

Connecting ShoreTel IP-PBX to BroadCloud SIP Trunk using AudioCodes Mediant™ E-SBC

Version 7.0



Table of Contents

1	Introduction	7
1.1	Intended Audience	7
1.2	About AudioCodes E-SBC Product Series.....	7
2	Component Information.....	9
2.1	IP-PBX Version	9
2.2	AudioCodes E-SBC Version	9
2.3	BroadCloud SIP Trunking Version	9
2.4	Interoperability Test Topology	10
2.4.1	Environment Setup	11
2.4.2	Known Limitations.....	11
3	Configuring ShoreTel IP-PBX.....	13
3.1	ShoreTel System Settings – General	13
3.2	Call Control Options	13
3.3	Sites Settings.....	15
3.4	Switch Settings - Allocating Ports for SIP Trunks.....	17
3.5	ShoreTel System Settings – Trunk Groups	19
3.6	SIP PSTN Trunk Group for BroadCloud	20
3.7	ShoreTel System Settings – Individual Trunks.....	21
3.8	Edit BroadCloud SIP Trunk Group.....	22
4	Configuring AudioCodes E-SBC.....	25
4.1	Step 1: IP Network Interfaces Configuration	26
4.1.1	Step 1a: Configure VLANs.....	27
4.1.2	Step 1b: Configure Network Interfaces.....	27
4.2	Step 2: Enable the SBC Application	29
4.3	Step 3: Configure Media Realms	30
4.4	Step 4: Configure SIP Signaling Interfaces.....	32
4.5	Step 5: Configure Proxy Sets	34
4.6	Step 6: Configure IP Profiles	38
4.7	Step 7: Configure IP Groups.....	44
4.8	Step 8: Configure IP-to-IP Call Routing Rules	46
4.9	Step 9: Configure IP-to-IP Manipulation Rules.....	53
4.10	Step 10: Configure Message Manipulation Rules	56
4.11	Step 11: Configure Registration Accounts	61
4.12	Step 12: Miscellaneous Configuration.....	62
4.12.1	Step 12a: Configure SBC Alternative Routing Reasons	62
4.13	Step 13: Reset the E-SBC	63
A	AudioCodes INI File	65

This page is intentionally left blank.

Notice

This document describes how to connect the IP-PBX and BroadCloud SIP Trunk using AudioCodes Mediant E-SBC product series.

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 and other documents as well as software files can be viewed by registered customers at <http://www.audiocodes.com/downloads>.

© Copyright 2016 AudioCodes Ltd. All rights reserved.

This document is subject to change without notice.

Date Published: February-3-2016

Trademarks

AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNOM and CloudBond 365 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.

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 www.audiocodes.com/support.

Document Revision Record

LTRT	Description
12560	Initial document release for Version 7.0.

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 <http://www.audiocodes.com/downloads>.

1 Introduction

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

1.1 Intended Audience

The document is intended for engineers, or AudioCodes and BroadCloud Partners who are responsible for installing and configuring BroadCloud'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 IP-PBX Version

Table 2-1: IP-PBX Version

Vendor	ShoreTel
Model	ShoreGear
Software Version	14.2_Build_19.45.8701.0
Protocol	SIP/UDP
Additional Notes	None

2.2 AudioCodes E-SBC Version

Table 2-2: AudioCodes E-SBC Version

SBC Vendor	AudioCodes
Models	▪ Mediant 500 E-SBC ▪ Mediant 800 Gateway & E-SBC ▪ Mediant 1000B Gateway & E-SBC ▪ Mediant 3000 Gateway & E-SBC ▪ Mediant 2600 E-SBC ▪ Mediant 4000 E-SBC
Software Version	SIP_F7.00A.049.003
Protocol	SIP/UDP (to the both BroadCloud SIP Trunk and IP-PBX)
Additional Notes	None

2.3 BroadCloud SIP Trunking Version

Table 2-3: BroadCloud Version

Vendor/Service Provider	BroadCloud
SSW Model/Service	BroadWorks
Software Version	21
Protocol	SIP/UDP
Additional Notes	None

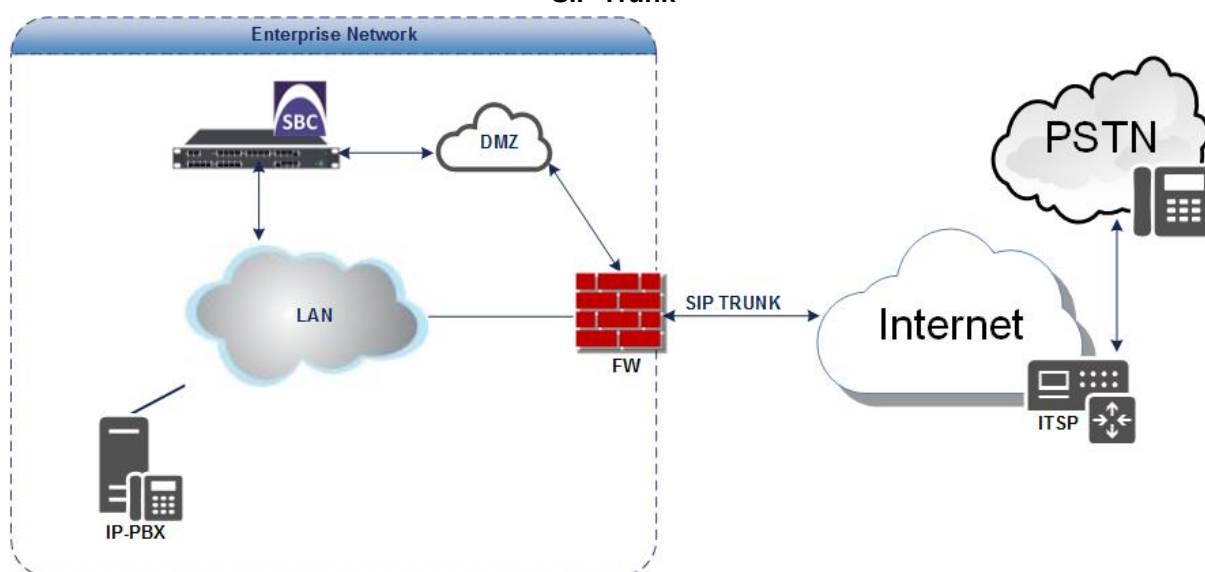
2.4 Interoperability Test Topology

The interoperability testing between AudioCodes E-SBC and BroadCloud SIP Trunk with 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 BroadCloud'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 BroadCloud'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 BroadCloud 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 is located on the Enterprise's LAN ▪ BroadCloud SIP Trunk is located on the WAN
Signaling Transcoding	▪ IP-PBX operates with SIP-over-UDP transport type ▪ BroadCloud SIP Trunk operates with SIP-over-UDP transport type
Codecs Transcoding	▪ IP-PBX supports G.711A-law, G.711U-law, and G.729 coder ▪ BroadCloud SIP Trunk supports G.711A-law, G.711U-law, and G.729 coder
Media Transcoding	▪ IP-PBX operates with RTP media type ▪ BroadCloud SIP Trunk operates 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 IP-PBX and BroadCloud 's SIP Trunk.

This page is intentionally left blank.

3 Configuring ShoreTel IP-PBX

This chapter describes how to configure basic parameters of the ShoreTel ShoreGear IP-PBX to operate with AudioCodes E-SBC.



Note: For more complicated configuration parameters please refer to User Manual of each IP-PBX.

3.1 ShoreTel System Settings – General

The first settings to address within the ShoreTel system are the general system settings. These configurations include the Call Control, the Site and the Switch settings. If these items have already been configured on your system, skip this section and go on to Section 3.5 on page 19 below.

3.2 Call Control Options

The first settings to configure within ShoreTel Director are the Call Control Options. To configure these settings for the ShoreTel system, log into ShoreTel Director and select **Administration > Call Control > Options**. The Call Control Options screen appears below.

Figure 3-1: Call Control Options Screen

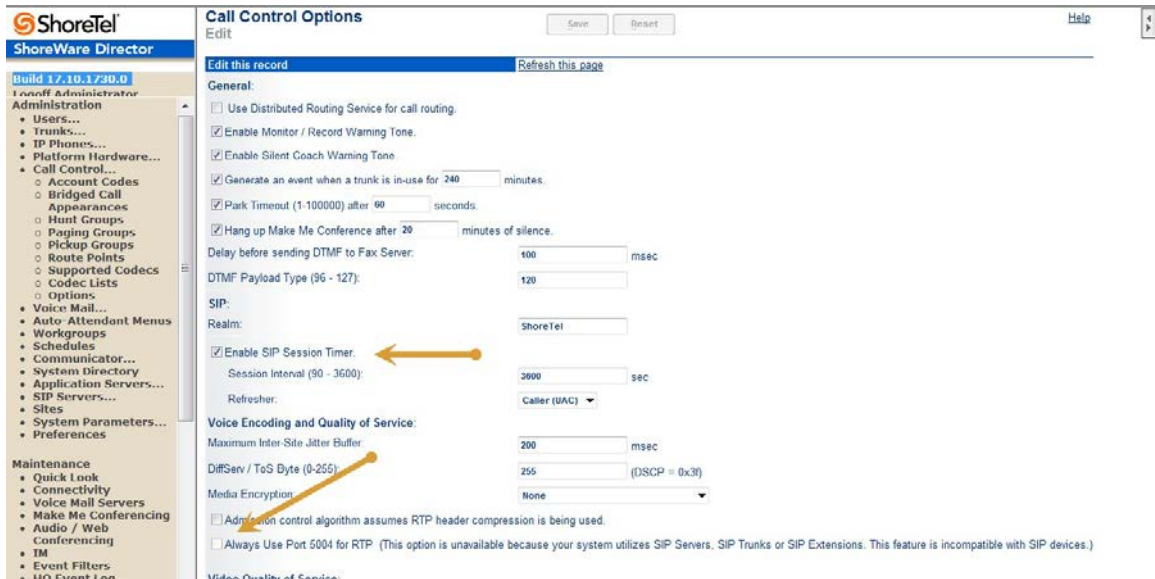
Within the Call Control Options SIP parameters, confirm that the appropriate settings are made for the Realm, Enable SIP Session Timer and Always Use Port 5004 for RTP parameters.

The 'Realm' parameter is used in authenticating all SIP devices. It is typically a description of the computer or system being accessed. Changing this value will require a reboot of all ShoreTel switches serving SIP extensions. It is not necessary to modify this parameter to get the ShoreTel IP PBX system functional with AudioCodes gateway.

➤ **To configure Call Control Options:**

1. Verify that the 'Enable SIP Session Timer' check box is selected.
2. Set the Session Interval Time to the recommended setting of 3600 seconds.
3. Select the appropriate refresher (from the pull down menu) for the SIP Session Timer. The "Refresher" field will be set either to "Caller (UAC)" [User Agent Client] or to "Callee (UAS)" [User Agent Server]. If the "Refresher" field is set to "Caller (UAC)", the Caller's device will be in control of the session timer refresh. If "Refresher" is set to "Callee (UAS)", the device of the person called will control the session timer refresh.
4. Verify the "Voice Encoding and Quality of Service", specifically the "Media Encryption" parameter. Make sure this parameter is set to "None"; otherwise you may experience one-way audio issues. Please refer to *ShoreTel Administration Guide* for additional details on media encryption and the other parameters in the "Voice Encoding and Quality of Service" area.
5. Disable (uncheck) the "Always Use Port 5004 for RTP" parameter if checked; it is required for implementing SIP trunks between ShoreTel systems only. For SIP configurations, Dynamic User Datagram Protocol (UDP) must be used for RTP Traffic. If the parameter is disabled, Media Gateway Control Protocol (MGCP) no longer uses UDP port 5004; MGCP and SIP traffic will use dynamic UDP ports (**Figure 3**).

Figure 3-2: Call Control Options Settings



The screenshot shows the 'Call Control Options' configuration page in the ShoreTel ShoreWare Director. The left sidebar shows the navigation tree with 'Call Control' selected. The main content area is divided into sections: General, SIP, and Voice Encoding and Quality of Service. In the General section, the 'Enable SIP Session Timer' checkbox is checked, and the 'Session Interval' is set to 3600 seconds. In the SIP section, the 'Refresher' dropdown is set to 'Caller (UAC)'. In the Voice Encoding and Quality of Service section, the 'Media Encryption' dropdown is set to 'None'. Two yellow arrows point to these specific settings.

6. Once this parameter is unchecked, make sure that "everything" (IP Phones, ShoreTel Voice Switches, ShoreTel Server, Distributed Voice Mail Servers / Remote Servers, Conference Bridges and Contact Centers) is "fully" rebooted – this is a "one time only" item. By not performing a full system reboot after changing this setting, one-way audio may occur during initial testing.
7. Be sure to save your changes before leaving this screen by clicking Save at the top of the page.

3.3 Sites Settings

The next settings to address are the administration of sites. These settings are modified under the ShoreTel Director by selecting **Administration > Sites**. The **Sites** screen appears.

➤ **To configure Sites:**

1. Within the Sites screen select the name of the site to configure. The Edit Site screen will then appear. The only changes required to the Edit Site screen are to the 'Admission Control Bandwidth', 'Intra-Site Calls' and 'Inter-Site Calls' parameters.

Figure 3-3: Site Bandwidth settings

2. Set the appropriate Admission Control Bandwidth for your network. Please refer to the *ShoreTel Planning and Installation Guide* for additional information on setting Admission Control Bandwidth for your network. Admission Control Bandwidth defines the bandwidth available to and from the site. This is important as SIP trunk calls will be counted against the site bandwidth.



Note: Bandwidth of 2046 kbps is just an example.

3. From the 'Inter-Site Calls' drop-down list, select **Very Low Bandwidth Codecs**. By default, **Very Low Bandwidth Codecs** contains two codecs - G.729 and G.711u - with G.729 being the primary codec of choice. The 'Inter-Site Calls' parameter defines which codecs will be used when establishing a call with AudioCodes – the preferred codec choice is G.729.



Note: Please do not modify the "Very Low Bandwidth Codecs" codec list.

4. Save changes before leaving this screen by clicking **Save** at the top of the page.

3.4 Switch Settings - Allocating Ports for SIP Trunks

The final general settings to configure are the ShoreTel Switch settings.

➤ **To configure ShoreTel Switch settings:**

1. Navigate to the Primary Voice Switches/Service Appliances screen by selecting **Administration > Switches > Primary** in ShoreTel Director, as shown in the figure below.

