

Enterprise Session Border Controllers

Mediant™ E-SBC Series

AudioCodes®

SBC Deployment Guide

Architecture Options and Configuration Examples



Version 6.4

April 2012

Document # LTRT-31620



Table of Contents

1	Introduction	7
2	Typical Applications	9
2.1	Enterprise IP PBX and ITSP SIP Trunk	9
2.2	Two Local SIP Entity Servers.....	9
2.3	Hosted IP PBX	10
3	Deployment Architecture.....	11
3.1	Location of E-SBC at the Enterprise	11
3.1.1	Connected to LAN using Single Network Interface	11
3.1.2	Connected to DMZ Network using Single Network Interface	12
3.1.3	Connected to LAN and DMZ using Two Network Interfaces.....	12
3.2	E-SBC Physical LAN Port Connections	13
3.2.1	Connected to LAN or DMZ	13
3.2.2	Connected to LAN and DMZ	13
3.3	Deployments Requiring Multiple SRDs	14
4	SBC Configuration Examples	15
4.1	Enterprise IP PBX with SIP Trunk and WAN Users	16
4.1.1	Step 1: Add Logical IP Network Interfaces for LAN and WAN	19
4.1.2	Step 2: Enable the SBC Application	20
4.1.3	Step 3: Add Media Realms for LAN and WAN	20
4.1.4	Step 4: Add SRDs for LAN and WAN.....	22
4.1.5	Step 5: Add SIP Interfaces for LAN and WAN.....	23
4.1.6	Step 6: Add IP Groups for IP PBX and ITSP Servers	24
4.1.7	Step 7: Add Proxy Sets for IP PBX and ITSP Servers	26
4.1.8	Step 8: Add Classification Rule for WAN Nomadic Users.....	28
4.1.9	Step 9: Add IP-to-IP Call Routing Rules.....	29
4.1.10	Step 10: Reset E-SBC and Verify Configuration in Syslog	30
4.1.11	Alternative Routing upon SIP Trunk Failure	31
4.1.11.1	SIP Trunk Redundancy	31
4.1.11.2	Setting up PSTN Fallback	36
4.2	Hosted IP PBX	44
4.2.1	Step 1: Add a Logical IP Network Interface for LAN and WAN	47
4.2.2	Step 2: Enable the SBC Application	47
4.2.3	Step 3: Add Media Realms for LAN and WAN	47
4.2.4	Step 4: Add SRDs for LAN and WAN.....	49
4.2.5	Step 5: Add SIP Interfaces for LAN and WAN.....	50
4.2.6	Step 6: Configure a NAT Translation Rule	50
4.2.7	Step 7: Add IP Groups for LAN Users and Hosted IP PBX.....	51
4.2.8	Step 8: Add Proxy Set for Hosted IP PBX Server	53
4.2.9	Step 9: Add Classification Rule for LAN Users	54
4.2.10	Step 10: Add IP-to-IP Call Routing Rules.....	55
4.2.11	Call Survivability for LAN Users.....	56
4.2.11.1	Step 1: Enable Keep-Alive for WAN IP PBX.....	56
4.2.11.2	Step 2: Add Alternative IP-to-IP Call Routing Rule for Call Survivability ..	57
4.2.12	Step 11: Reset E-SBC and Verify Configuration in Syslog	58
4.3	SIP Normalization between SIP Entity Servers.....	59
4.3.1	Step 1: Add a Logical IP Network Interface for LAN	62
4.3.2	Step 2: Enable the SBC Application	62
4.3.3	Step 3: Add a SIP Interface for LAN.....	62
4.3.4	Step 4: Add IP Groups for SIP Entity Servers	63

4.3.5	Step 5: Add Proxy Sets for SIP Entity Servers	64
4.3.6	Step 6: Add IP-to-IP Call Routing Rules.....	66
4.3.7	Voice Transcoding	67
4.3.7.1	Step 1: Add Coder Groups for SIP Entities	68
4.3.7.2	Step 2: Add IP Profiles for SIP Entities	69
4.3.7.3	Step 3: Assign IP Profiles to SIP Entity IP Groups	69
4.3.8	Number Manipulation.....	71
4.3.9	SIP Message Manipulation	72
4.3.9.1	Step 1: Add a SIP Message Manipulation Rule	72
4.3.9.2	Step 2: Assign Manipulation Rule to IP Group of SIP Entity Server #2 ...	74

Notice

This document provides an overview of typical SBC deployment topologies and configuration examples for AudioCodes Mediant Enterprise Session Border Controllers (E-SBC).

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. Before consulting this document, check the corresponding Release Notes regarding feature preconditions and/or specific support in this release. In cases where there are discrepancies between this document and the Release Notes, the information in the Release Notes supersedes that in this document. Updates to this document and other documents as well as software files can be downloaded by registered customers at <http://www.audiocodes.com/downloads>.

© Copyright 2012 AudioCodes Ltd. All rights reserved.

This document is subject to change without notice.

