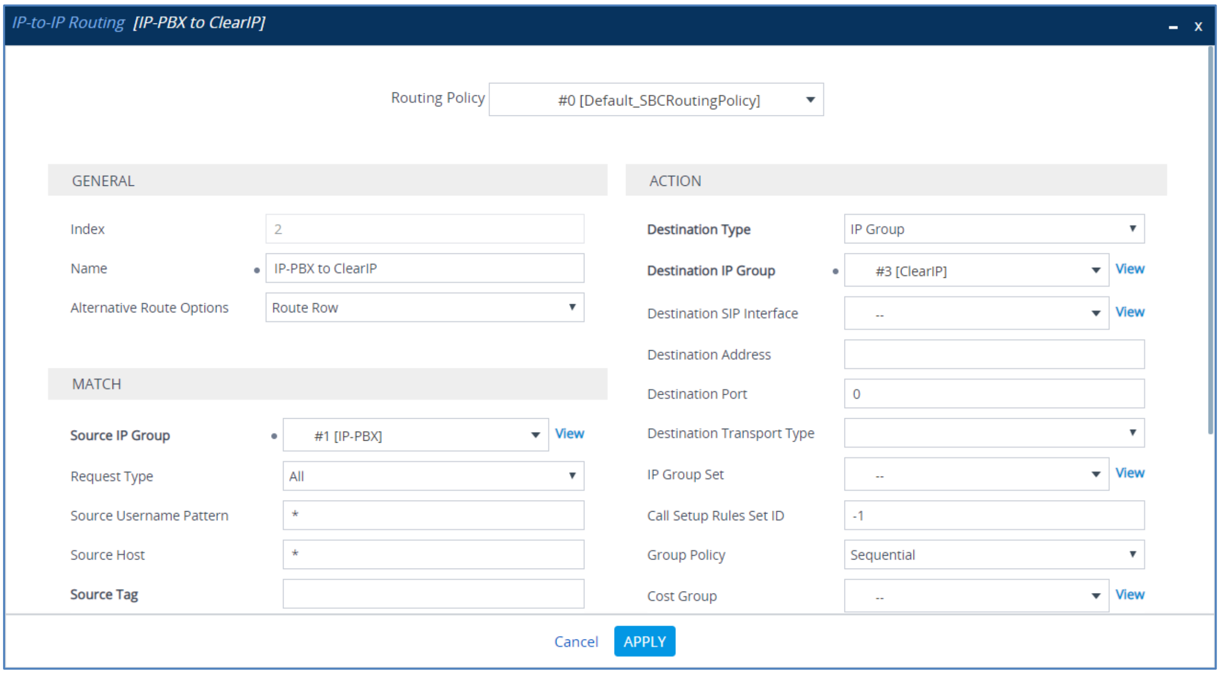


   b. Click **Apply**.

4. Configure a rule to route calls from IP-PBX to ClearIP software platform:
   h. Click **New**, and then configure the parameters as follows:

Parameter	Value
Index	**2**
Route Name	**IP-PBX to ClearIP** (arbitrary descriptive name)
Source IP Group	**IP-PBX**
Destination Type	**IP Group**
Destination IP Group	**ClearIP**

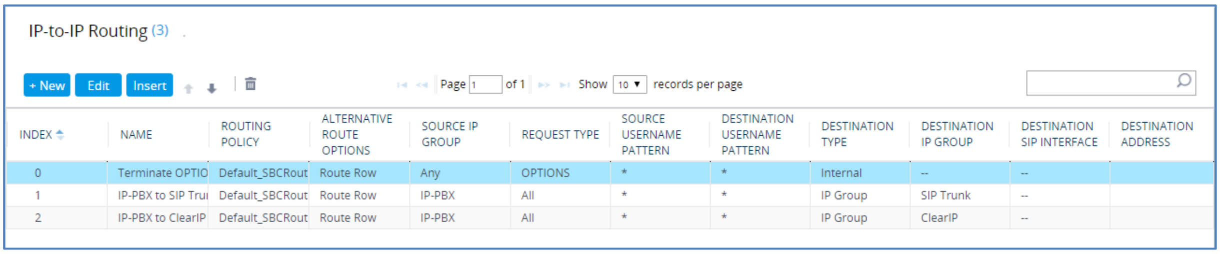
Figure 3-22: Configuring IP-to-IP Routing Rule for IP-PBX to ClearIP



   i. Click **Apply**.

The configured routing rules are shown in the figure below:

Figure 3-23: Example of the Configured IP-to-IP Routing Rules in the Originating SBC



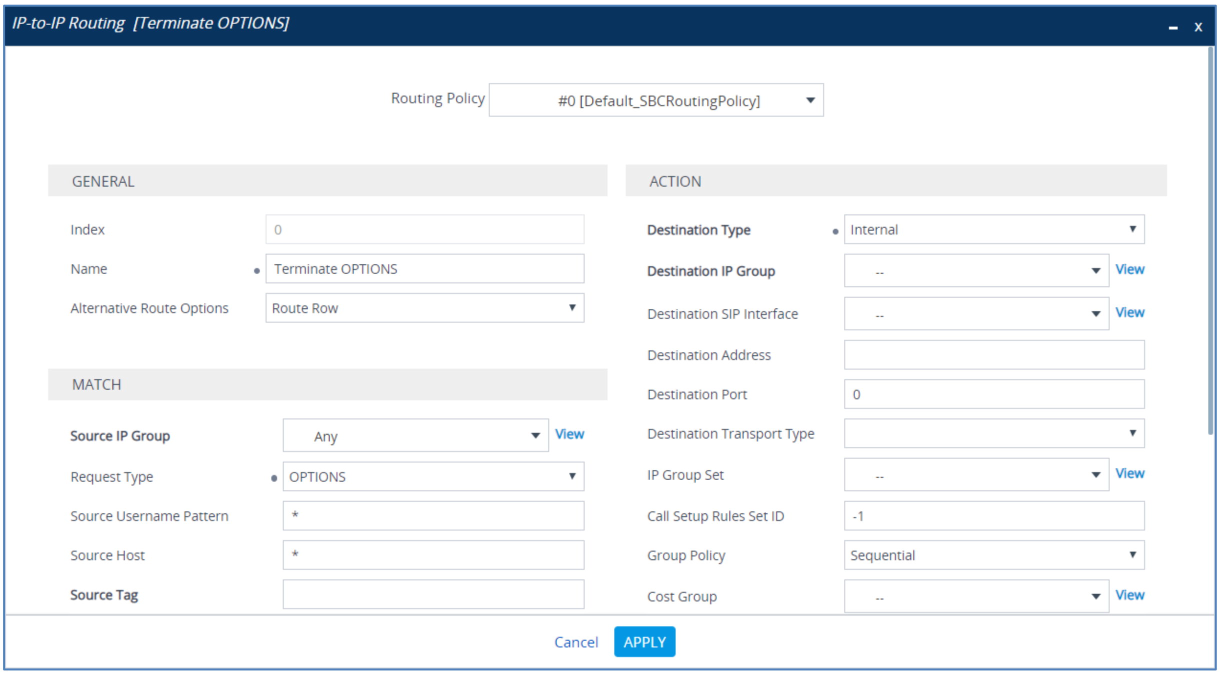
3.7.2 Configure IP-to-IP Call Routing Rules for Terminating SBC