Figure 3-4: Administration Switches

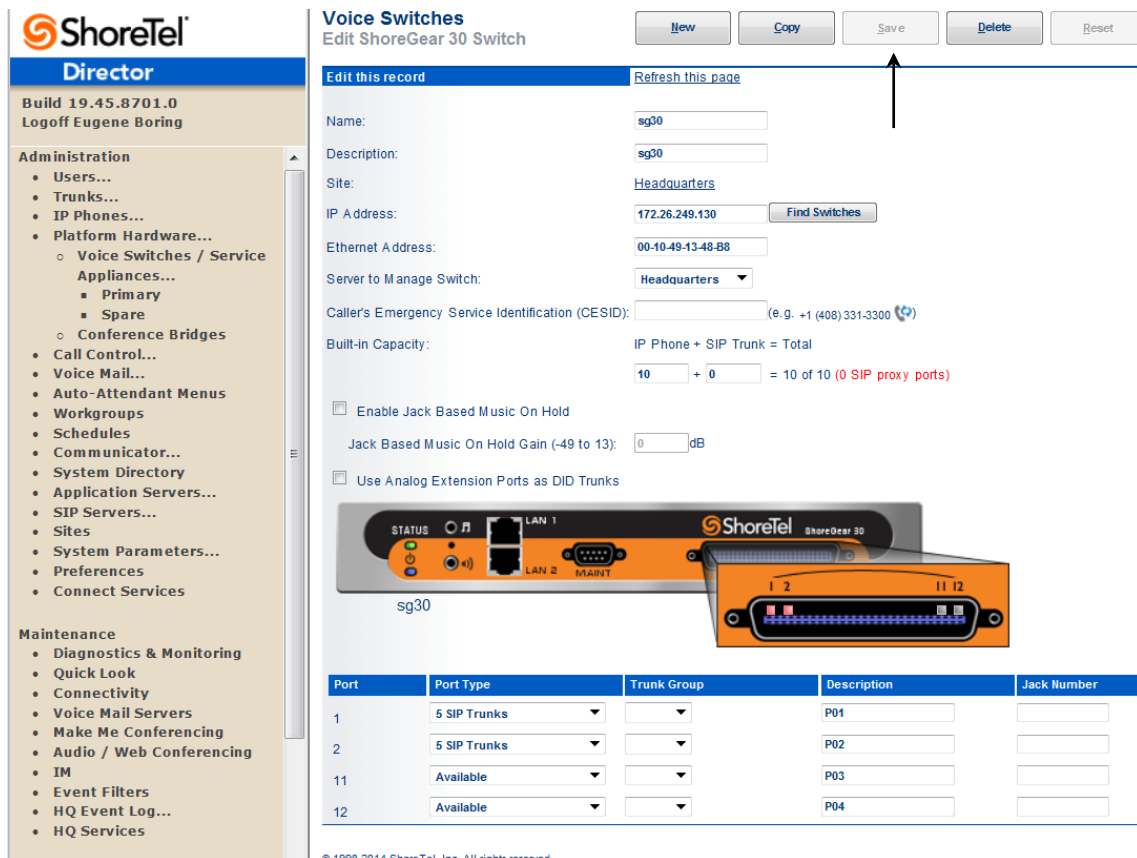
Primary Voice Switches / Service Appliances

Add new switch/appliance at site: of type: [Go](#)

Name	Quick Launch	Description	Site	Server	Database Server	Type	IP Address	MAC Address	Serial Number	IP Phones In Use	IP Phones Capacity
pbxlab40/8		pbxlab40/8	Headquarters	Headquarters		40/8	172.26.249.4	00-10-49-08-0D-F7	08JC08070B0DF7	13	20
sg30		sg30	Headquarters	Headquarters		SG-30	172.26.249.130	00-10-49-13-48-B8	S30J09321348B8	0	10
shoretelcc1		shoretelcc1	Headquarters	shoretelcc1	Headquarters	SW	172.26.249.6			0	0
shoretelremote1		shoretelremote1	Headquarters	shoretelremote1	Headquarters	SW	172.26.249.7			0	0
shoretelremote2		shoretelremote2	Headquarters	shoretelremote2	Headquarters	SW	172.26.249.8			0	0
SoftSwitch		SoftSwitch	Headquarters	Headquarters	Headquarters	SW	172.26.249.3			0	0
Total										13	30

© 1998-2014 ShoreTel, Inc. All rights reserved.

2. From the Switches screen, choose the name of the switch to configure for SIP trunks; the Edit ShoreTel Switch screen appears.
3. On the Edit ShoreTel Switch screen, select the desired number of SIP Trunks from the available ports.

Figure 3-5: ShoreTel Switch Settings


Voice Switches
Edit ShoreGear 30 Switch

[New](#) [Copy](#) [Save](#) [Delete](#) [Reset](#)

[Edit this record](#) [Refresh this page](#)

Name: sg30

Description: sg30

Site: Headquarters

IP Address: 172.26.249.130 [Find Switches](#)

Ethernet Address: 00-10-49-13-48-B8

Server to Manage Switch: Headquarters

Caller's Emergency Service Identification (CESID): (e.g. +1 (408) 331-3300)

Built-in Capacity: IP Phone + SIP Trunk = Total
10 + 0 = 10 of 10 (0 SIP proxy ports)

☐ Enable Jack Based Music On Hold

Jack Based Music On Hold Gain (-49 to 13): 0 dB

☐ Use Analog Extension Ports as DID Trunks

sg30

Port	Port Type	Trunk Group	Description	Jack Number
1	5 SIP Trunks		P01	
2	5 SIP Trunks		P02	
11	Available		P03	
12	Available		P04	

© 1998-2014 ShoreTel, Inc. All rights reserved.

Each port designated as a Port Type of a SIP Trunk enables the support for five individual SIP trunks. Each trunk can support one concurrent call between the ShoreTel system and the BroadCloud SIP Trunk.

4. Determine the desired capacity of the interconnection between the two systems and configure the necessary resources as required, and then proceed to the next section.
5. Be sure to save your changes before leaving this screen by clicking **Save** at the top of the screen.

3.5 ShoreTel System Settings – Trunk Groups

ShoreTel Trunk Groups only support Static IP Addresses for Individual Trunks. In trunk planning, the following needs to be considered. AudioCodes gateway interfaces should always be configured to use a “static” IP Address.

The settings for Trunk Groups are changed by selecting **Administration > Trunks > Trunk Groups** within ShoreTel Director, as shown below.

Figure 3-6: Administration Trunk Groups

The screenshot displays the ShoreTel Director interface. On the left, the 'Administration' menu is expanded, showing 'Trunk Groups' as the selected option. The main area is titled 'Trunk Groups' and contains a table of existing trunk groups. Above the table, there is a form to 'Add new trunk group at site: Headquarters of type: SIP' with a 'Go' button highlighted by an arrow. The table lists various trunk types like Analog Loop Start, Digital Loop Start, and SIP Trunk, along with their respective sites, trunk counts, DIDs, destinations, and access codes.

Name	Type	Site	Trunks	DID	Destination	Access Code
Analog Loop Start	Analog Loop Start	Headquarters	2	No	700	9
Digital Loop Start	Digital Loop Start	Headquarters	0	No	700	9
Digital Vlink Start	Digital Vlink Start	Headquarters	0	No	700	9
SIP Trunk	SIP	Headquarters	5	Yes	700	80
SIP PSTN	SIP	Headquarters	5	Yes	700	81

➤ **To configure Trunk Groups:**

1. From the pull down menus on the Trunk Groups screen, select the site desired and select the **SIP** trunk type to configure.
2. Click on the **Go** link from **Add new trunk group at site**. The Edit SIP Trunk Group screen appears.

3.6 SIP PSTN Trunk Group for BroadCloud

Figure 3-7: BroadCloud SIP Trunk Group (SIP PSTN)


Director
Build 19.45.8701.0
Logoff Eugene Boring

- Administration
 - Users...
 - Trunks...
 - Individual Trunks
 - Trunk Groups
 - SIP Profiles
 - ISDN Profiles
 - Local Prefixes
 - IP Phones...
 - Platform Hardware...
 - Call Control...
 - Voice Mail...
 - Auto-Attendant Menus
 - Workgroups
 - Schedules
 - Communicator...
 - System Directory
 - Application Servers...
 - SIP Servers...
 - Sites
 - System Parameters...
 - Preferences
 - Connect Services
- Maintenance
 - Diagnostics & Monitoring
 - Quick Look
 - Connectivity
 - Voice Mail Servers
 - Make Me Conferencing
 - Audio / Web Conferencing
 - IM
 - Event Filters
 - HQ Event Log...
 - HQ Services
- Reporting
 - Reports...
 - Options
- Documentation
 - Administration Guide

Trunk Groups
Edit SIP Trunk Group

[New](#) [Copy](#) [Save](#) [Delete](#) [Print](#)

Edit this record

[Refresh this page](#)

Name: sip-trunk
Site: Headquarters
Language: English

☐ Enable SIP Info for G.711 DTMF Signaling
Profile: Default ITSP
Digest Authentication: <None>
Username:
Password:
Inbound:

Number of Digits from CO: 3
☒ DNS [Edit DNS Map](#)
☒ DID [Edit DID Range](#)
☒ Extension

☒ Translation Table: <None>
☐ Prepend Dial In Prefix:
☐ Use Site Extension Prefix

☒ Tandem Trunking
User Group: Executives
Prepend Dial In Prefix: 80
Destination: 700 : Default [Search](#)

☒ Outbound:
Network Call Routing:
Access Code: 81
Local Area Code: 732 [Edit](#)
Additional Local Area Codes: [Edit](#)
Nearby Area Codes: [Edit](#)
Billing Telephone Number: (8 00) +1 (408) 331-3300

Trunk Services:

☒ Local
☒ Long Distance
☒ International
☒ Enable Original Caller Information
☒ n11 (e.g. 411, 611, except 911 which is specified below)
☒ Emergency (e.g. 911)
☒ Easily Recognizable Codes (ERC) (e.g. 800, 888, 900)
☒ Explicit Carrier Selection (e.g. 1010xxx)
☒ Operator Assisted (e.g. 0*)
☒ Caller ID not blocked by default
☐ Enable Caller ID (Please confirm with the Carrier(s) or the Service Provider(s) on how the end-to-end caller name is delivered)
When Site Name is used for the Caller ID, overwrite it with:

Trunk Digit Manipulation:

☐ Remove leading 1 from 1+10D
Hint: Required for some long distance service providers.
☐ Remove leading 1 for Local Area Codes (for all prefixes unless a specific local prefix list is provided below)
Hint: Required for some local service providers with overlay area codes.
☐ Dial 7 digits for Local Area Code (for all prefixes unless a specific local prefix list is provided below)
Hint: Local prefixes required for some local service providers with mixed 7D and 1+10D in the same home area.
☐ Dial in E.164 Format
Local Prefixes: Non [Go to Local Prefixes List](#)
Prepend Dial Out Prefix:
Off System Extensions: [Edit](#)
Translation Table: <None>

3.7 ShoreTel System Settings – Individual Trunks

This section describes the configuration of individual trunks.

➤ **To configure individual trunks:**

1. Navigate to the Trunks Group screen by selecting **Administration > Trunks > Individual Trunks**.
2. The Trunks by Group screen is used to change the individual trunks settings that appear.

Figure 3-8: Trunks by Group

Name	Type	Site	Trunks	DID	Destination	Access Code
Analog Loop Start	Analog Loop Start	Headquarters	2	No	700	9
Digital Loop Start	Digital Loop Start	Headquarters	0	No	700	9
Digital Wink Start	Digital Wink Start	Headquarters	0	No	700	9
SIP Lync	SIP	Headquarters	5	Yes	700	80
SIP PSTN	SIP	Headquarters	5	Yes	700	81

© 1998-2013 ShoreTel, Inc. All rights reserved.

Figure 3-9: Individual Trunk Setting for BroadCloud SIP Trunk Group

Trunks
Edit Trunk

[New](#) [Copy](#) [Save](#) [Delete](#) [Reset](#)

[Edit this record](#) [Refresh this page](#)

Site: Headquarters

Trunk Group: sip pstn

Name: sip pstn

Switch: sq3

IP Address: 172.26.249.31

© 1998-2014 ShoreTel, Inc. All rights reserved.

3.8 Edit BroadCloud SIP Trunk Group

➤ To edit BroadCloud SIP Trunk Group:

1. Enter your preferred name for the new trunk group. In the example in Figure 3-7, the **SIP PSTN** has been created.
2. The 'Enable SIP Info for G.711 DTMF Signaling' parameter should not be selected. 'Enabling SIP info' is currently only used with SIP tie trunks between ShoreTel systems.
3. The 'Profile' parameter should be left at its default setting of **Default ITSP**; it is not necessary to modify this parameter when connecting to the AudioCodes SBC.
4. The 'Digest Authentication' parameter defaults to "<None>" and modification is not required when connecting to the AudioCodes SBC.
5. The next item to change in the Edit SIP Trunks Group screen is to make the appropriate settings for the 'Inbound' parameters in the figure below.

Figure 3-10: Inbound

Inbound:

Number of Digits from CO:

☒ DNIS [Edit DNIS Map](#)

☒ DID [Edit DID Range](#)

☒ Extension

☒ Translation Table:

☐ Prepend Dial In Prefix:

☐ Use Site Extension Prefix

☒ Tandem Trunking

User Group:

Prepend Dial In Prefix:

Destination: [Search](#)

6. Within the 'Inbound:' settings, ensure the **Number of Digits from CO** is set to match what the ShoreTel SIP trunk switch will be receiving from AudioCodes SBC and ensure that the 'DNIS', 'DID' and 'Extension' check boxes are selected.
7. It is recommended that the 'Tandem Trunking' check box should be selected. Otherwise transfers to external telephone numbers will fail via SIP trunks. For additional information on this parameter please refer to the *ShoreTel Planning and Installation Guide*.
8. Make the appropriate changes for the 'Outbound' parameters below.