Date Published: April-24-2012

Trademarks

AudioCodes, AC, AudioCoded, Ardito, CTI2, CTI², CTI Squared, HD VoIP, HD VoIP Sounds Better, InTouch, IPmedia, Mediant, MediaPack, NetCoder, Netrake, Nuera, Open Solutions Network, OSN, Stretto, TrunkPack, VMAS, VoicePacketizer, VoIPerfect, VoIPerfectHD, What's Inside Matters, Your Gateway To VoIP and 3GX 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 service are generally provided by AudioCodes' Distributors, Partners, and Resellers from whom the product was purchased. For technical support for products purchased directly from AudioCodes, or for customers subscribed to AudioCodes Customer Technical Support (ACTS), contact support@audiocodes.com.

Abbreviations and Terminology

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

Related Documentation

Manual Name
Mediant 800 MSBG SIP User's Manual
Mediant 800 Gateway and E-SBC SIP User's Manual
Mediant 1000 MSBG User's Manual
Mediant 1000B Gateway & E-SBC User's Manual
Mediant 3000 SIP User's Manual
Mediant 4000 E-SBC User's Manual
Mediant Software E-SBC User's Manual



Note: Throughout this manual, unless otherwise specified, the term *E-SBC* refers to AudioCodes E-SBC products.



Note: The scope of this document does not fully cover security aspects for deploying the device in your environment. Security measures should be done in accordance with your organization's security policies. For basic security guidelines, you can refer to AudioCodes Recommended Security Guidelines document.



Note: This document describes typical E-SBC deployments. However, your E-SBC deployment may require additional configurations specific to your network topology. If you have any questions regarding required configuration, please contact your AudioCodes sales representative.

1 Introduction

This document describes typical deployment topologies for AudioCodes family of Mediant™ Enterprise Session Border Controllers (E-SBC) products and provides step-by-step configuration examples of various E-SBC applications.

This document is applicable to the following AudioCodes E-SBC products:

- Mediant 800 MSBG
- Mediant 800 Gateway & SBC
- Mediant 1000 MSBG
- Mediant 1000B Gateway & SBC
- Mediant 3000
- Mediant 4000 E-SBC
- Mediant Software E-SBC

Reader's Notes

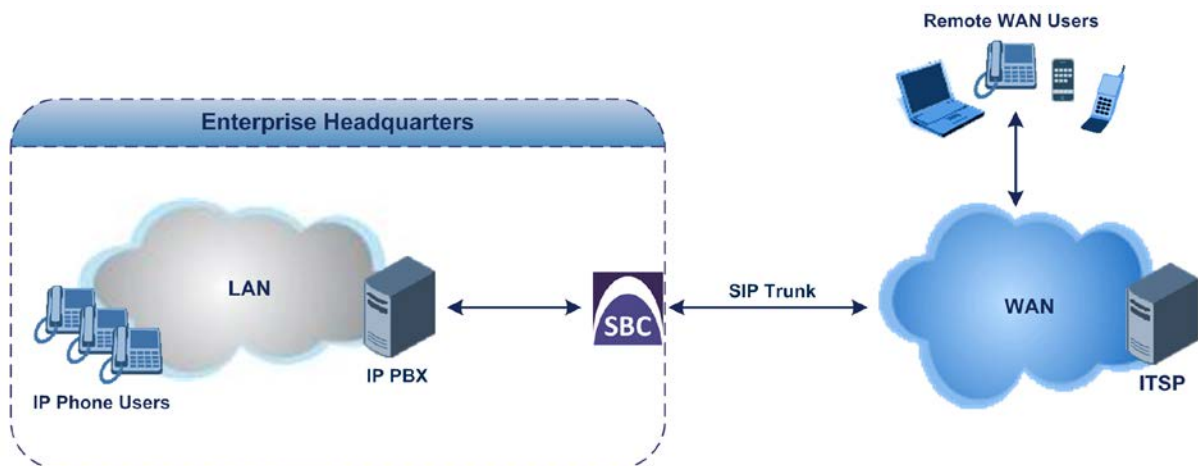
2 Typical Applications

This section describes typical Enterprise applications in which the E-SBC device can be deployed.

2.1 Enterprise IP PBX and ITSP SIP Trunk

The E-SBC can be deployed in applications in which it interfaces between a local IP PBX, located in the Enterprise LAN, and a SIP Trunk provided by an Internet Telephony Service Provider (ITSP). In addition, the application can include remote users (or far-end users) located in the WAN, and that may be located behind NAT.