➢ **To configure IP-to-IP routing rules for Terminating SBC:**

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 any entity:
   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	**Internal**
Internal Action	**Reply (Response='200')**

Figure 3-24: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS

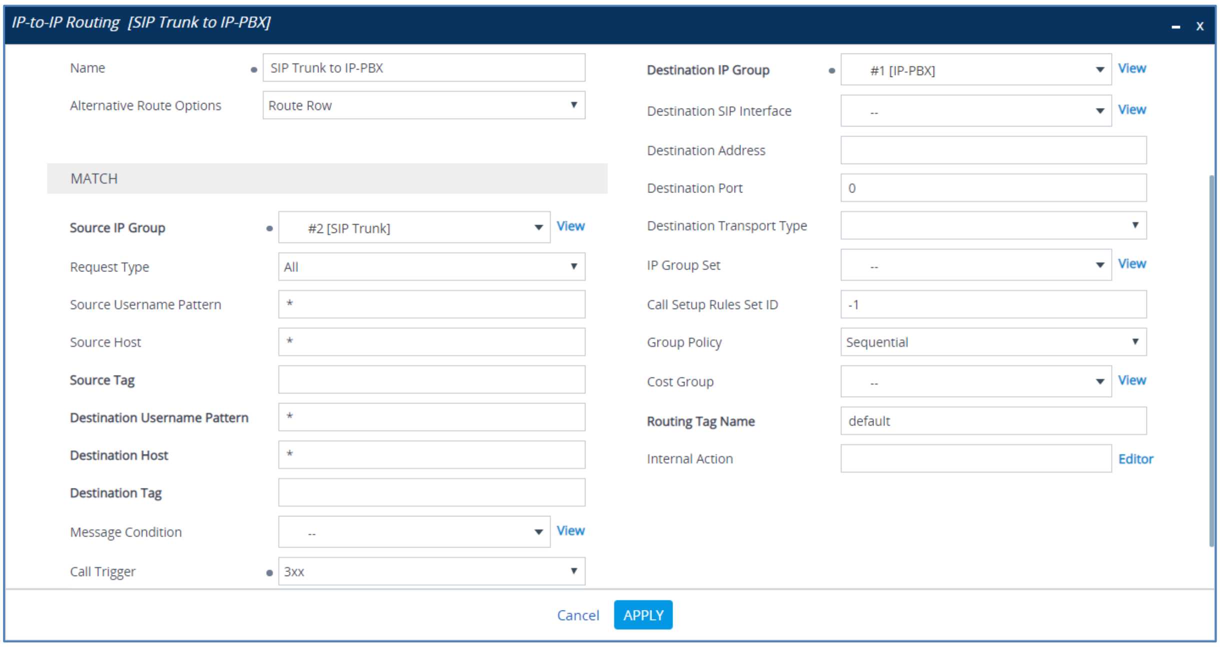


   b. Click **Apply**.

4. Configure a rule to re-route messages from IP-PBX towards SIP Trunk after receiving SIP 3xx response from ClearIP software platform:
   a. Click **New**, and then configure the parameters as follows:

Parameter	Value
Index	**1**
Route Name	**SIP Trunk to IP-PBX** (arbitrary descriptive name)
Source IP Group	**SIP Trunk**
Call Triger	**3xx**
Destination Type	**IP Group**
Destination IP Group	**IP-PBX**

Figure 3-25: Configuring IP-to-IP Routing Rule for Re-Routing after Receiving 3xx



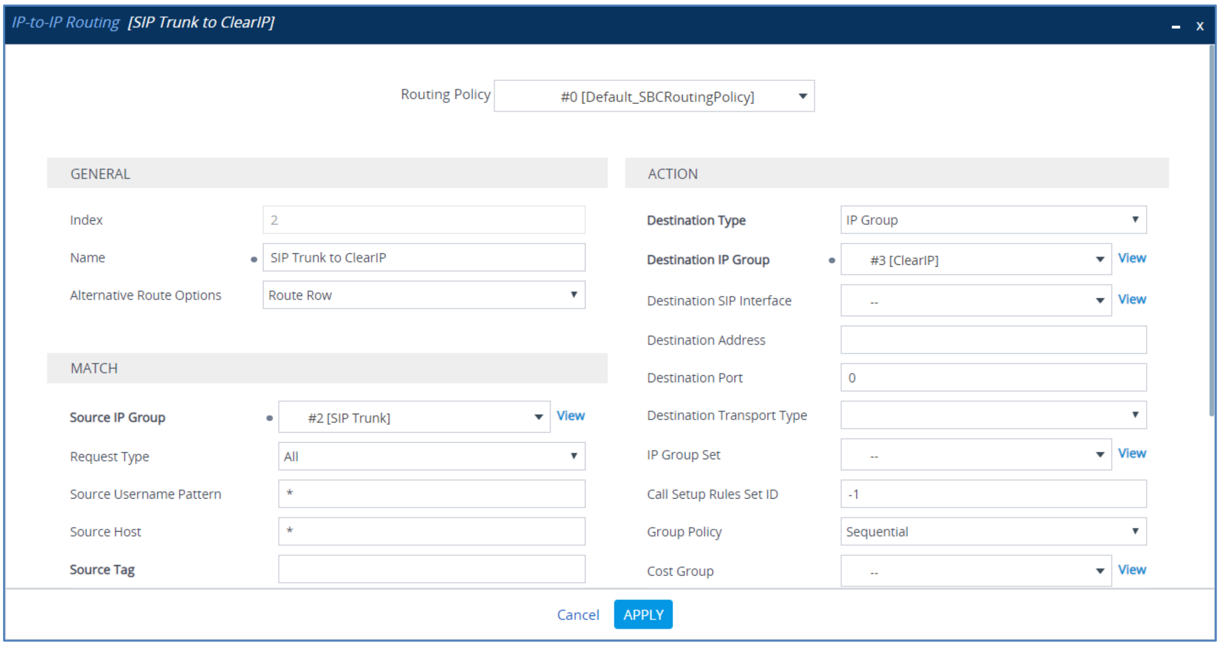
   c. Click **Apply**.