Figure 3-11: Outbound and Trunk Services

☒ **Outbound:**

Network Call Routing:

Access Code:

Local Area Code:

Additional Local Area Codes:

Nearby Area Codes:

Billing Telephone Number: (e.g. +1 (408) 331-3300 )

Trunk Services:

☒ Local

☒ Long Distance

☒ International

☐ Enable Original Caller Information

☒ n11 (e.g. 411, 611, except 911 which is specified below)

☒ Emergency (e.g. 911)

☒ Easily Recognizable Codes (ERC) (e.g. 800, 888, 900)

☒ Explicit Carrier Selection (e.g. 1010xxx)

☒ Operator Assisted (e.g. 0+)

☒ Caller ID not blocked by default

9. Select the 'Outbound' parameter and define a Trunk 'Access Code' and 'Local Area Code' as appropriate.
10. Under the **Trunk Services** group, make sure the appropriate services are enabled or disabled based on your needs. In general, we are only using this trunk group to dial the off system extensions to reach the BroadCloud audio conferencing bridge or softphone users.
11. The 'Caller ID not blocked by default' field determines if the call is sent out as <unknown> or with caller information (Caller ID). User DID will impact how information is passed out to the SIP Trunk group.
12. The final parameters for configuration in the Trunk Group are 'Trunk Digit Manipulation' below.

Figure 3-12: Trunk Digit Manipulation

Trunk Digit Manipulation:

☐ Remove leading 1 from 1+10D
Hint: Required for some long distance service providers.

☐ Remove leading 1 for Local Area Codes (for all prefixes unless a specific local prefix list is provided below)
Hint: Required for some local service providers with overlay area codes.

☐ Dial 7 digits for Local Area Code (for all prefixes unless a specific local prefix list is provided below)
Hint: Local prefixes required for some local service providers with mixed 7D and 1+10D in the same home area.

☐ Dial in E.164 Format

Local Prefixes: Non ▼ [Go to Local Prefixes List](#)

Prepend Dial Out Prefix:

Off System Extensions: Edit

Translation Table: <None ▼

13. Select the 'Dial in E.164 Format' parameter 'IF NEEDED' and define a Trunk 'Access Code' and 'Local Area Code' as appropriate.
14. Next you must create the Off System Extension (OSE) range that will be used to represent the BroadCloud audio conferencing bridge or BroadCloud softphone users. An OSE is required for every BroadCloud SIP Trunk endpoint that will be using the ShoreTel system.
15. Click the Edit button next to Off System Extensions; the Off Systems Extension Range dialog is displayed below.

Figure 3-13: Off System Extension Ranges

☐ Explicit Carrier Selection (e.g. 1010xxx)

☐ Operator Assisted (e.g. 0+)

☒ Caller ID not blocked by default

☐ Enable Caller ID (Please confirm with the Carrier(s) or the Service Provider(s) on how the end-to-end caller name is delivered)
 When Site Name is used for the Caller ID, overwrite it with:

Trunk Digit Manipulation:

☐ Remove leading 1 from 1+10D
Hint: Required for some long distance service providers.

☐ Remove leading 1 for Local Area Codes (for all prefixes unless a specific local prefix list is provided below)
Hint: Required for some local service providers with overlay area codes.

☐ Dial 7 digits for Local Area Code (for all prefixes unless a specific local prefix list is provided below)
Hint: Local prefixes required for some local service providers with mixed 7D and 1+10D in the same home area.

☐ Dial in E.164 Format

Local Prefixes: Non ▼ [Go to Local Prefixes List](#)

Prepend Dial Out Prefix:

Off System Extensions: Edit

Translation Table: <None ▼

Off System Extension Ranges -- Webpage Dialog

Range:

New... Edit... Remove

OK Cancel

16. Click New and define the first range for the extensions that will represent the BroadCloud endpoints on the ShoreTel system.
17. Click OK to save the first range and repeat if necessary to create sufficient extensions for all your BroadCloud endpoints.
18. After all your setting changes are made to the Edit SIP Trunk Group screen, click **Save** at the top of the screen.

4 Configuring AudioCodes E-SBC

This chapter provides step-by-step procedures on how to configure AudioCodes E-SBC for interworking between IP-PBX and the BroadCloud 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 - BroadCloud 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*).

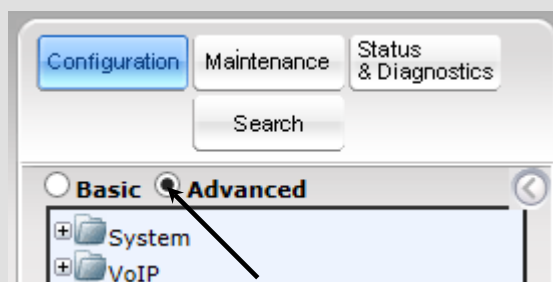
Notes:

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

- ✓ **SBC**
- ✓ **Security**
- ✓ **DSP**
- ✓ **RTP**
- ✓ **SIP**

For more information about the Software License Key, contact your AudioCodes sales representative.

- The scope of this interoperability test and document does **not** cover all security aspects for connecting the SIP Trunk to the IP-PBX environment. 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.
- Before you begin configuring the E-SBC, ensure that the E-SBC's Web interface Navigation tree is in Advanced-menu display mode. To do this, select the **Advanced** option, as shown below:



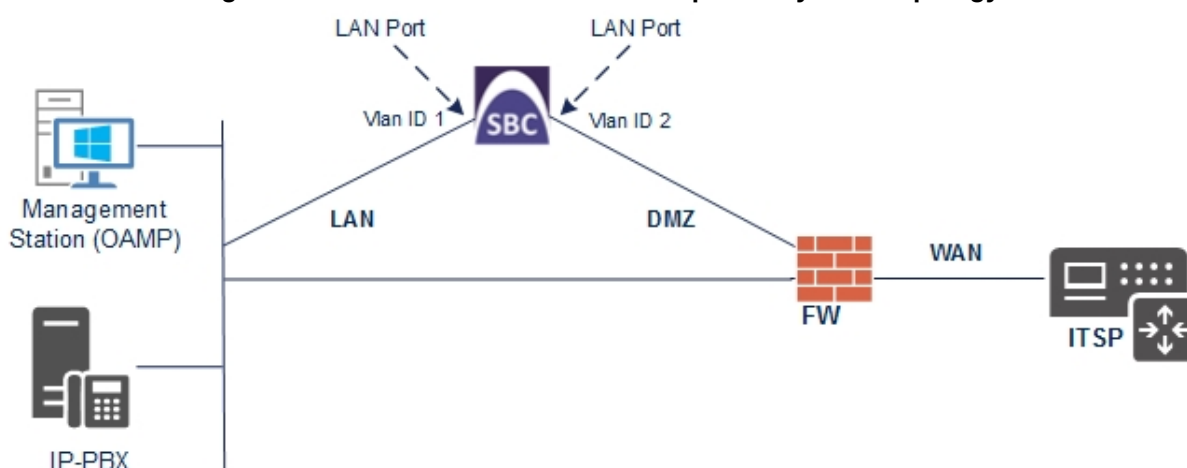
Note that when the E-SBC is reset, the Navigation tree reverts to Basic-menu display.

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
 - BroadCloud 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 WAN 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)
 - WAN (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 "Voice")
- WAN VoIP (assigned the name "WANSP")

➤ **To configure the VLANs:**

1. Open the Ethernet Device Table page (**Configuration** tab > **VoIP** menu > **Network** > **Ethernet Device Table**).
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 Table

The screenshot shows the 'Ethernet Device Table' interface. At the top, there are buttons for 'Add +', 'Edit', 'Delete', and 'Show / Hide'. To the right, there is a dropdown menu set to 'All', a search bar labeled 'Search in table', and a 'Search' button. The table itself has five columns: 'Index', 'VLAN ID', 'Underlying Interface', 'Name', and 'Tagging'. There are two rows of data. The first row has Index 0, VLAN ID 1, Underlying Interface GROUP_1, Name vlan 1, and Tagging Untagged. The second row has Index 1, VLAN ID 2, Underlying Interface GROUP_2, Name vlan 2, and Tagging Untagged. At the bottom, there is a pagination bar showing 'Page 1 of 1' and a 'View 1 - 2 of 2' indicator.

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 "Voice")
- WAN VoIP (assigned the name "WANSP")

➤ **To configure the IP network interfaces:**

1. Open the IP Interfaces Table page (**Configuration** tab > **VoIP** menu > **Network** > **IP Interfaces Table**).

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
IP Address	172.26.100.169 (IP address of E-SBC)
Prefix Length	24 (subnet mask in bits for 255.255.255.0)
Default Gateway	172.26.100.001
VLAN ID	1
Interface Name	Voice (arbitrary descriptive name)
Underlying Device	vlan 1

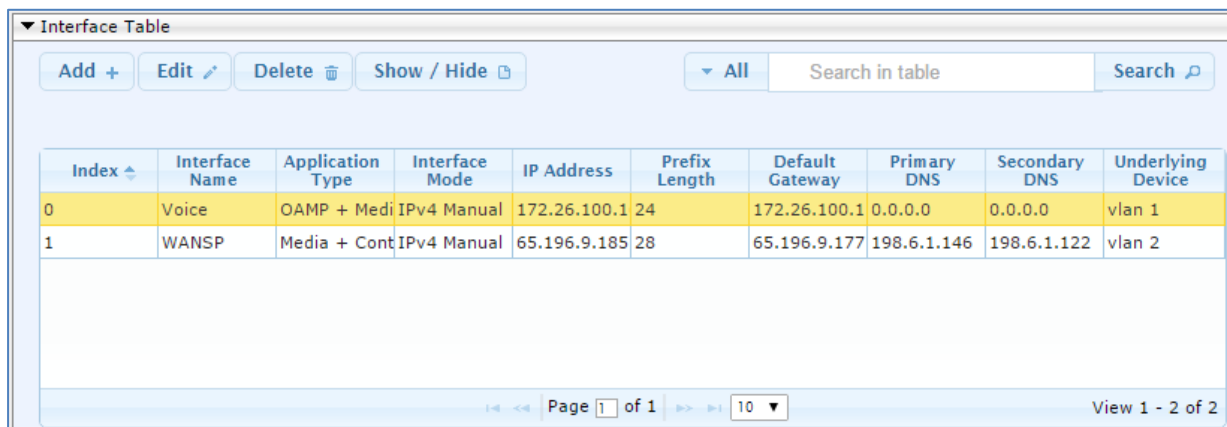
3. Add a network interface for the WAN side:
 - a. Enter **1**, and then click **Add Index**.
 - b. Configure the interface as follows:

Parameter	Value
Application Type	Media + Control
IP Address	65.196.9.185 (WAN IP address)
Prefix Length	28 (for 255.255.255.240)
Default Gateway	65.196.9.177 (router's IP address)
VLAN ID	2
Interface Name	WANSP
Primary DNS Server IP Address	198.6.1.146
Secondary DNS Server IP Address	198.6.1.122
Underlying Device	vlan 2

4. Click **Apply**, and then **Done**.

The configured IP network interfaces are shown below:

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



▼ Interface Table									
Add +		Edit ✎	Delete 🗑	Show / Hide 📄		▼ All	Search in table		Search 🔍
Index ▲	Interface Name	Application Type	Interface Mode	IP Address	Prefix Length	Default Gateway	Primary DNS	Secondary DNS	Underlying Device
0	Voice	OAMP + Medi	IPv4 Manual	172.26.100.1	24	172.26.100.1	0.0.0.0	0.0.0.0	vlan 1
1	WANSP	Media + Cont	IPv4 Manual	65.196.9.185	28	65.196.9.177	198.6.1.146	198.6.1.122	vlan 2

Page 1 of 1 10 ▼ View 1 - 2 of 2

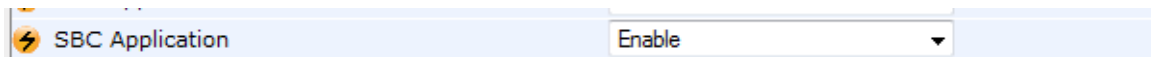
4.2 Step 2: Enable the SBC Application

This step describes how to enable the SBC application.

➤ **To enable the SBC application:**

1. Open the Applications Enabling page (**Configuration** tab > **VoIP** menu > **Applications Enabling** > **Applications Enabling**).

Figure 4-4: Enabling SBC Application



2. From the 'SBC Application' drop-down list, select **Enable**.
3. Click **Submit**.
4. Reset the E-SBC with a burn to flash for this setting to take effect (see Section 4.13 on page 63).

4.3 Step 3: Configure Media Realms

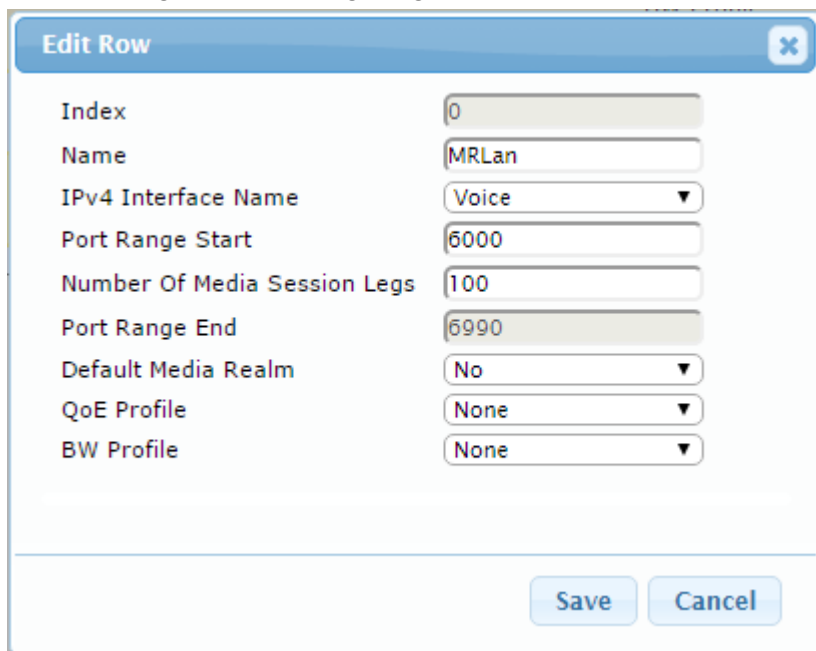
This step describes how to configure Media Realms. The simplest configuration is to create two Media Realms - one for internal (LAN) traffic and one for external (WAN) traffic.