5. Configure a rule to route calls from SIP Trunk to the ClearIP platform:

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

Parameter	Value
Index	**2**
Route Name	**SIP Trunk to ClearIP** (arbitrary descriptive name)
Source IP Group	**SIP Trunk**
Destination Type	**IP Group**
Destination IP Group	**ClearIP**

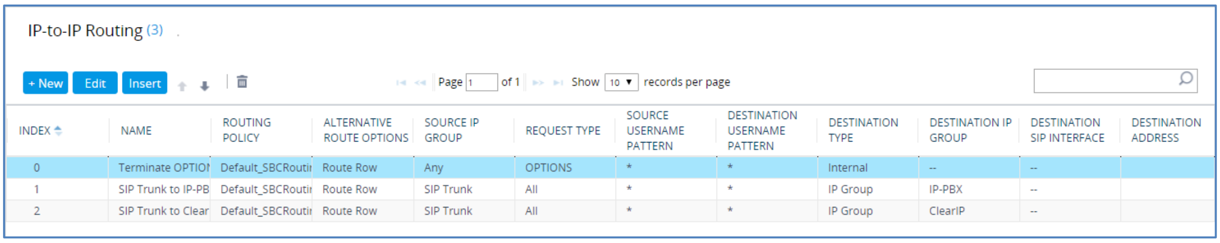
Figure 3-26: Configuring IP-to-IP Routing Rule for SIP Trunk to ClearIP



   b. Click **Apply**.

The configured routing rules are shown in the figure below:

Figure 3-27: Example of the Configured IP-to-IP Routing Rules in the Terminating SBC



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

3.8 Configure Message Manipulation Rules

This section 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.

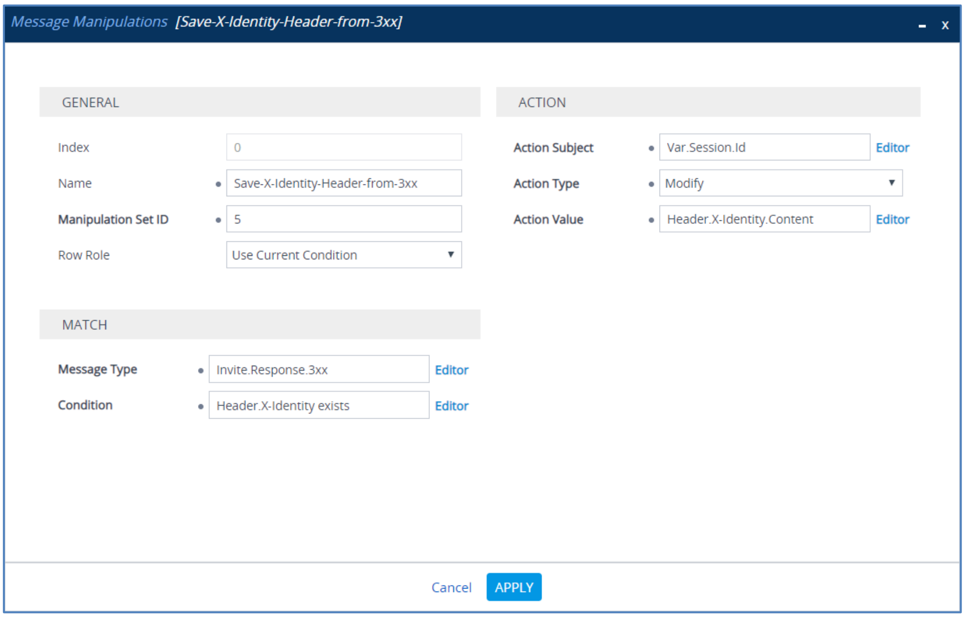
3.8.1 Configure Message Manipulation Rules for Originating SBC

➢ **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 5) for ClearIP. This rule applies to messages received from ClearIP IP Group. This save the content of the X-Identity header (if it exists) from the SIP 302 response for further usage.

Parameter	Value
Index	**0**
Name	**Save-X-Identity-Header-from-3xx**
Manipulation Set ID	**5**
Message Type	**Invite.Response.3xx**
Condition	**Header.X-Identity exists**
Action Subject	**Var.Session.Id**
Action Type	**Modify**
Action Value	**Header.X-Identity.Content**

Figure 3-28: Configuring SIP Message Manipulation Rule 5 (for ClearIP)



3. Configure another manipulation rule (Manipulation Set 4) for SIP Trunk. This rule is applied to any request messages sent to the SIP Trunk IP Group. This add SIP Identity Header to all messages sent to SIP Trunk, with the content, saved from the SIP 302 response.

Parameter	Value
Index	**1**
Name	**Add-Identity-to-Invite**
Manipulation Set ID	**4**
Message Type	**Invite.Request**
Condition	**Var.Session.Id != ''**
Action Subject	**Header.Identity**
Action Type	**Add**
Action Value	**Var.Session.Id**

Figure 3-29: Configuring SIP Message Manipulation Rule 1 (for SIP Trunk)

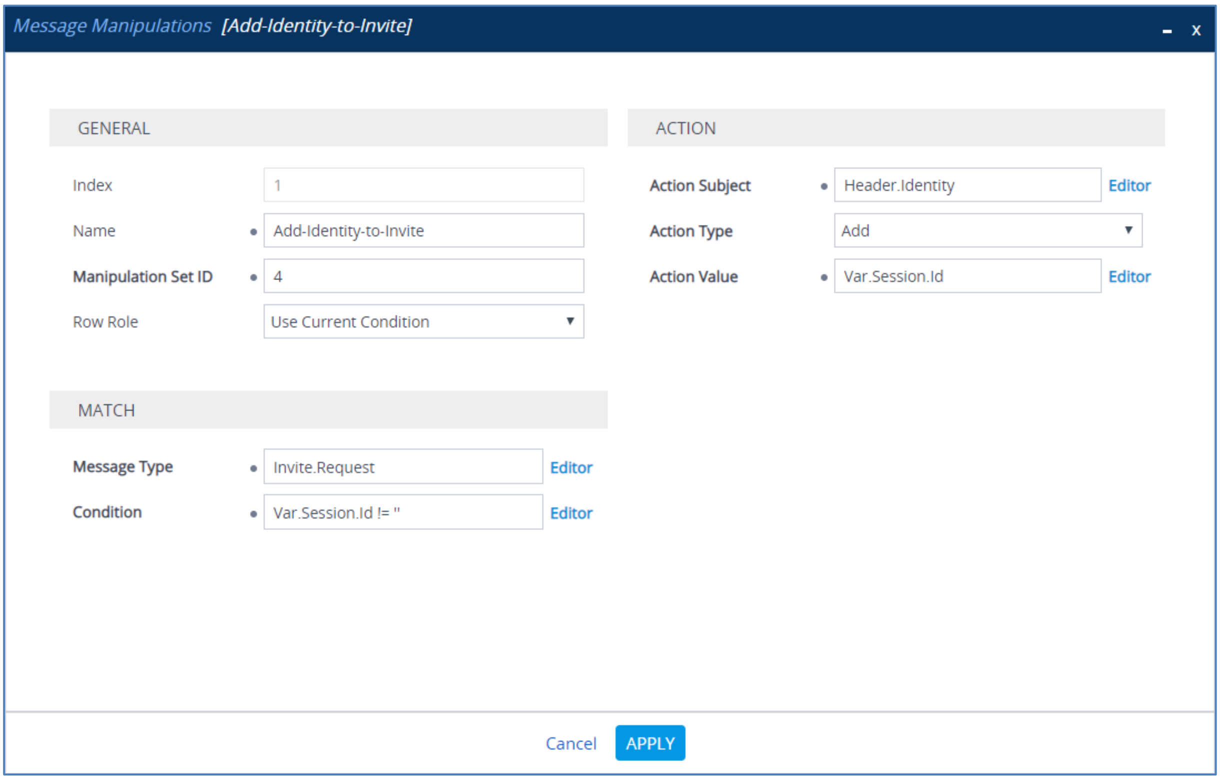
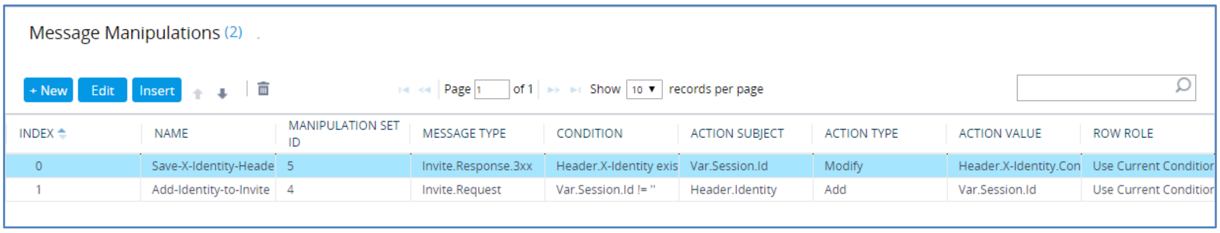