➤ **To configure Media Realms:**

1. Open the Media Realm Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **Media Realm Table**).
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
Media Realm Name	MRLan (descriptive name)
IPv4 Interface Name	Voice
Port Range Start	6000 (as required by IP-PBX)
Number of Media Session Legs	100 (media sessions assigned with port range)

Figure 4-5: Configuring Media Realm for LAN



Edit Row

Index

0

Name

MRLan

IPv4 Interface Name

Voice

Port Range Start

6000

Number Of Media Session Legs

100

Port Range End

6990

Default Media Realm

No

QoS Profile

None

BW Profile

None

Save

Cancel

3. Configure a Media Realm for WAN traffic:

Parameter	Value
Index	1
Media Realm Name	MRWan (arbitrary name)
IPv4 Interface Name	WANSP
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

Add Row

Index: 1

Name: MRWan

IPv4 Interface Name: WANSP

Port Range Start: 7000

Number Of Media Session Legs: 100

Port Range End: -1

Default Media Realm: No

QoE Profile: None

BW Profile: None

Add Cancel

The configured Media Realms are shown in the figure below:

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

Media Realm Table

Add + Edit Delete Show / Hide

All Search in table Search

Index	Name	IPv4 Interface Name	Port Range Start	Number Of Media Session Legs	Port Range End	Default Media Realm
0	MRLan	Voice	6000	100	6990	No
1	MRWan	WANSP	7000	100	7990	No

Page 1 of 1 10 View 1 - 2 of 2

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 Interface Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **SIP Interface Table**).
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
Interface Name	IP-PBX (see Note below)
Network Interface	Voice
Application Type	SBC
UDP Port	5060
TCP and TLS	0
Media Realm	MRLan

3. Configure a SIP Interface for the WAN:

Parameter	Value
Index	1
Interface Name	BroadCloud (see Note below)
Network Interface	WANSP
Application Type	SBC
UDP Port	5060
TCP and TLS	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 Interface Table									
Add +		Edit ✎	Delete 🗑	Show / Hide 📄		▼ All	Search in table		Search 🔍
Index ↕	Name	SRD	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	Encapsulatin Protocol	Media Realm
0	IP-PBX	DefaultSRD	Voice	SBC	5060	0	0	No encapsulati	MRLan
1	BroadCloud	DefaultSRD	WANSP	SBC	5060	0	0	No encapsulati	MRWan
⏪ ⏩ Page 1 of 1 10 ▼ View 1 - 2 of 2									



Note: Unlike in previous software releases where configuration entities (e.g., SIP Interface, Proxy Sets, and IP Groups) were associated with each other using table row indices, Version 7.0 uses the string **names** of the configuration entities. 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
- BroadCloud 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 page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **Proxy Sets Table**).
2. Add a Proxy Set for the IP-PBX. You can use the default Proxy Set (Index 0), but modify it as shown below:

Parameter	Value
Proxy Set ID	0
Proxy Name	IP-PBX
SBC IPv4 SIP Interface	IP-PBX
Proxy Keep Alive	Using Options

Figure 4-9: Configuring Proxy Set for IP-PBX

Edit Row

Index: 0
SRD: DefaultSRD
Name: IP-PBX
Gateway IPv4 SIP Interface: None
SBC IPv4 SIP Interface: IP-PBX
Proxy Keep-Alive: Using OPTIONS
Proxy Keep-Alive Time [sec]: 60
Redundancy Mode:
Proxy Load Balancing Method: Disable
DNS Resolve Method:
Proxy Hot Swap: Disable
Keep-Alive Failure Responses:
Classification Input: IP Address only
TLS Context Name: None

Save Cancel

3. Configure a Proxy Address Table for Proxy Set for IP-PBX:
 - a. Go to Configuration tab > VoIP menu > VoIP Network > Proxy Sets Table > Proxy Address Table.

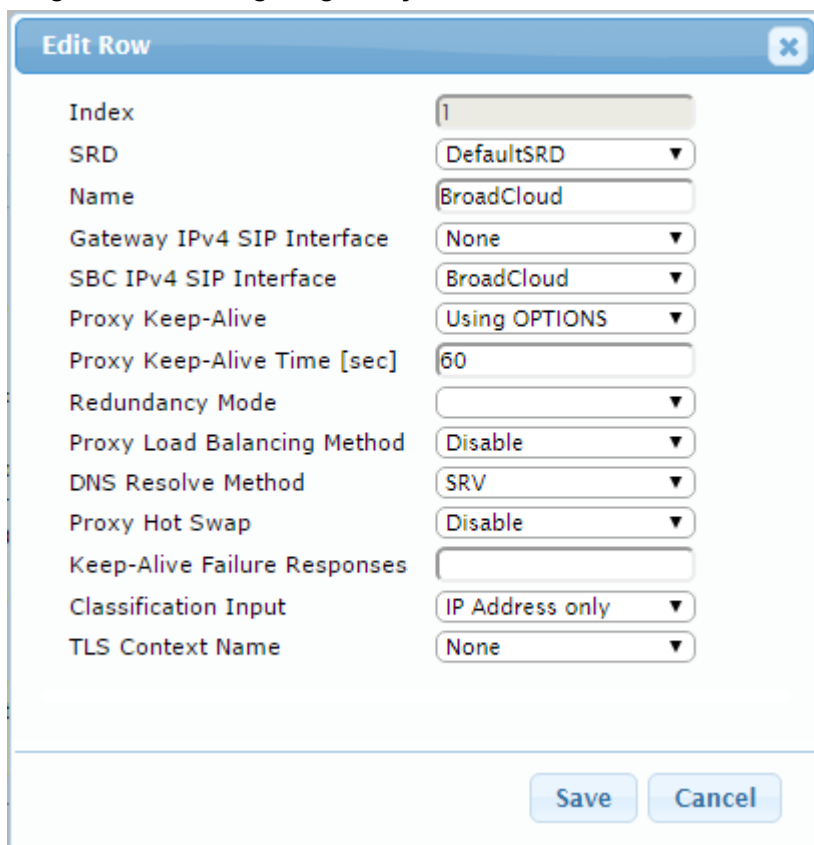
Parameter	Value
Index	0
Proxy Address	172.26.249.130:5060 (IP-PBX IP address / FQDN and destination port)
Transport Type	UDP

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

The screenshot shows a web-based configuration interface with a modal dialog titled "Edit Row". Inside the dialog, there are three input fields: "Index" with the value "0", "Proxy Address" with the value "172.26.249.130:5060", and "Transport Type" with a dropdown menu showing "UDP". At the bottom right of the dialog, there are two buttons: "Save" and "Cancel".

4. Configure a Proxy Set for the BroadCloud SIP Trunk:

Parameter	Value
Proxy Set ID	1
Proxy Name	BroadCloud
SBC IPv4 SIP Interface	BroadCloud
Proxy Keep Alive	Using Options

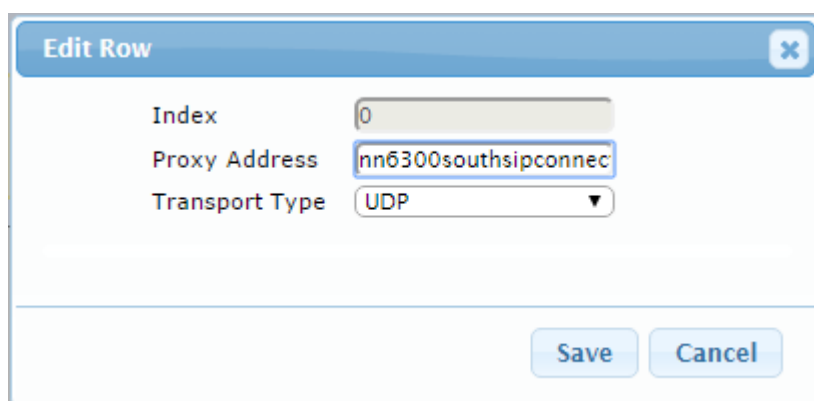
Figure 4-11: Configuring Proxy Set for BroadCloud SIP Trunk


Edit Row	
Index	1
SRD	DefaultSRD
Name	BroadCloud
Gateway IPv4 SIP Interface	None
SBC IPv4 SIP Interface	BroadCloud
Proxy Keep-Alive	Using OPTIONS
Proxy Keep-Alive Time [sec]	60
Redundancy Mode	
Proxy Load Balancing Method	Disable
DNS Resolve Method	SRV
Proxy Hot Swap	Disable
Keep-Alive Failure Responses	
Classification Input	IP Address only
TLS Context Name	None

Save Cancel

- Configure a Proxy Address Table for Proxy Set 1:
- Go to Configuration tab > VoIP menu > VoIP Network > Proxy Sets Table > Proxy Address Table.

Parameter	Value
Index	0
Proxy Address	nn6300southsipconnect.adpt-tech.com (IP-PBX IP address / FQDN and destination port)
Transport Type	UDP

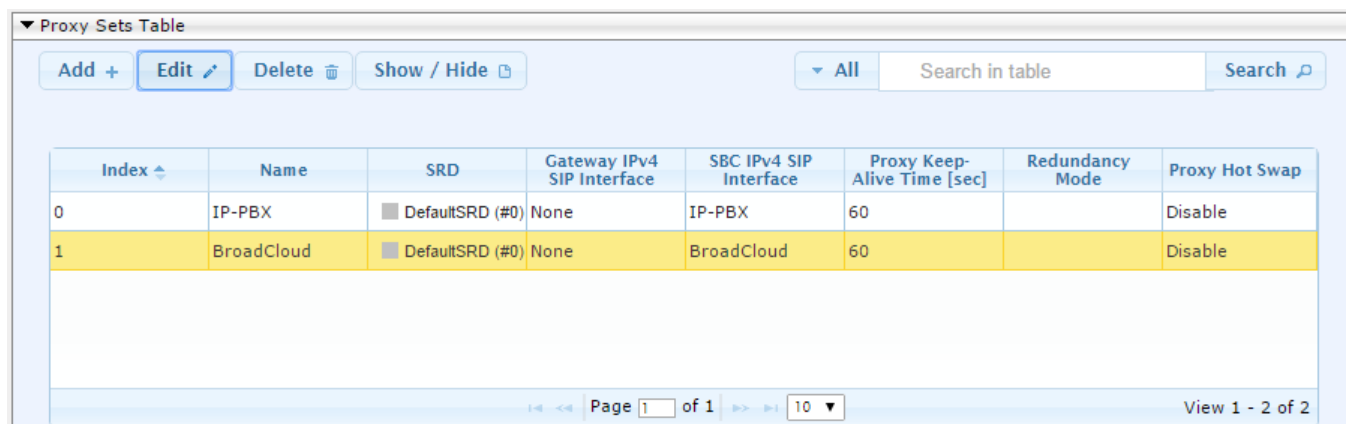
Figure 4-12: Configuring Proxy Address for


Edit Row	
Index	0
Proxy Address	nn6300southsipconnec
Transport Type	UDP

Save Cancel

The configured Proxy Sets are shown in the figure below:

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



The screenshot displays the 'Proxy Sets Table' interface. At the top, there are buttons for 'Add +', 'Edit' (with a pencil icon), 'Delete' (with a trash icon), and 'Show / Hide' (with a list icon). To the right, there is a dropdown menu set to 'All', a search bar labeled 'Search in table', and a 'Search' button with a magnifying glass icon. Below these controls is a table with the following data:

Index	Name	SRD	Gateway IPv4 SIP Interface	SBC IPv4 SIP Interface	Proxy Keep-Alive Time [sec]	Redundancy Mode	Proxy Hot Swap
0	IP-PBX	■ DefaultSRD (#0)	None	IP-PBX	60		Disable
1	BroadCloud	■ DefaultSRD (#0)	None	BroadCloud	60		Disable

At the bottom of the table, there is a pagination bar showing 'Page 1 of 1' and a dropdown menu set to '10'. On the far right, it says 'View 1 - 2 of 2'.

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:

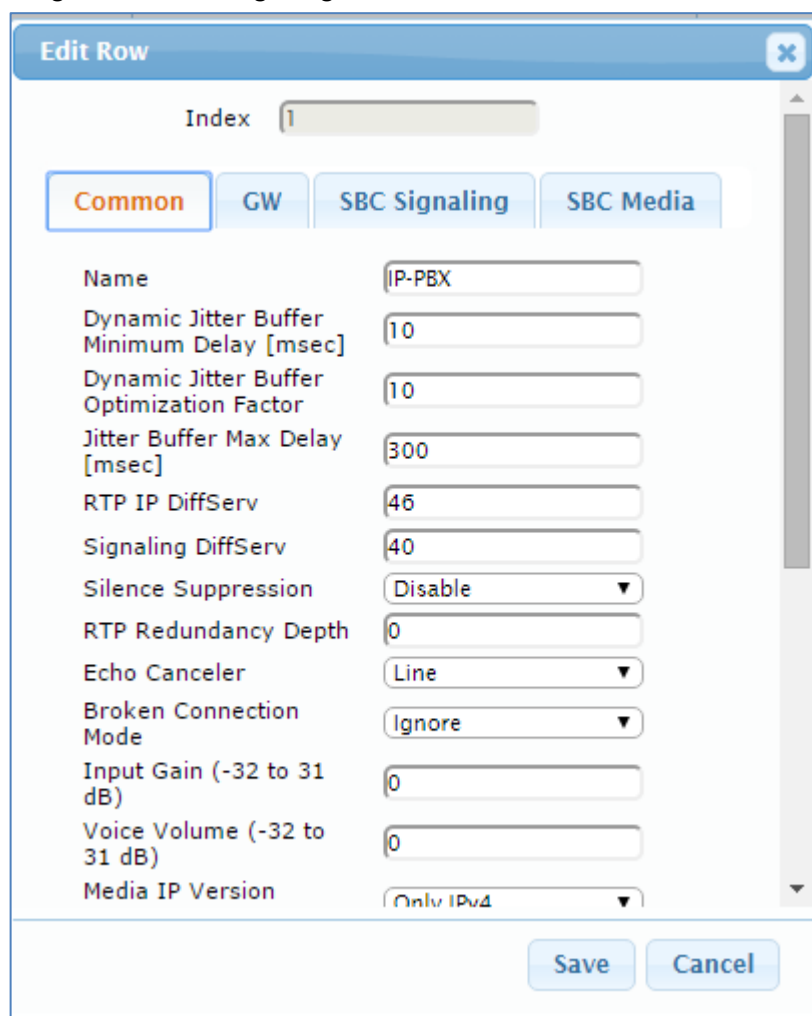
- IP-PBX - to operate in non-secure mode using RTP and UDP
- BroadCloud SIP trunk - to operate in non-secure mode using RTP and UDP

➤ To configure IP Profile for the IP-PBX:

1. Open the IP Profile Settings page (**Configuration** tab > **VoIP** > **Coders and Profiles** > **IP Profile Settings**).
2. Click **Add**.
3. Click the **Common** tab, and then configure the parameters as follows:

Parameter	Value
Index	1
Name	IP-PBX

Figure 4-14: Configuring IP Profile for IP-PBX – Common Tab



The screenshot shows the 'Edit Row' dialog box for configuring an IP Profile. The 'Index' is set to 1. The 'Common' tab is selected, showing the following parameters and values:

Parameter	Value
Name	IP-PBX
Dynamic Jitter Buffer Minimum Delay [msec]	10
Dynamic Jitter Buffer Optimization Factor	10
Jitter Buffer Max Delay [msec]	300
RTP IP DiffServ	46
Signaling DiffServ	40
Silence Suppression	Disable
RTP Redundancy Depth	0
Echo Canceler	Line
Broken Connection Mode	Ignore
Input Gain (-32 to 31 dB)	0
Voice Volume (-32 to 31 dB)	0
Media IP Version	Only IPv4

Buttons: Save, Cancel

4. Click the **SBC Signaling** tab, and then configure the parameters as follows:

Parameter	Value
Remote Update Support	Supported
Remote re-INVITE Support	Supported

Figure 4-15: Configuring IP Profile for IP-PBX – SBC Signaling Tab

Edit Row [X]

Index:

Common | GW | **SBC Signaling** | SBC Media

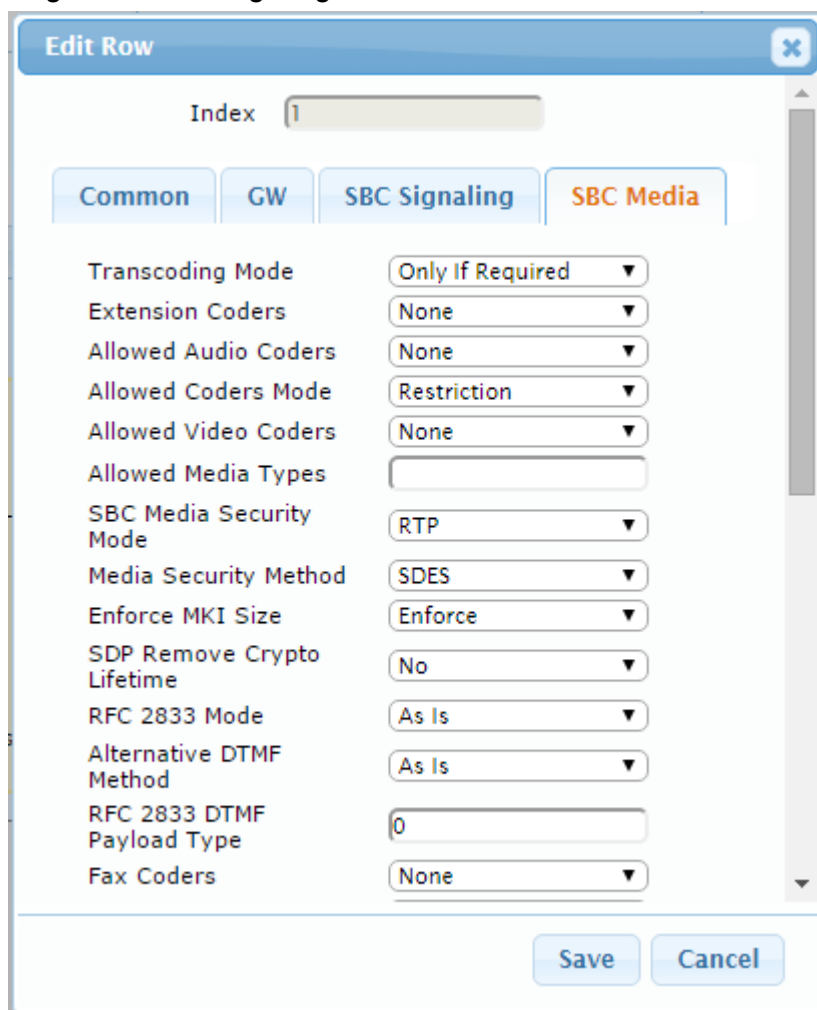
PRACK Mode	Transparent
P-Asserted-Identity Header Mode	As Is
Diversion Header Mode	As Is
History-Info Header Mode	As Is
Session Expires Mode	Transparent
Remote Update Support	Supported
Remote re-INVITE	Supported
Remote Delayed Offer Support	Supported
User Registration Time	0
NAT UDP Registration Time	-1
NAT TCP Registration Time	-1
Remote REFER Mode	Regular
Remote Replaces Mode	Standard

Save Cancel

5. Click the **SBC Media** tab, and then configure the parameters as follows:

Parameter	Value
Media Security Behavior	RTP

Figure 4-16: Configuring IP Profile for IP-PBX – SBC Media Tab



Edit Row [X]

Index: 1

Common | GW | SBC Signaling | **SBC Media**

Transcoding Mode	Only If Required ▼
Extension Coders	None ▼
Allowed Audio Coders	None ▼
Allowed Coders Mode	Restriction ▼
Allowed Video Coders	None ▼
Allowed Media Types	
SBC Media Security Mode	RTP ▼
Media Security Method	SDES ▼
Enforce MKI Size	Enforce ▼
SDP Remove Crypto Lifetime	No ▼
RFC 2833 Mode	As Is ▼
Alternative DTMF Method	As Is ▼
RFC 2833 DTMF Payload Type	0
Fax Coders	None ▼

Save Cancel

➤ To configure an IP Profile for the BroadCloud SIP Trunk:

1. Click **Add**.
2. Click the **Common** tab, and then configure the parameters as follows:

Parameter	Value
Index	2
Profile Name	BroadCloud

Figure 4-17: Configuring IP Profile for BroadCloud SIP Trunk – Common Tab

Edit Row [X]

Index: 2

Common | GW | SBC Signaling | SBC Media

Name: BroadCloud

Dynamic Jitter Buffer Minimum Delay [msec]: 10

Dynamic Jitter Buffer Optimization Factor: 10

Jitter Buffer Max Delay [msec]: 300

RTP IP DiffServ: 46

Signaling DiffServ: 40

Silence Suppression: Disable

RTP Redundancy Depth: 0

Echo Canceler: Line

Broken Connection Mode: Ignore

Input Gain (-32 to 31 dB): 0

Voice Volume (-32 to 31 dB): 0

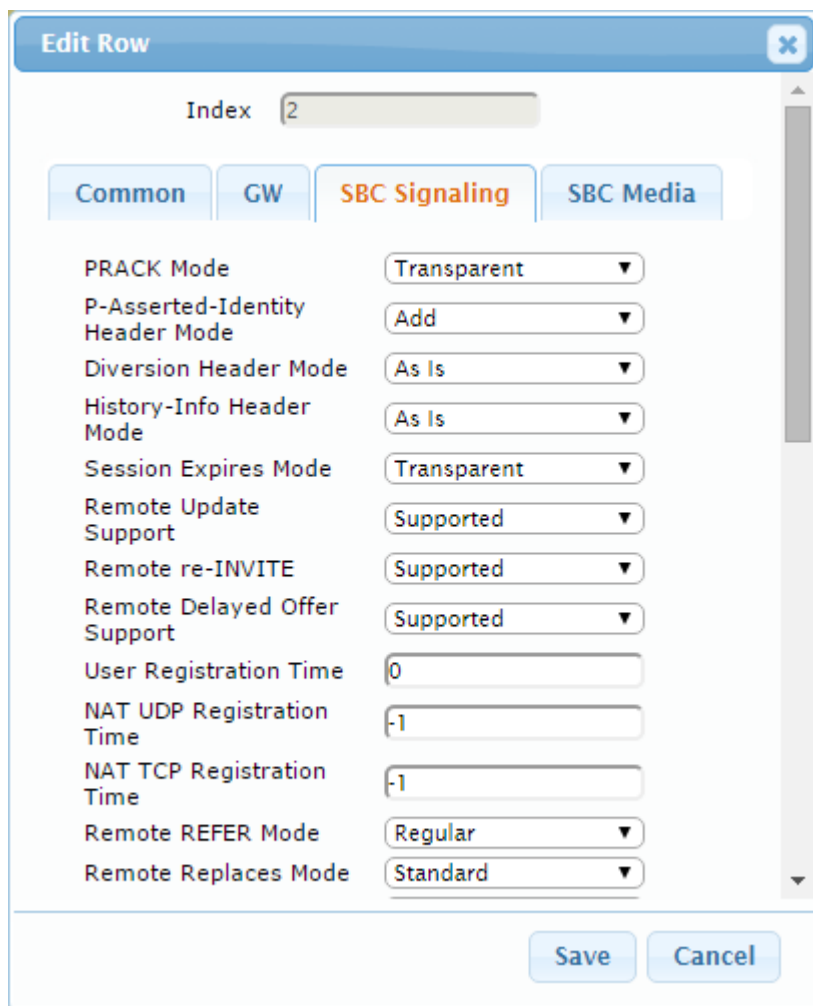
Media IP Version: Only IPv4

Save Cancel

3. Click the **SBC Signaling** tab, and then configure the parameters as follows:

Parameter	Value
P-Asserted-Identity Header Mode	Add (required for anonymous calls)

Figure 4-18: Configuring IP Profile for BroadCloud SIP Trunk – SBC Signaling Tab



Edit Row [X]

Index: 2

Common | GW | **SBC Signaling** | SBC Media

PRACK Mode	Transparent ▼
P-Asserted-Identity Header Mode	Add ▼
Diversion Header Mode	As Is ▼
History-Info Header Mode	As Is ▼
Session Expires Mode	Transparent ▼
Remote Update Support	Supported ▼
Remote re-INVITE	Supported ▼
Remote Delayed Offer Support	Supported ▼
User Registration Time	0
NAT UDP Registration Time	-1
NAT TCP Registration Time	-1
Remote REFER Mode	Regular ▼
Remote Replaces Mode	Standard ▼

Save Cancel

4. Click the **SBC Media** tab, and then configure the parameters as follows:

Parameter	Value
Media Security Behavior	RTP

Figure 4-19: Configuring IP Profile for BroadCloud SIP Trunk – SBC Media Tab

The screenshot shows the 'Edit Row' dialog box for configuring SBC Media parameters. The 'Index' is 2. The 'SBC Media' tab is selected. The parameters and their values are as follows:

Parameter	Value
Transcoding Mode	Only If Required
Extension Coders	None
Allowed Audio Coders	None
Allowed Coders Mode	Restriction
Allowed Video Coders	None
Allowed Media Types	
SBC Media Security Mode	RTP
Media Security Method	SDES
Enforce MKI Size	Don't enforce
SDP Remove Crypto Lifetime	No
RFC 2833 Mode	As Is
Alternative DTMF Method	As Is
RFC 2833 DTMF Payload Type	0
Fax Coders	None

Buttons: Save, Cancel

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
- BroadCloud SIP Trunk located on WAN

➤ To configure IP Groups:

1. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group Table**).
2. Add an IP Group for the IP-PBX. You can use the default IP Group (Index 0), but modify it as shown below:

Parameter	Value
Index	0
Name	IP-PBX
Type	Server
Proxy Set	IP-PBX
IP Profile	IP-PBX
Media Realm	MRLan
SIP Group Name	172.26.249.130 (according to IP-PBX requirement)

3. Configure an IP Group for the BroadCloud SIP Trunk:

Parameter	Value
Index	1
Name	BroadCloud
Type	Server
Proxy Set	BroadCloud
IP Profile	BroadCloud
Media Realm	MRWan
SIP Group Name	interop.adpt-tech.com (according to ITSP requirement)

The configured IP Groups are shown in the figure below:

Figure 4-20: Configured IP Groups in IP Group Table

▼ IP Group Table											
Add +		Edit ↗		Delete 🗑		Show / Hide 📄		▼ All		Search in table	Search 🔍
Index	Name	SRD	Type	SBC Operation Mode	Proxy Set	IP Profile	Media Realm	SIP Group Name	Classify By Proxy Set	Inbound Message Manipulation Set	Outbound Message Manipulation Set
0	IP-PBX	DefaultSRD Server		Not Configured	IP-PBX	IP-PBX	MRLan	172.26.249.130	Enable	-1	4
1	BroadCloud	DefaultSRD Server		Not Configured	BroadCloud	BroadCloud	MRWan	interop.adpt-tech.c	Enable	-1	4
⏪ ⏩ Page 1 of 1 10 ▼ View 1 - 2 of 2											

4.8 Step 8: 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 to denote the source and destination of the call. As configured in Section 4.7 on page 37, IP Group 1 represents IP-PBX, and IP Group 2 represents BroadCloud SIP Trunk.