Figure 3-30: Example of Configured SIP Message Manipulation Rules for Originating SBC



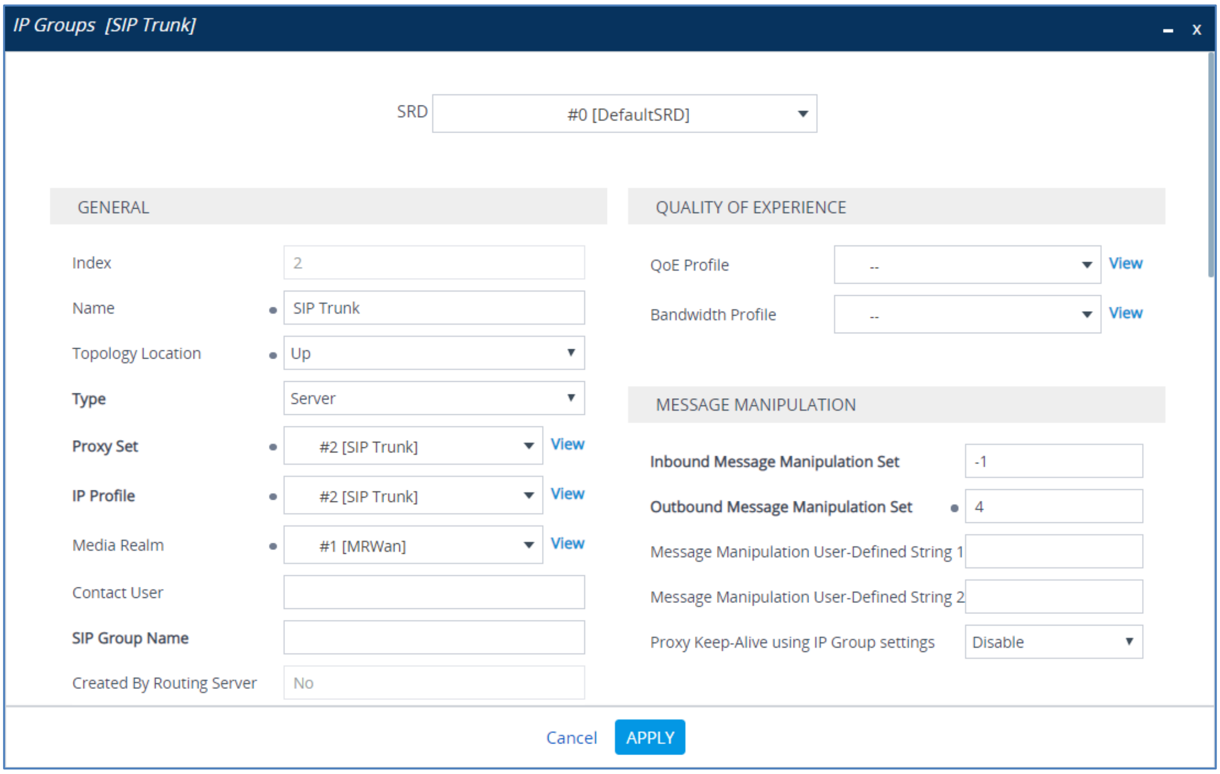
4. Assign Manipulation Set ID 4 to the SIP trunk IP Group:

a. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).

b. Select the row of the SIP trunk IP Group, and then click **Edit**.

c. Set the 'Outbound Message Manipulation Set' field to **4**.

Figure 3-31: Assigning Manipulation Set to the SIP Trunk IP Group



d. Click **Apply**.

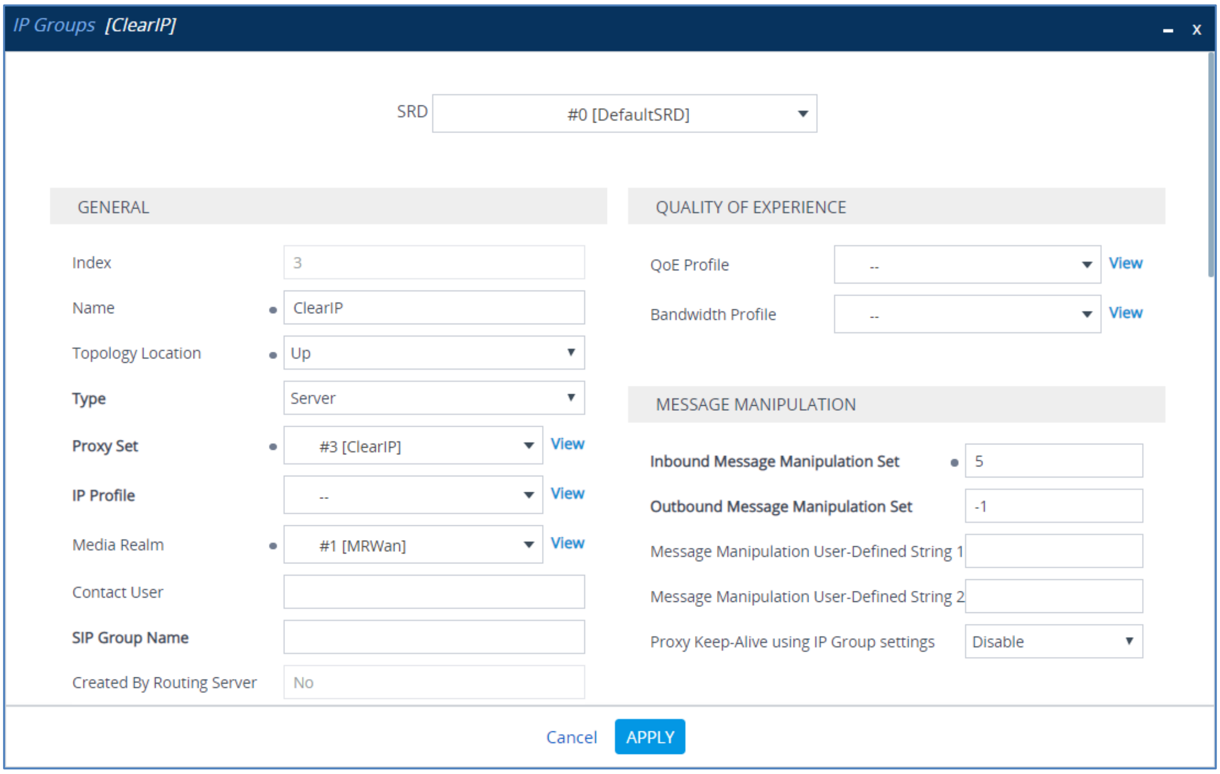
5. Assign Manipulation Set ID 5 to the ClearIP IP Group:

   a. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).