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

- Terminate SIP OPTIONS messages on the E-SBC
- Calls from IP-PBX to BroadCloud SIP Trunk
- Calls from BroadCloud SIP Trunk to IP-PBX

➤ To configure IP-to-IP routing rules:

1. Open the IP-to-IP Routing Table page (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **IP-to-IP Routing Table**).
2. Configure a rule to terminate SIP OPTIONS messages received from the LAN:
 - a. Click **Add**.
 - b. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	0
Name	Terminate OPTIONS (arbitrary descriptive name)
Source IP Group	Any
Request Type	OPTIONS

Figure 4-21: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS – Rule Tab

Edit Row

Index: 0

Routing Policy: Default_SBCRouting

Rule | Action

Name: Terminate OPTIONS

Alternative Route Options: Route Row

Source IP Group: Any

Request Type: OPTIONS

Source Username Prefix: *

Source Host: *

Destination Username Prefix: *

Destination Host: *

Message Condition: None

Call Trigger: Any

ReRoute IP Group: Any

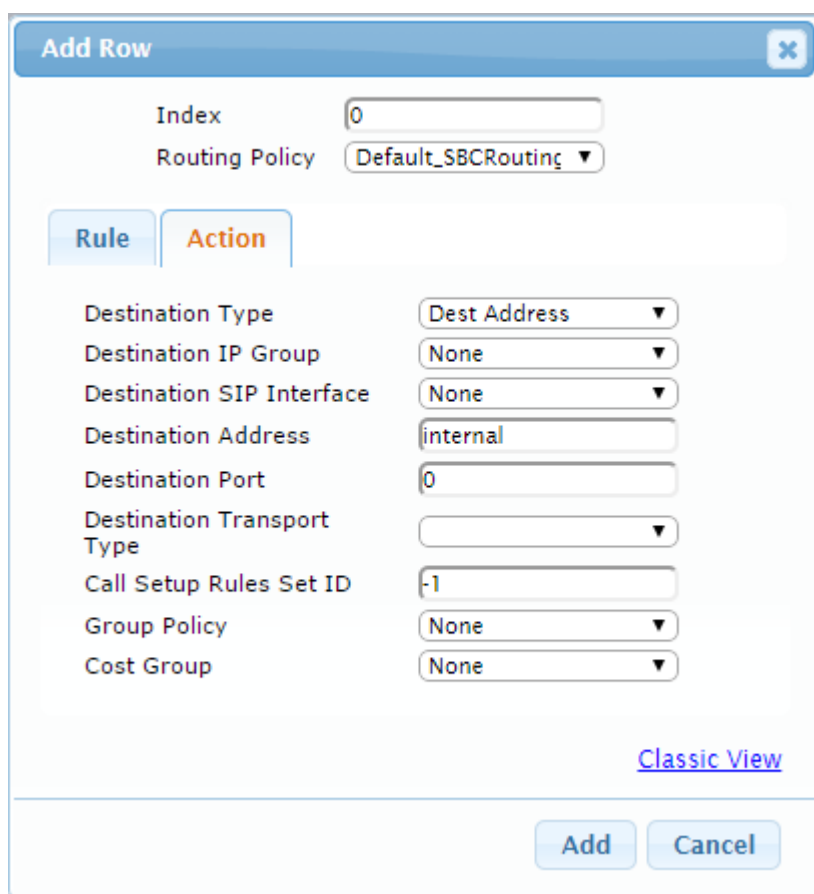
[Classic View](#)

Save Cancel

- c. Click the **Action** tab, and then configure the parameters as follows:

Parameter	Value
Destination Type	Dest Address
Destination Address	internal

Figure 4-22: Configuring IP-to-IP Routing Rule for Terminating SIP OPTIONS – Action Tab



3. Configure a rule to route calls from Skype IP-PBX to BroadCloud SIP Trunk:
 - a. Click **Add**.
 - b. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	1
Route Name	IP-PBX to ITSP (arbitrary descriptive name)
Source IP Group	IP-PBX

Figure 4-23: Configuring IP-to-IP Routing Rule for IP-PBX to ITSP – Rule tab

Edit Row

Index: 1
Routing Policy: Default_SBCRouting

Rule | Action

Name: IP-PBX to ITSP
Alternative Route Options: Route Row
Source IP Group: IP-PBX
Request Type: All
Source Username Prefix: *
Source Host: *
Destination Username Prefix: *
Destination Host: *
Message Condition: None
Call Trigger: Any
ReRoute IP Group: Any

[Classic View](#)

Save Cancel

- c. Click the **Action** tab, and then configure the parameters as follows:

Parameter	Value
Destination Type	IP Group
Destination IP Group	BroadCloud
Destination SIP Interface	BroadCloud

Figure 4-24: Configuring IP-to-IP Routing Rule for IP-PBX to ITSP – Action tab

Edit Row

Index

1

Routing Policy

Default_SBCRouting

Rule

Action

Destination Type

IP Group

Destination IP Group

BroadCloud

Destination SIP Interface

BroadCloud

Destination Address

Destination Port

0

Destination Transport Type

Call Setup Rules Set ID

-1

Group Policy

None

Cost Group

None

[Classic View](#)

Save

Cancel

4. To configure rule to route calls from BroadCloud SIP Trunk to IP-PBX:
 - a. Click **Add**.
 - b. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	2
Route Name	ITSP to IP-PBX (arbitrary descriptive name)
Source IP Group	BroadCloud

Figure 4-25: Configuring IP-to-IP Routing Rule for ITSP to IP-PBX – Rule tab

Edit Row

Index: 2
Routing Policy: Default_SBCRouting

Rule | **Action**

Name: ITSP to IP-PBX
Alternative Route Options: Route Row
Source IP Group: BroadCloud
Request Type: All
Source Username Prefix: *
Source Host: *
Destination Username Prefix: *
Destination Host: *
Message Condition: None
Call Trigger: Any
ReRoute IP Group: Any

[Classic View](#)

Save Cancel

- a. Click the **Action** tab, and then configure the parameters as follows:

Parameter	Value
Destination Type	IP Group
Destination IP Group	IP-PBX
Destination SIP Interface	IP-PBX

Figure 4-26: Configuring IP-to-IP Routing Rule for ITSP to IP-PBX – Action tab

Edit Row
✕

Index
Routing Policy Default_SBCRouting ▼

Rule

Action

Destination Type IP Group ▼
Destination IP Group IP-PBX ▼
Destination SIP Interface IP-PBX ▼
Destination Address
Destination Port
Destination Transport Type ▼
Call Setup Rules Set ID
Group Policy None ▼
Cost Group None ▼

[Classic View](#)

Save
Cancel

The configured routing rules are shown in the figure below:

Figure 4-27: Configured IP-to-IP Routing Rules in IP-to-IP Routing Table

▼ IP-to-IP Routing Table

Add +
Edit ✎
Delete ✖
Insert +
Up ↑
Down ↓

▼ All

Search 🔍

Show / Hide 📄

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 OPTI	Default_SB	Route Row	Any	OPTIONS	*	*	Dest Address	None	None	internal
1	IP-PBX to ITSP	Default_SB	Route Row	IP-PBX	All	*	*	IP Group	BroadCloud	BroadCloud	
2	ITSP to IP-PBX	Default_SB	Route Row	BroadCloud	All	*	*	IP Group	IP-PBX	IP-PBX	

⏪
⏩
Page 1 of 1
10 ▼

View 1 - 3 of 3



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

4.9 Step 9: Configure IP-to-IP Manipulation Rules

This step describes how to configure IP-to-IP manipulation rules. These rules manipulate the source and / or destination number. The manipulation rules use the configured IP Groups to denote the source and destination of the call. As configured in Section 4.7 on page 37, IP Group 0 represents IP-PBX, and IP Group 1 represents BroadCloud SIP Trunk.



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

For example, for this interoperability test topology, a manipulation was configured to add the prefix to the destination number for calls from the IP-PBX IP Group to the BroadCloud SIP Trunk IP Group for specific destination username prefix.

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

1. Open the IP-to-IP Outbound Manipulation page (**Configuration** tab > **VoIP** menu > **SBC** > **Manipulations SBC** > **IP-to-IP Outbound**).
2. Click **Add**.
3. Click the **Rule** tab, and then configure the parameters as follows:

Parameter	Value
Index	0
Name	Call to desk
Source IP Group	IP-PBX
Destination IP Group	BroadCloud
Destination Username Prefix	4347

Figure 4-28: Configuring IP-to-IP Outbound Manipulation Rule – Rule Tab

Edit Row

Index
0
Routing Policy
Default_SBCRouting

Rule

Action

Name

Call to desk

Additional Manipulation

No

Request Type

All

Source IP Group

IP-PBX

Destination IP Group

BroadCloud

Source Username Prefix

*

Source Host

*

Destination Username Prefix

4347

Destination Host

*

Calling Name Prefix

*

Message Condition

None

Call Trigger

Any

ReRoute IP Group

Any

Save

Cancel

- Click the **Action** tab, and then configure the parameters as follows:

Parameter	Value
Manipulated Item	Destination URI
Prefix to Add	0119723976

Figure 4-29: Configuring IP-to-IP Outbound Manipulation Rule - Action Tab

Edit Row

Index: 0

Routing Policy: Default_SBCRouting

Rule **Action**

Manipulated Item: Destination URI

Remove From Left: 0

Remove From Right: 0

Leave From Right: 255

Prefix to Add: 0119723976

Suffix to Add:

Privacy Restriction Mode: Transparent

[Classic View](#)

Save Cancel

5. Click **Submit**.

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

Figure 4-30: Example of Configured IP-to-IP Outbound Manipulation Rules

▼ IP to IP Outbound Manipulation

Add + Edit Delete Insert + Up ↑ Down ↓
 ▼ All Search in table Search 🔍

Show / Hide

Index	Name	Routing Policy	Additio Mani	Source IP Group	Destinatio IP Group	Source Usernam Prefix	Destinat Usernam Prefix	Manipuli Item	Remove From Left	Remove From Right	Leave From Right	Prefix to Add	Suffix to Add
0	Call to desk	Default_S	No	IP-PBX	BroadCloud	*	4347	Destinatio	0	0	255	01197239	
1	Call to mobile	Default_S	No	IP-PBX	BroadCloud	*	4774	Destinatio	1	0	255	01197254	
2	For Anonymo	Default_S	No	IP-PBX	BroadCloud	*	*	Source UR	0	0	255		

Page 1 of 1 10 View 1 - 3 of 3

4.10 Step 10: 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).

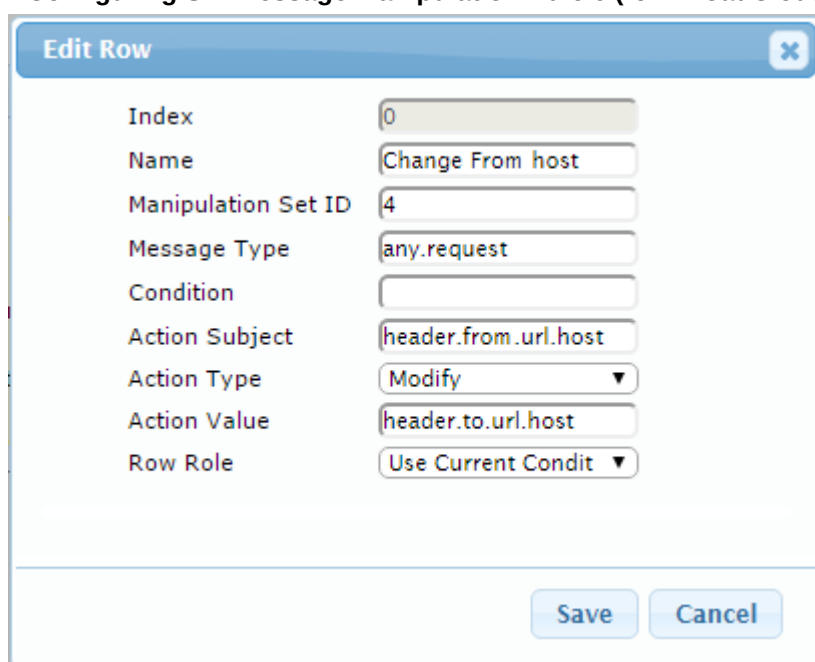
Once you have configured the SIP message manipulation rules, you need to assign them to the relevant IP Group (in the IP Group table) and determine whether they must be applied to inbound or outbound messages.

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

1. Open the Message Manipulations page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).
2. Configure a new manipulation rule (Manipulation Set 4) for BroadCloud SIP Trunk. This rule applies to messages sent to the BroadCloud SIP Trunk IP Group. This replaces the host part of the SIP From Header with the value from the SIP To Header.

Parameter	Value
Index	0
Name	Change From host
Manipulation Set ID	4
Message Type	any.request
Action Subject	header.from.url.host
Action Type	Modify
Action Value	header.to.url.host

Figure 4-31: Configuring SIP Message Manipulation Rule 0 (for BroadCloud SIP Trunk)



Edit Row

Index

0

Name

Change From host

Manipulation Set ID

4

Message Type

any.request

Condition

Action Subject

header.from.url.host

Action Type

Modify

Action Value

header.to.url.host

Row Role

Use Current Condit

Save

Cancel

3. Configure another manipulation rule (Manipulation Set 4) for BroadCloud SIP Trunk. This rule applies to messages sent to the BroadCloud SIP Trunk IP Group. This replaces the host part of the SIP P-Asserted-Identity Header with the value from the SIP To Header.

Parameter	Value
Index	1
Manipulation Name	Change P-Asserted host
Manipulation Set ID	4
Message Type	any.request
Condition	header.p-asserted-identity exists
Action Subject	header.p-asserted-identity
Action Type	Modify
Action Value	header.to.url.host

Figure 4-32: Configuring SIP Message Manipulation Rule 1 (for BroadCloud SIP Trunk)

The screenshot shows a web-based configuration interface for SIP message manipulation rules. A dialog box titled "Edit Row" is open, displaying the configuration for a rule with Index 1. The fields and their values are as follows:

Index	1
Name	Change P-Asserted host
Manipulation Set ID	4
Message Type	any.request
Condition	header.p-asserted-ident
Action Subject	header.p-asserted-ident
Action Type	Modify
Action Value	header.to.url.host
Row Role	Use Current Condit

At the bottom right of the dialog are "Save" and "Cancel" buttons.

4. Configure another manipulation rule (Manipulation Set 4) for BroadCloud SIP Trunk. This rule applies to messages sent to the BroadCloud SIP Trunk IP Group in the call transfer scenario. This replaces the user part of the SIP From Header with the value from the SIP Diversion Header.