   b. Select the row of the ClearIP IP Group, and then click **Edit**.

   c. Set the 'Inbound Message Manipulation Set' field to **5**.

Figure 3-32: Assigning Manipulation Set 5 to the ClearIP IP Group



   d. Click **Apply**.

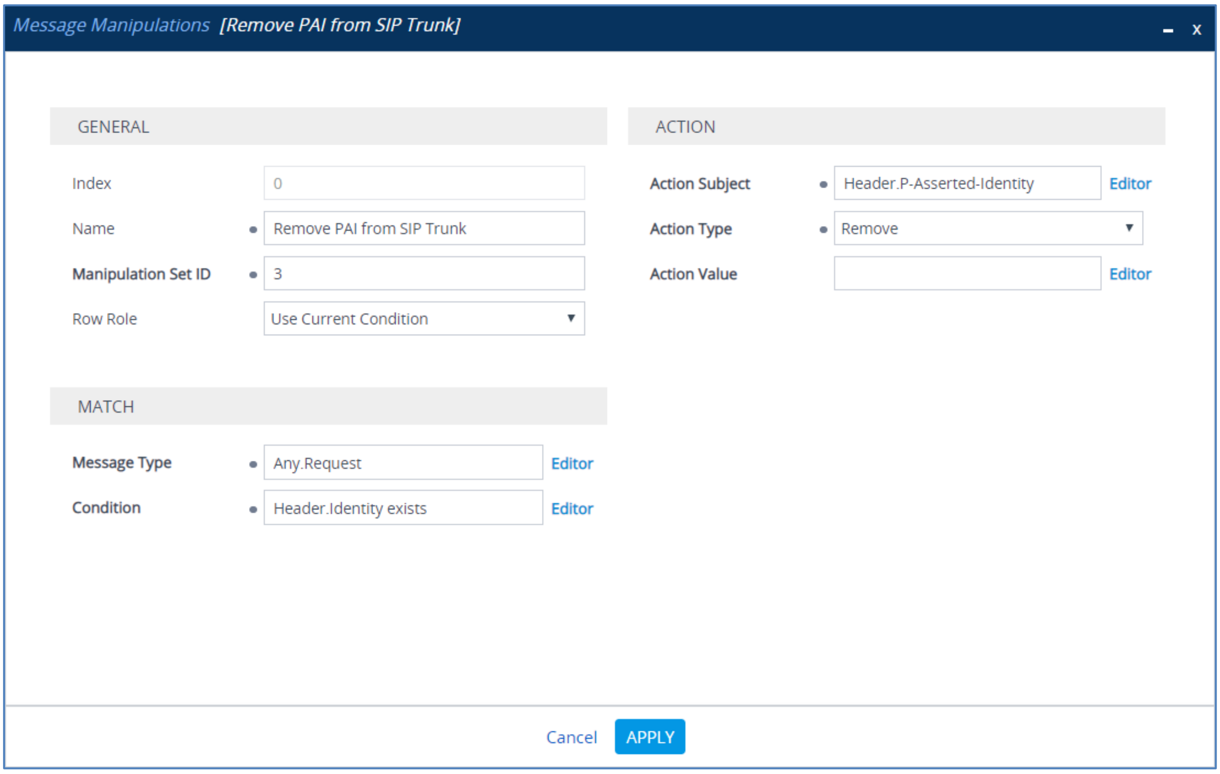
3.8.2 Configure Message Manipulation Rules for Terminating SBC

➢ **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 3) for SIP Trunk. This rule applies to messages received from the SIP Trunk IP Group. This removes the SIP P-Asserted-Identity Header from any message, if the SIP Identity Header exists.

Parameter	Value
Index	**0**
Name	**Remove PAI from SIP Trunk**
Manipulation Set ID	**3**
Message Type	**Any.Request**
Condition	**Header.Identity exists**
Action Subject	**Header.P-Asserted-Identity**
Action Type	**Remove**

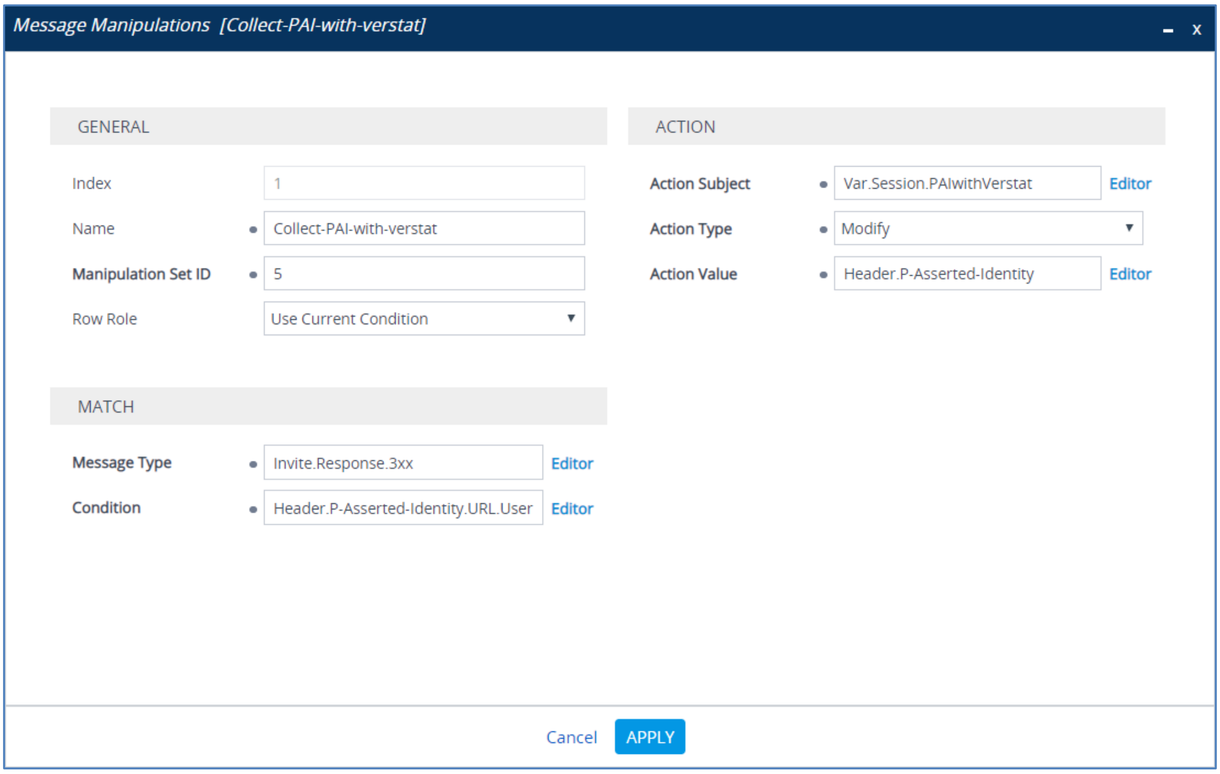
Figure 3-33: Configuring SIP Message Manipulation Rule 3 (for SIP Trunk)