Parameter	Value
Index	2
Manipulation Name	Diversion
Manipulation Set ID	4
Message Type	invite.request
Condition	header.diversion regex (<sip:)(.)(.)(@)(.)(.)
Action Subject	header.from.url.user
Action Type	Modify
Action Value	\$3

Figure 4-33: Configuring SIP Message Manipulation Rule 2 (for BroadCloud SIP Trunk)

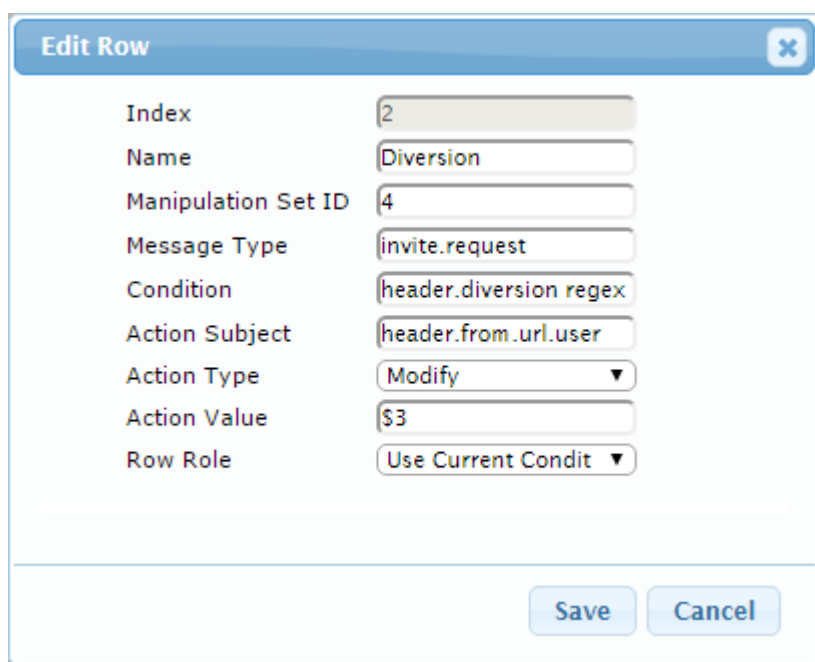
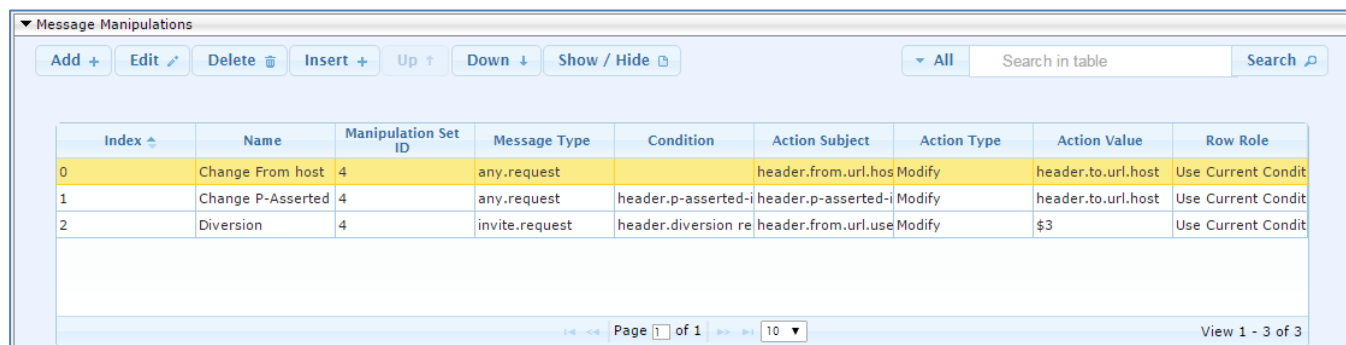


Figure 4-34: Example of Configured SIP Message Manipulation Rules



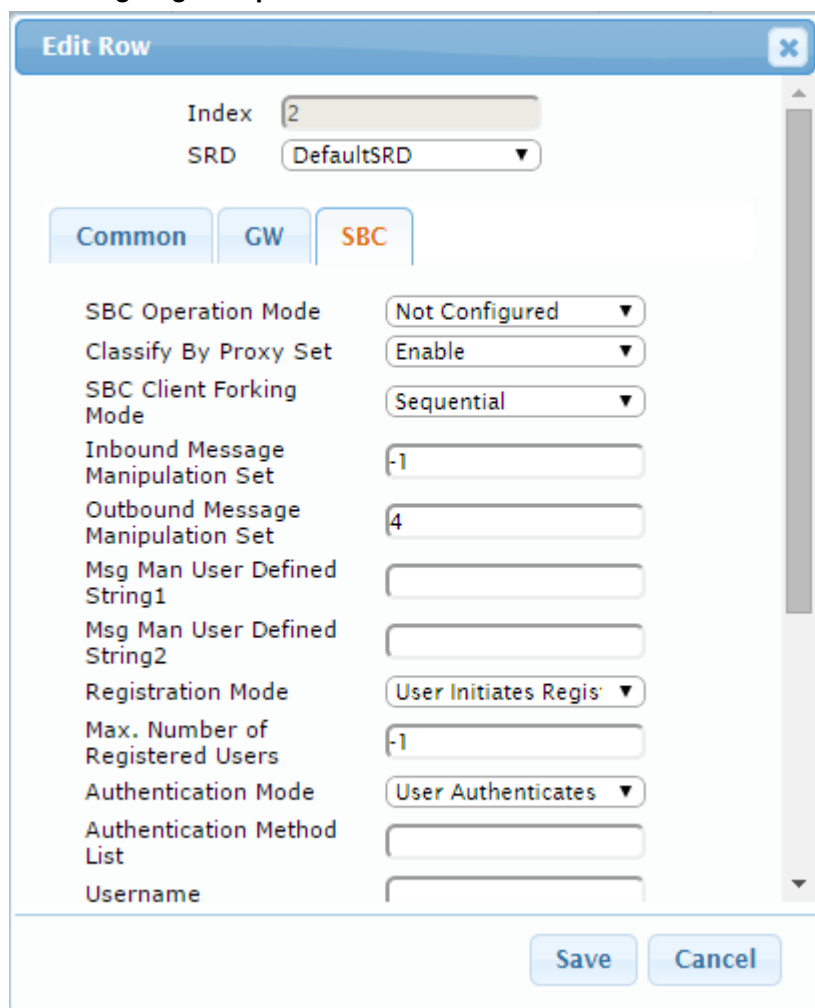
Index	Name	Manipulation Set ID	Message Type	Condition	Action Subject	Action Type	Action Value	Row Role
0	Change From host	4	any.request		header.from.url.hos	Modify	header.to.url.host	Use Current Condit
1	Change P-Asserted	4	any.request	header.p-asserted-i	header.p-asserted-i	Modify	header.to.url.host	Use Current Condit
2	Diversion	4	invite.request	header.diversion re	header.from.url.use	Modify	\$3	Use Current Condit

The table displayed below includes SIP message manipulation rules, which are bound together by commonality via the Manipulation Set ID 4, which are executed for messages sent to the BroadCloud SIP Trunk IP Group. These rules are specifically required to enable proper interworking between BroadCloud 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 applies to messages sent to the BroadCloud SIP Trunk IP Group. This replaces the host part of the SIP From Header with the value from the SIP To Header.	BroadCloud SIP Trunk required that all messages should be from known hosts.
1	This rule applies to messages sent to the BroadCloud SIP Trunk IP Group. This replaces the host part of the SIP P-Asserted-Identity Header with the value from the SIP To Header.	
2	This rule applies to messages sent to the BroadCloud SIP Trunk IP Group in the call transfer scenario. This replaces the user part of the SIP From Header with the value from the SIP Diversion Header.	

5. Assign Manipulation Set ID 4 to the BroadCloud SIP trunk IP Group:
 - a. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group Table**).
 - b. Select the row of the BroadCloud SIP trunk IP Group, and then click **Edit**.
 - c. Click the **SBC** tab.
 - d. Set the 'Outbound Message Manipulation Set' field to 4.

Figure 4-35: Assigning Manipulation Set 4 to the BroadCloud SIP Trunk IP Group



Edit Row

Index 2

SRD DefaultSRD

Common GW **SBC**

SBC Operation Mode Not Configured

Classify By Proxy Set Enable

SBC Client Forking Mode Sequential

Inbound Message Manipulation Set -1

Outbound Message Manipulation Set 4

Msg Man User Defined String1

Msg Man User Defined String2

Registration Mode User Initiates Regis'

Max. Number of Registered Users -1

Authentication Mode User Authenticates

Authentication Method List

Username

Save Cancel

- e. Click **Submit**.

4.11 Step 11: Configure Registration Accounts

This step describes how to configure SIP registration accounts. This is required so that the E-SBC can register with the BroadCloud SIP Trunk on behalf of IP-PBX. The BroadCloud SIP Trunk requires registration and authentication to provide service.

In the interoperability test topology, the Served IP Group is IP-PBX IP Group and the Serving IP Group is BroadCloud SIP Trunk IP Group.

➤ **To configure a registration account:**

1. Open the Account Table page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Account Table**).
2. Enter an index number (e.g., "0"), and then click **Add**.
3. Configure the account according to the provided information from , for example:

Parameter	Value
Application Type	SBC
Served IP Group	IP-PBX
Serving IP Group	BroadCloud
Username	As provided by BroadCloud
Password	As provided by BroadCloud
Host Name	interop.adpt-tech.com
Register	Regular
Contact User	8325624857 (pilot number)

4. Click **Apply**.

Figure 4-36: Configuring SIP Registration Account

The screenshot shows the 'Account Table' interface. At the top, there are buttons for 'Add +', 'Edit', 'Delete', 'Action', and 'Show / Hide'. Below these is a search bar with 'All' selected and a 'Search in table' input field. The table itself has columns: Index, Application Type, Served Trunk Group, Served IP Group, Serving IP Group, User Name, Password, Host Name, Register, and Contact User. A single row is displayed with the following values: Index 0, Application Type SBC, Served Trunk Group -1, Served IP Group IP-PBX, Serving IP Group BroadCloud, User Name 8325624857, Password *, Host Name interop.adpt-, Register Regular, and Contact User 8325624857. At the bottom, there is a pagination bar showing 'Page 1 of 1' and a 'View 1 - 1 of 1' indicator.

Index	Application Type	Served Trunk Group	Served IP Group	Serving IP Group	User Name	Password	Host Name	Register	Contact User
0	SBC	-1	IP-PBX	BroadCloud	8325624857	*	interop.adpt-	Regular	8325624857

4.12 Step 12: Miscellaneous Configuration

This section describes miscellaneous E-SBC configuration.

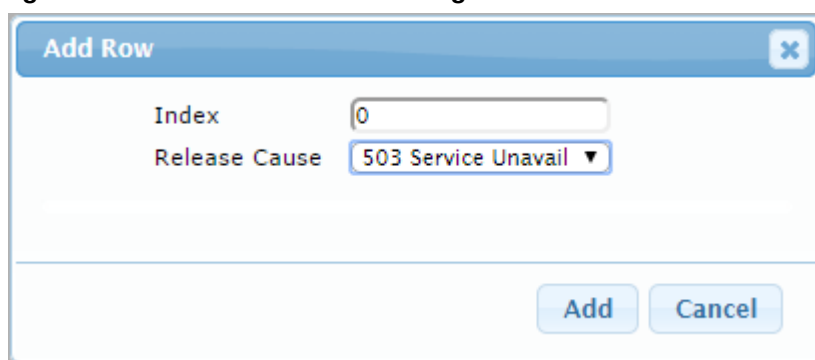
4.12.1 Step 12a: Configure SBC Alternative Routing Reasons

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 SBC Alternative Routing Reasons page (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **SBC Alternative Routing Reasons**).
2. Click **Add**; the following dialog box appears:

Figure 4-37: SBC Alternative Routing Reasons Table - Add Record



Add Row	
Index	0
Release Cause	503 Service Unavail ▼
Add Cancel	

3. Click **Submit**.

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 save the configuration to flash memory:**

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

Figure 4-38: Resetting the E-SBC

The screenshot displays a web-based configuration interface for an E-SBC. It is divided into three main sections, each with a dropdown arrow on the left:

- Reset Configuration:** Contains three rows. The first row is 'Reset Board' with a 'Reset' button. The second row is 'Burn To FLASH' with a dropdown menu set to 'Yes'. The third row is 'Graceful Option' with a dropdown menu set to 'No'.
- LOCK / UNLOCK:** Contains three rows. The first row is 'Lock' with a 'LOCK' button. The second row is 'Graceful Option' with a dropdown menu set to 'No'. The third row is 'Gateway Operational State' with the text 'UNLOCKED'.
- Save Configuration:** Contains one row, 'Burn To FLASH', with a 'BURN' button.

2. Ensure that the 'Burn to FLASH' field is set to **Yes** (default).
3. Click the **Reset** button.

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 25, is shown below:



Note: To load and save an ini file, use the Configuration File page (**Maintenance** tab > **Software Update** menu > **Configuration File**).

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

;Board: Mediant 800 E-SBC
;HW Board Type: 69  FK Board Type: 72
;Serial Number: 5916116
;Slot Number: 1
;Software Version: 7.00A.049.003
;DSP Software Version: 5014AE3_R => 700.44
;Board IP Address: 172.21.128.28
;Board Subnet Mask: 255.255.0.0
;Board Default Gateway: 172.21.1.1
;Ram size: 496M  Flash size: 64M  Core speed: 500Mhz
;Num of DSP Cores: 3  Num DSP Channels: 90
;Num of physical LAN ports: 4
;Profile: NONE
;;;Key features;;Board Type: 72 ;QOE features: VoiceQualityMonitoring
MediaEnhancement ;IP Media: VXML ;Channel Type: DspCh=90 ;HA ;BRITrunks=6
;DATA features: ;Security: IPSEC MediaEncryption StrongEncryption
EncryptControlProtocol ;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 ;DSP Voice features:
RTCP-XR V150=50 ;E1Trunks=2 ;T1Trunks=2 ;E&M Ports=6 ;Control Protocols:
MSFT FEU=600 TestCall=100 MGCP SIP SASurvivability SBC=100 ;Default
features;;Coders: G711 G726;

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

[SYSTEM Params]

SyslogServerIP = 172.20.22.17
EnableSyslog = 1
NTPServerUTCOffset = 7200
;VpFileLastUpdateTime is hidden but has non-default value
NTPServerIP = '0.0.0.0'
;LastConfigChangeTime 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]

```
EP_Num_0 = 0
EP_Num_1 = 1
EP_Num_2 = 1
EP_Num_3 = 0
EP_Num_4 = 0
```

[PSTN Params]

[SS7 Params]

[Voice Engine Params]

```
ENABLEMEDIASEcurity = 1
```

[WEB Params]

```
UserProductName = 'Mediant 800 E-SBC'
WebLogoText = 'BroadCloud'
UseWeblogo = 1
;UseLogoInWeb is hidden but has non-default value
UseProductName = 1
HTTPSCipherString = 'RC4:EXP'
;HTTPSPkeyFileName is hidden but has non-default value
```