3. Configure another manipulation rule (Manipulation Set 5) for ClearIP. This rule is applied to any 3xx responses received from the ClearIP IP Group. This saves the content of the user part of the SIP P-Asserted-Identity Header received from ClearIP (if it contains string ';verstat=TN-Validation-Passed') for further usage.

Parameter	Value
Index	**1**
Name	**Collect-PAI-with-verstat**
Manipulation Set ID	**5**
Message Type	**Invite.Response.3xx**
Condition	**Header.P-Asserted-Identity.URL.User regex (.*)(;verstat=TN-Validation-Passed)**
Action Subject	**Var.Session.PAIwithVerstat**
Action Type	**Modify**
Action Value	**Header.P-Asserted-Identity**

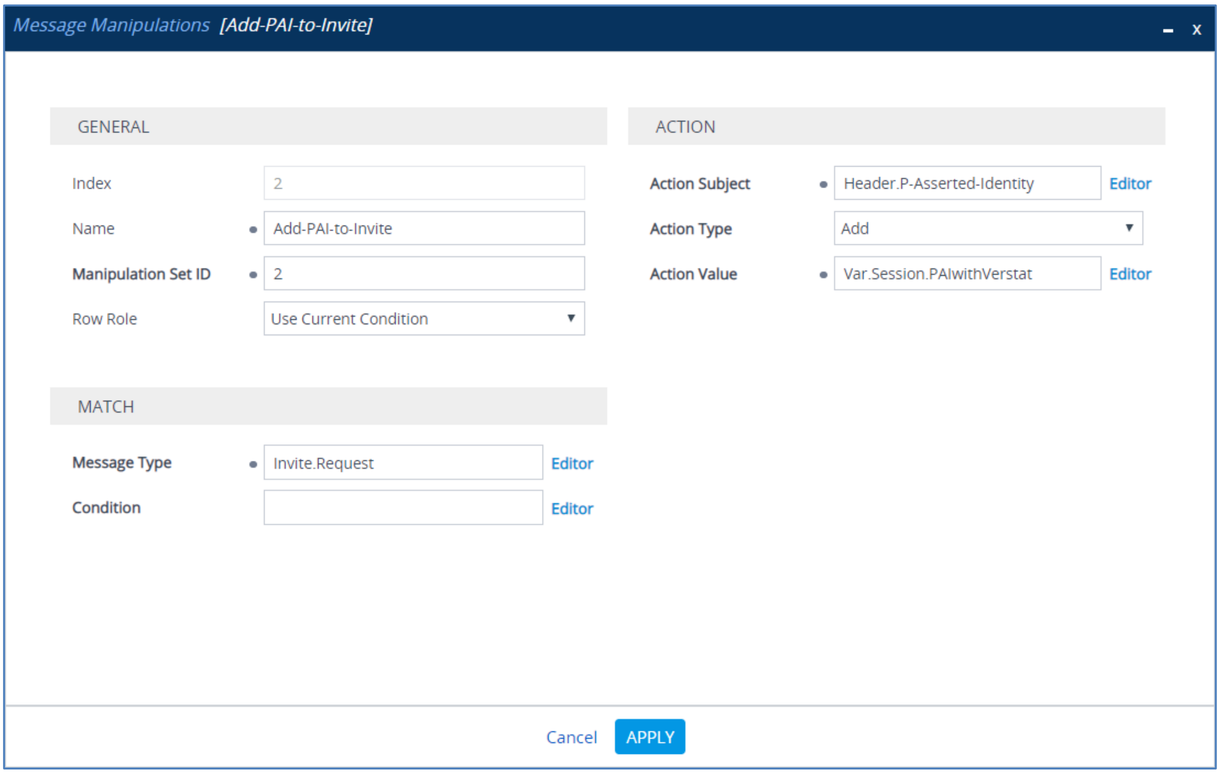
Figure 3-34: Configuring SIP Message Manipulation Rule 1 (for SIP Trunk)



4. Configure another manipulation rule (Manipulation Set 2) for IP-PBX. This rule is applied to messages sent to the IP-PBX IP Group. This adds the SIP P-Asserted-Identity Header to all INVITE request messages sent to the IP-PBX, with the content, saved from the SIP 302 response.

Parameter	Value
Index	**2**
Name	**Add-PAI-to-Invite**
Manipulation Set ID	**2**
Message Type	**Invite.Request**
Action Subject	**Header.P-Asserted-Identity**
Action Type	**Add**
Action Value	**Var.Session.PAIwithVerstat**

Figure 3-35: Configuring SIP Message Manipulation Rule 2 (for IP-PBX)



5. If it's required by the customer, configure another manipulation rule (Manipulation Set 2) for IP-PBX. This rule is applied to messages sent to the IP-PBX IP Group. This removes the SIP Identity Header (if it's exists) from any messages sent to the IP-PBX.

Parameter	Value
Index	**3**
Name	**Remove Identity**
Manipulation Set ID	**2**
Message Type	**Any.Request**
Condition	**Header.Identity exists**
Action Subject	**Header.Identity**
Action Type	**Remove**

Figure 3-36: Configuring SIP Message Manipulation Rule 3 (for IP-PBX)

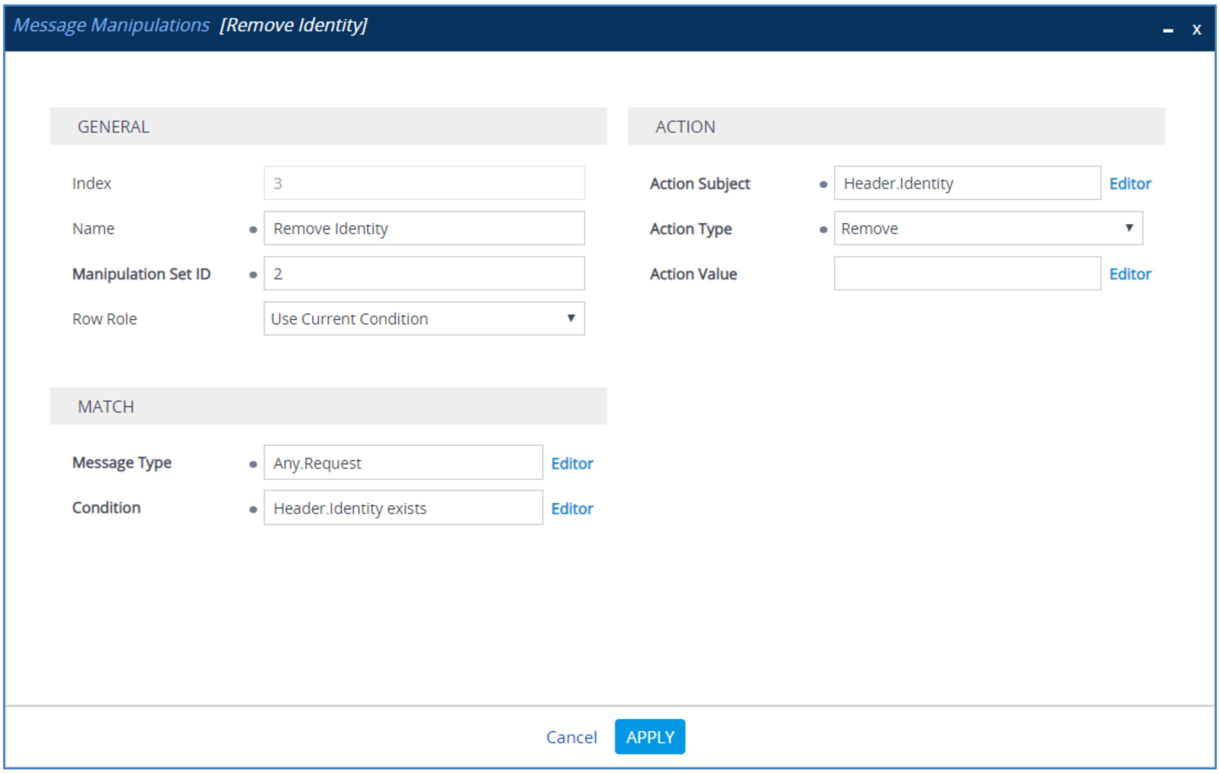
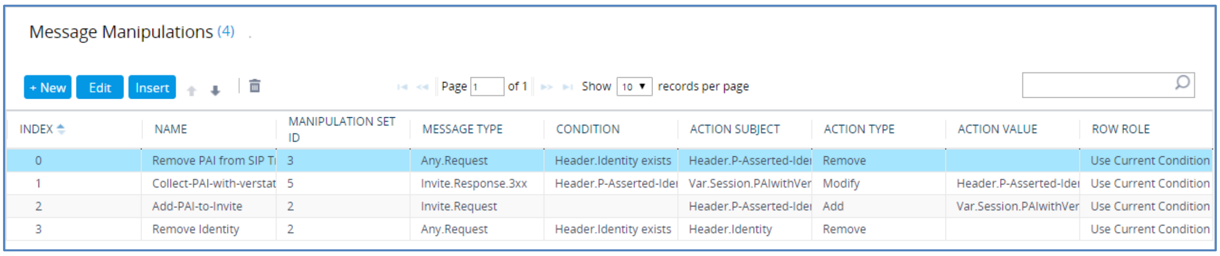


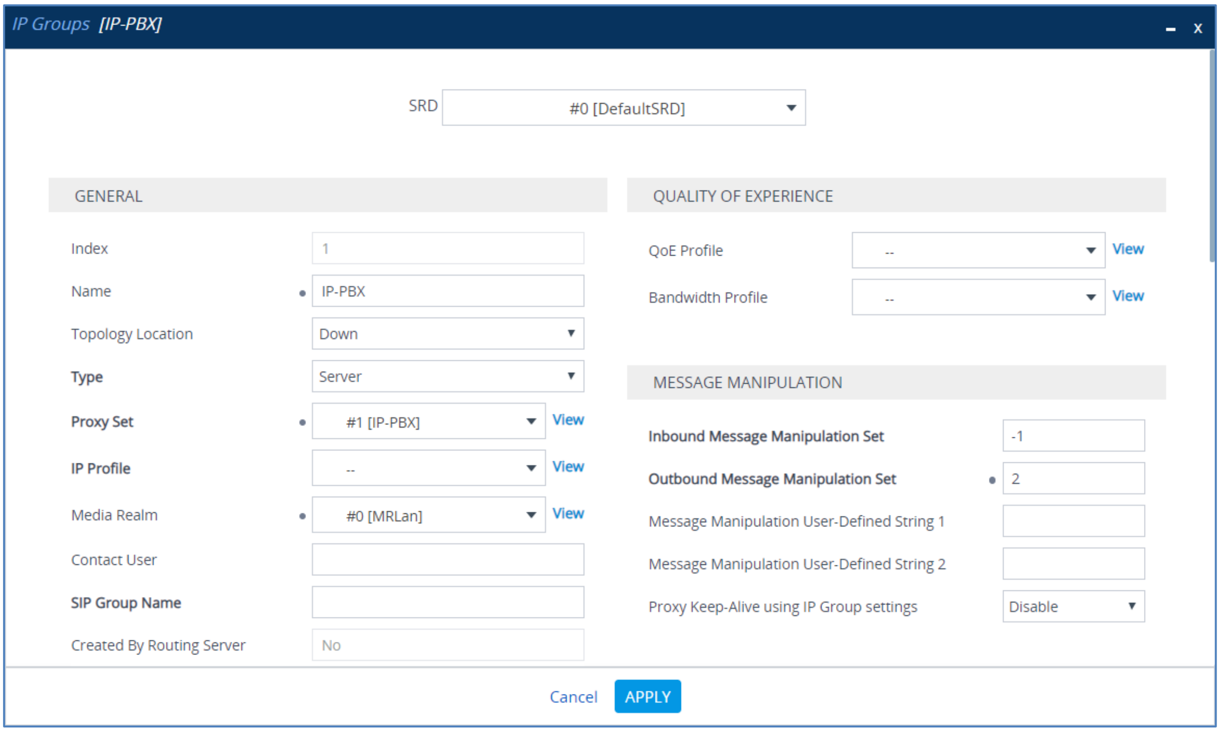
Figure 3-37: Example of Configured SIP Message Manipulation Rules for Terminating SBC



INDEX	NAME	MANIPULATION SET ID	MESSAGE TYPE	CONDITION	ACTION SUBJECT	ACTION TYPE	ACTION VALUE	ROW ROLE
0	Remove PAI from SIP Ti	3	Any.Request	Header.Identity exists	Header.P-Asserted-Ide	Remove		Use Current Condition
1	Collect-PAI-with-verstat	5	Invite.Response.3xx	Header.P-Asserted-Ide	Var.Session.PAIwithVer	Modify	Header.P-Asserted-Ide	Use Current Condition
2	Add-PAI-to-Invite	2	Invite.Request		Header.P-Asserted-Ide	Add	Var.Session.PAIwithVer	Use Current Condition
3	Remove Identity	2	Any.Request	Header.Identity exists	Header.Identity	Remove		Use Current Condition

6. Assign Manipulation Set ID 2 to the IP-PBX IP Group:
   a. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
   b. Select the row of the IP-PBX IP Group, and then click **Edit**.
   c. Set the 'Outbound Message Manipulation Set' field to **2**.