[SIP Params]

```
MEDIACHANNELS = 30
GWDEBUGLEVEL = 5
;ISPRACKREQUIRED is hidden but has non-default value
ENABLESBCAPPLICATION = 1
```

```

MSLDAPPRIMARYKEY = 'telephoneNumber'
MEDIACDRREPORTLEVEL = 1
SBCFORKINGHANDLINGMODE = 1
ENERGYDETECTORCMD = 587202560
ANSWERDETECTORCMD = 10486144
;GWAPPCONFIGURATIONVERSION is hidden but has non-default value

[SCTP Params]

[IPsec Params]

[Audio Staging 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 0 = 1, "GROUP_1", "vlan 1", 0;
DeviceTable 1 = 2, "GROUP_2", "vlan 2", 0;

[ \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, 172.26.249.31, 24, 172.26.249.1, "ShoreTel",
0.0.0.0, 0.0.0.0, "vlan 1";
InterfaceTable 1 = 5, 10, 65.196.9.185, 28, 65.196.9.177, "DMZ",
198.6.1.146, 198.6.1.122, "vlan 2";

[ \InterfaceTable ]

[ DspTemplates ]

;
; *** TABLE DspTemplates ***
; This table contains hidden elements and will not be exposed.
; This table exists on board and will be saved during restarts.
;

[ \DspTemplates ]

[ WebUsers ]

FORMAT WebUsers_Index = WebUsers_Username, WebUsers_Password,
WebUsers_Status, WebUsers_PwAgeInterval, WebUsers_SessionLimit,
WebUsers_SessionTimeout, WebUsers_BlockTime, WebUsers_UserLevel,
WebUsers_PwNonce;
WebUsers 0 = "Admin",
"$1$z/3i5+fh5+Hn5rvq4+vruby+1NDS14XdhYPQ3onZjojYiZPDw8HAXpTCnJvLw8rIxppmZ
WczZ2c+P20x0D1u0zc=", 1, 0, 2, 15, 60, 200,
"a4e40b4a1ef60fad38601e9bf6d0c1ce";
WebUsers 1 = "User",
"$1$EiUhIXBycnohfit/L3otExUbFkYcFBJMERNJGUwYGVIGV1UFB1VSDl8MA1hbDA5ydHdx
CR/Jn15Ln11e38qMWg=", 3, 0, 2, 15, 60, 50,
"a5bdea28146076a2e00cabbb04f2139f";

[ \WebUsers ]

[ TLSContexts ]

FORMAT TLSContexts_Index = TLSContexts_Name, TLSContexts_TLSVersion,
TLSContexts_ServerCipherString, TLSContexts_ClientCipherString,
TLSContexts_OcspEnable, TLSContexts_OcspServerPrimary,
TLSContexts_OcspServerSecondary, TLSContexts_OcspServerPort,
TLSContexts_OcspDefaultResponse;
TLSContexts 0 = "default", 0, "RC4:EXP", "ALL:!ADH", 0, , , 2560, 0;

[ \TLSContexts ]

[ IpProfile ]
```

```

FORMAT IpProfile_Index = IpProfile_ProfileName, IpProfile_IpPreference,
IpProfile_CodersGroupID, IpProfile_IsFaxUsed,
IpProfile_JitterBufMinDelay, IpProfile_JitterBufOptFactor,
IpProfile_IPDiffServ, IpProfile_SigIPDiffServ, IpProfile_SCE,
IpProfile_RTPRedundancyDepth, IpProfile_RemoteBaseUDPPort,
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_SBCExtensionCodersGroupID,
IpProfile_MediaIPVersionPreference, IpProfile_TranscodingMode,
IpProfile_SBCAllowedMediaTypes, IpProfile_SBCAllowedCodersGroupID,
IpProfile_SBCAllowedVideoCodersGroupID, IpProfile_SBCAllowedCodersMode,
IpProfile_SBCMediaSecurityBehaviour, IpProfile_SBCRFC2833Behavior,
IpProfile_SBCAlternativeDTMFMethod, IpProfile_SBCAssertIdentity,
IpProfile_AMDSensitivityParameterSuit, IpProfile_AMDSensitivityLevel,
IpProfile_AMDMaxGreetingTime, IpProfile_AMDMaxPostSilenceGreetingTime,
IpProfile_SBCDiversionsMode, IpProfile_SBCHistoryInfoMode,
IpProfile_EnableQSIGTunneling, IpProfile_SBCFaxCodersGroupID,
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 1 = "IP-PBX", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0, 0,
0, -1, 1, 0, 0, -1, 0, 4, -1, 1, 1, 0, 0, "", -1, 0, 0, "", -1, -1, 0, 2,
0, 0, 0, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0, 2, 2, 1, 0, 0, 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, 300, -1, -1, 0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, -1, 0, "", 0;

IpProfile 2 = "BroadCloud", 1, 0, 0, 10, 10, 46, 40, 0, 0, 0, 0, 2, 0, 0,
0, 0, -1, 1, 0, 0, -1, 0, 4, -1, 1, 1, 0, 0, "", -1, 0, 0, "", -1, -1, 0,
2, 0, 0, 1, 0, 8, 300, 400, 0, 0, 0, -1, 0, 0, 1, 3, 0, 2, 2, 1, 0, 0, 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, 300, -1, -1, 0, 0, 0, 0, 0, 0, 0, -1, -1, -1, -1, -1, 0, "", 0;

```

```
[ \IpProfile ]

[ CpMediaRealm ]

FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName,
CpMediaRealm_IPv4IF, CpMediaRealm_IPv6IF, CpMediaRealm_PortRangeStart,
CpMediaRealm_MediaSessionLeg, CpMediaRealm_PortRangeEnd,
CpMediaRealm_IsDefault, CpMediaRealm_QoeProfile, CpMediaRealm_BWProfile;
CpMediaRealm 0 = "MRLan", "ShoreTel", "", 6000, 100, 6999, 0, "", "";
CpMediaRealm 1 = "MRWan", "DMZ", "", 7000, 100, 7999, 0, "", "";

[ \CpMediaRealm ]

[ SBCRoutingPolicy ]

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

[ \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 ]

[ SIPInterface ]

FORMAT SIPInterface_Index = SIPInterface_InterfaceName,
SIPInterface_NetworkInterface, SIPInterface_ApplicationType,
SIPInterface_UDPPort, SIPInterface_TCPPort, SIPInterface_TLSPort,
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 0 = "IP-PBX", "ShoreTel", 2, 5060, 0, 0, "DefaultSRD", "",
"", -1, 0, 500, -1, 0, "MRLan", 0, -1, -1, -1, 0;
SIPInterface 1 = "BroadCloud", "DMZ", 2, 5060, 0, 0, "DefaultSRD", "",
"", -1, 0, 500, -1, 0, "MRWan", 0, -1, -1, -1, 0;

[ \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_SASIPv4SIPInterfaceName,
ProxySet_GWIPv6SIPInterfaceName, ProxySet_SBCIPv6SIPInterfaceName,
ProxySet_SASIPv6SIPInterfaceName;
ProxySet 0 = "IP-PBX", 1, 60, 0, 0, "DefaultSRD", 0, "", -1, -1, "", "",
"IP-PBX", "", "", "", "";
ProxySet 1 = "BroadCloud", 1, 60, 0, 0, "DefaultSRD", 0, "", -1, 1, "",
"", "BroadCloud", "", "", "", "";

[ \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_EnableSBCCClientForking, IPGroup_SourceUriInput,
IPGroup_DestUriInput, IPGroup_ContactName, IPGroup_Username,
IPGroup_Password, IPGroup_UUIFormat, IPGroup_QOEProfile,
IPGroup_BWProfile, IPGroup_MediaEnhancementProfile,
IPGroup_AlwaysUseSourceAddr, IPGroup_MsgManUserDef1,
IPGroup_MsgManUserDef2, IPGroup_SIPConnect, IPGroup_SBCPSAPMode,
IPGroup_DTLSContext, IPGroup_CreatedByRoutingServer,
IPGroup_UsedByRoutingServer, IPGroup_SBCOperationMode,
IPGroup_SBCRouteUsingRequestURIPort, IPGroup_SBCKeepOriginalCallID,
IPGroup_SBCDialPlanName;
IPGroup 0 = 0, "IP-PBX", "IP-PBX", "172.26.249.130", "", -1, 0,
"DefaultSRD", "MRlan", 1, "IP-PBX", -1, -1, -1, 0, 0, "", 0, -1, -1, "",
"", "$1$gQ==", 0, "", "", "", 0, "", "", 0, 0, "", 0, 0, -1, 0, 0, "";
IPGroup 1 = 0, "BroadCloud", "BroadCloud", "interop.adpt-tech.com", "", -
1, 0, "DefaultSRD", "MRwan", 1, "BroadCloud", -1, -1, 4, 0, 0, "", 0, -1,
-1, "", "", "$1$gQ==", 0, "", "", "", 0, "", "", 0, 0, "", 0, 0, -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 = "0", 0, "172.26.249.130:5060", 0;
ProxyIp 1 = "1", 0, "nn6300southsipconnect.adpt-tech.com", 0;

```

```
[ \ProxyIp ]

[ Account ]

FORMAT Account_Index = Account_ServedTrunkGroup,
Account_ServedIPGroupName, Account_ServingIPGroupName, Account_Username,
Account_Password, Account_HostName, Account_Register,
Account_ContactUser, Account_ApplicationType;
Account 0 = -1, "IP-PBX", "BroadCloud", "8325624857",
"$1$SSg/LyUiDSA0NCFhZGRj", "interop.adpt-tech.com", 1, "8325624857", 2;

[ \Account ]

[ 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 0 = "Terminate OPTIONS", "Default_SBCRoutingPolicy", "Any",
"\"", "\"", "\"", "\"", 6, "\"", "Any", 0, -1, 1, "\"", "\"", "internal", 0, -1, 0,
0, "\"", "\"", "\"";
IP2IPRouting 1 = "IP-PBX to ITSP", "Default_SBCRoutingPolicy", "IP-PBX",
"\"", "\"", "\"", "\"", 0, "\"", "Any", 0, -1, 0, "BroadCloud", "BroadCloud",
"\"", 0, -1, 0, 0, "\"", "\"", "\"";
IP2IPRouting 2 = "ITSP to IP-PBX", "Default_SBCRoutingPolicy",
"\"BroadCloud\"", "\"", "\"", "\"", "\"", 0, "\"", "Any", 0, -1, 0, "IP-PBX", "IP-
PBX", "\"", 0, -1, 0, 0, "\"", "\"", "\"";

[ \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 = "Clip 1", "Default_SBCRoutingPolicy", 0, "IP-
PBX", "BroadCloud", "", "*", "[1732,1832]", "", "*", "", 0, "Any", 0,
1, 1, 0, 255, "", "", 0, "", "";
IPOutboundManipulation 1 = "Clip +1 from source",
"Default_SBCRoutingPolicy", 0, "IP-PBX", "BroadCloud", "+", "", "",
"*, "", "", 0, "Any", 0, 0, 2, 0, 255, "", "", 0, "", "";
IPOutboundManipulation 2 = "Call to desk", "Default_SBCRoutingPolicy", 0,
"IP-PBX", "BroadCloud", "", "*", "1170", "", "*", "", 0, "Any", 0, 1,
0, 0, 255, "1732652", "", 0, "", "";
IPOutboundManipulation 3 = "4852->118", "Default_SBCRoutingPolicy", 0,
"BroadCloud", "IP-PBX", "", "*", "8325624852", "", "*", "", 0, "Any",
0, 1, 10, 0, 255, "118", "", 0, "", "";
IPOutboundManipulation 4 = "4853->119", "Default_SBCRoutingPolicy", 0,
"BroadCloud", "IP-PBX", "", "*", "8325624853", "", "*", "", 0, "Any",
0, 1, 10, 0, 255, "119", "", 0, "", "";
IPOutboundManipulation 5 = "For Test 19", "Default_SBCRoutingPolicy", 0,
"BroadCloud", "IP-PBX", "", "*", "*", "*", "*", "*", "", 0, "Any", 0, 0, 0,
0, 255, "", "", 0, "", "";

[ \IPOutboundManipulation ]

[ CodersGroup0 ]

FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime,
CodersGroup0_rate, CodersGroup0_PayloadType, CodersGroup0_Sce,
CodersGroup0_CoderSpecific;
CodersGroup0 0 = "g711Ulaw64k", 20, 0, -1, 0, "";
CodersGroup0 1 = "g711Alaw64k", 20, 0, -1, 0, "";

[ \CodersGroup0 ]

[ CodersGroup1 ]

FORMAT CodersGroup1_Index = CodersGroup1_Name, CodersGroup1_pTime,
CodersGroup1_rate, CodersGroup1_PayloadType, CodersGroup1_Sce,
CodersGroup1_CoderSpecific;
CodersGroup1 0 = "g711Ulaw64k", 20, 0, -1, 0, "";
CodersGroup1 1 = "g711Alaw64k", 20, 0, -1, 0, "";

[ \CodersGroup1 ]

[ CodersGroup2 ]

FORMAT CodersGroup2_Index = CodersGroup2_Name, CodersGroup2_pTime,
CodersGroup2_rate, CodersGroup2_PayloadType, CodersGroup2_Sce,
CodersGroup2_CoderSpecific;
CodersGroup2 0 = "g729", 20, 0, -1, 0, "";

[ \CodersGroup2 ]

[ AllowedCodersGroup1 ]

FORMAT AllowedCodersGroup1_Index = AllowedCodersGroup1_Name;

```

```

AllowedCodersGroup1 0 = "g711Ulaw64k";
AllowedCodersGroup1 1 = "g711Alaw64k";

[ \AllowedCodersGroup1 ]

[ AllowedCodersGroup2 ]

FORMAT AllowedCodersGroup2_Index = AllowedCodersGroup2_Name;
AllowedCodersGroup2 0 = "g729";
AllowedCodersGroup2 1 = "g711Alaw64k";

[ \AllowedCodersGroup2 ]

[ MessageManipulations ]

FORMAT MessageManipulations_Index =
MessageManipulations_ManipulationName, MessageManipulations_ManSetID,
MessageManipulations_MessageType, MessageManipulations_Condition,
MessageManipulations_ActionSubject, MessageManipulations_ActionType,
MessageManipulations_ActionValue, MessageManipulations_RowRole;
MessageManipulations 0 = "Change From host", 4, "any.request", "",
"header.from.url.host", 2, "header.to.url.host", 0;
MessageManipulations 1 = "Change P-Asserted host", 4, "any.request",
"header.p-asserted-identity exists", "header.p-asserted-
identity.url.host", 2, "header.to.url.host", 0;
MessageManipulations 2 = "Diversion", 4, "invite.request",
"header.diversion regex (<sip:)(..)(.*)"(.*)"(.*)", "header.from.url.user",
2, "$3", 0;

[ \MessageManipulations ]

[ GwRoutingPolicy ]

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

[ \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 ]

```

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: www.audiocodes.com/info

Website: www.audiocodes.com



Document #: LTRT-12560