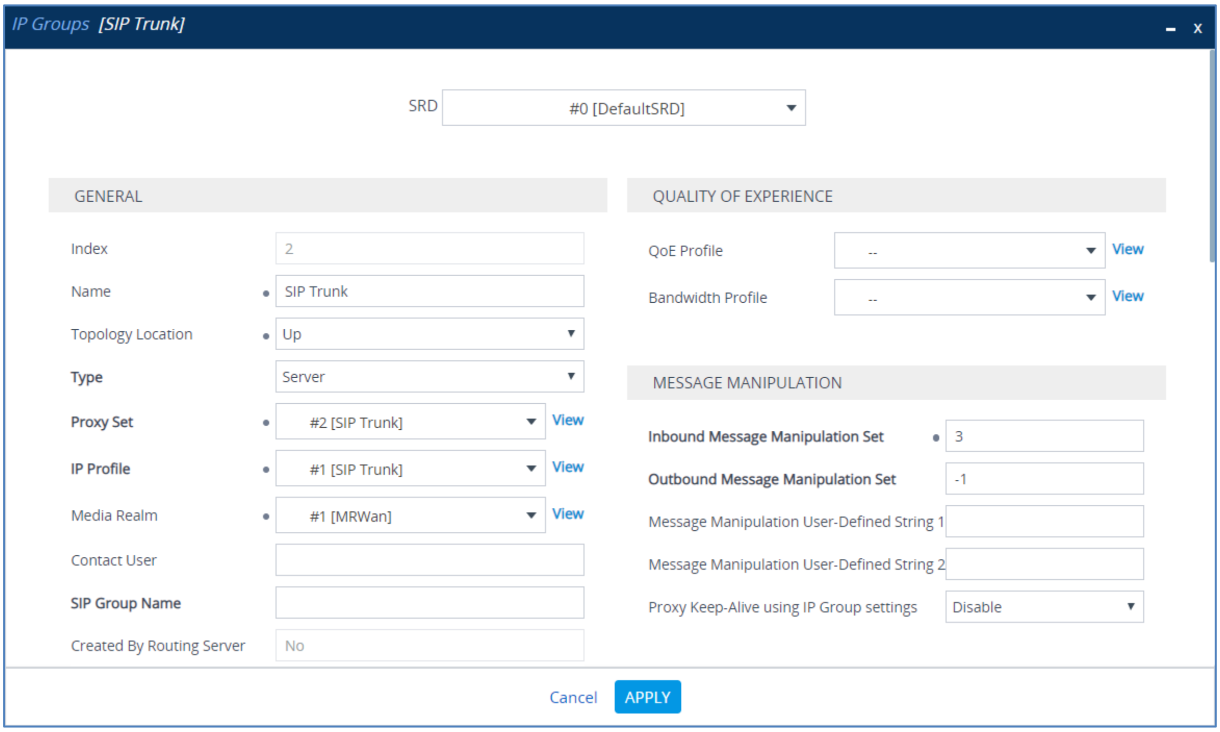
Figure 3-38: Assigning Manipulation Set to the IP-PBX IP Group



   d. Click **Apply**.

7. Assign Manipulation Set ID 3 to the 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 SIP Trunk IP Group, and then click **Edit**.
   c. Set the 'Inbound Message Manipulation Set' field to **3**.

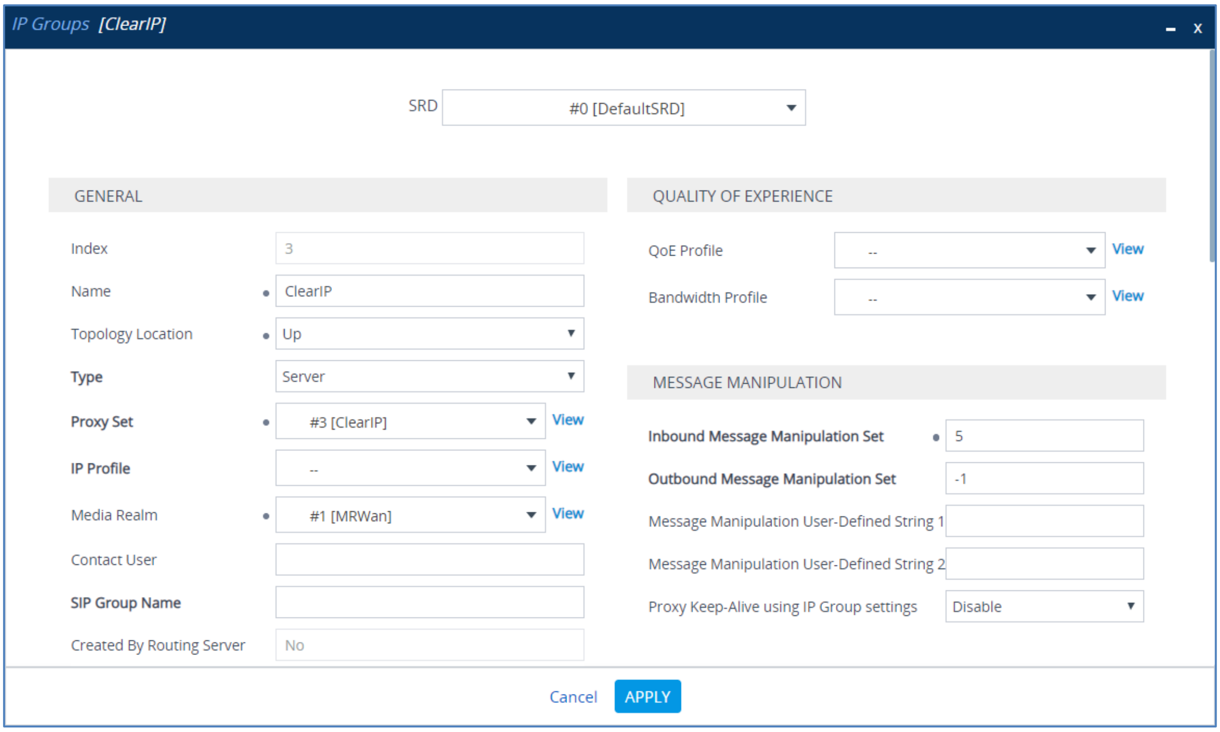
Figure 3-39: Assigning Manipulation Set 3 to the SIP Trunk IP Group



   d. Click **Apply**.

8. Assign Manipulation Set ID 5 to the ClearIP IP Group:
   a. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
   b. Select the row of the ClearIP IP Group, and then click **Edit**.
   c. Set the 'Inbound Message Manipulation Set' field to **5**.

Figure 3-40: Assigning Manipulation Set 5 to the ClearIP IP Group



   d. Click **Apply**.

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/

©2019 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway to VoIP, 3GX, VocaNom, AudioCodes One Voice and CloudBond are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

Document #: LTRT-13250