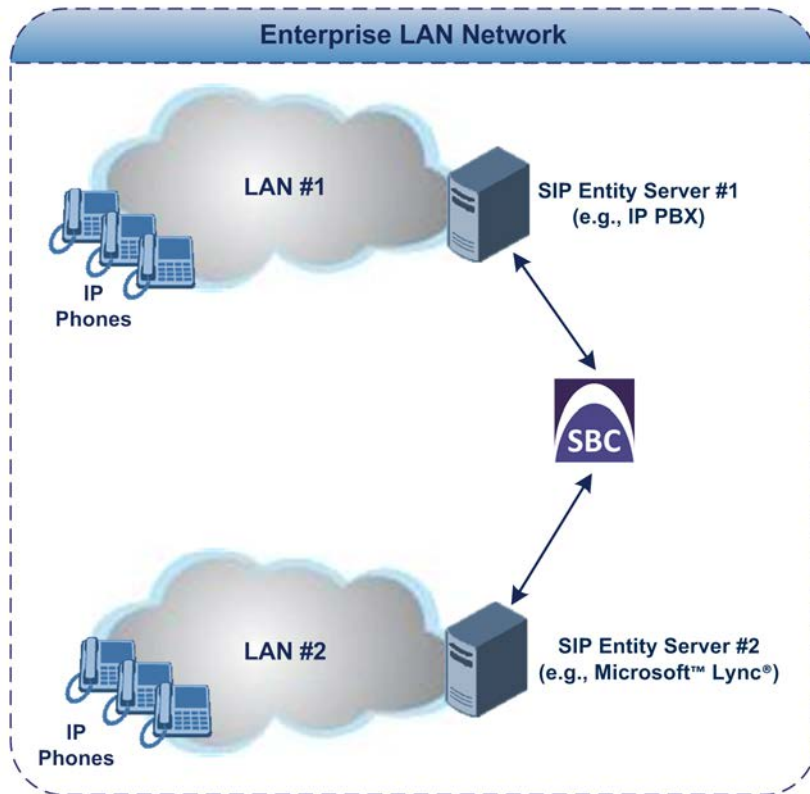
Figure 2-1: Application of Enterprise IP PBX and ITSP SIP Trunk



2.2 Two Local SIP Entity Servers

The E-SBC can be deployed in applications in which it interfaces between two local SIP entity servers (e.g., IP PBX and Microsoft Lync Server 2010) located in the Enterprise LAN. In such applications, the E-SBC is typically implemented for SIP normalization and voice transcoding.

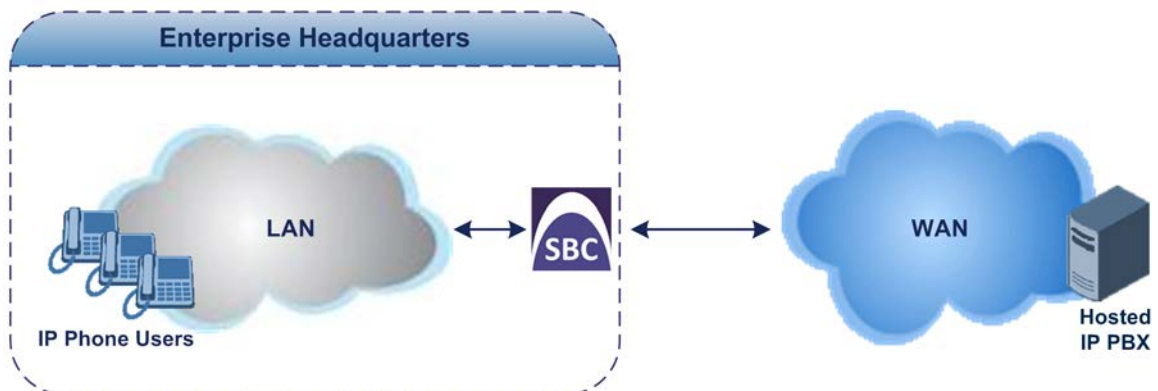
Figure 2-2: Application of Two Local SIP Entity Servers (e.g., IP PBXs)



2.3 Hosted IP PBX

The E-SBC can be deployed in applications in which it interfaces between the Enterprise users located in the LAN and a hosted IP PBX located in the WAN.

Figure 2-3: Application of Enterprise Users and Hosted IP PBX



3 Deployment Architecture

This chapter provides an overview of typical network topologies in which the E-SBC can be deployed. The topology includes the following factors:

- Number of E-SBC logical network
- Number of E-SBC physical LAN ports
- Number of SRDs

Once you have established the required network topology, you can configure the E-SBC accordingly.

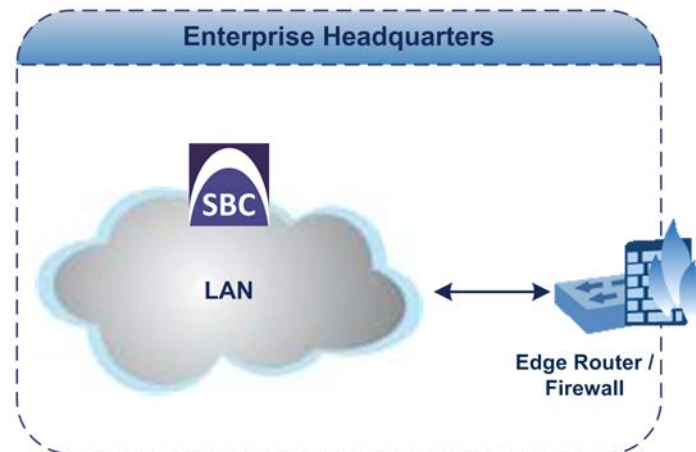
3.1 Location of E-SBC at the Enterprise

This section describes various methods that the E-SBC can be connected to the Enterprise network.

3.1.1 Connected to LAN using Single Network Interface

The E-SBC can be connected to the Enterprise LAN through a single logical network interface.

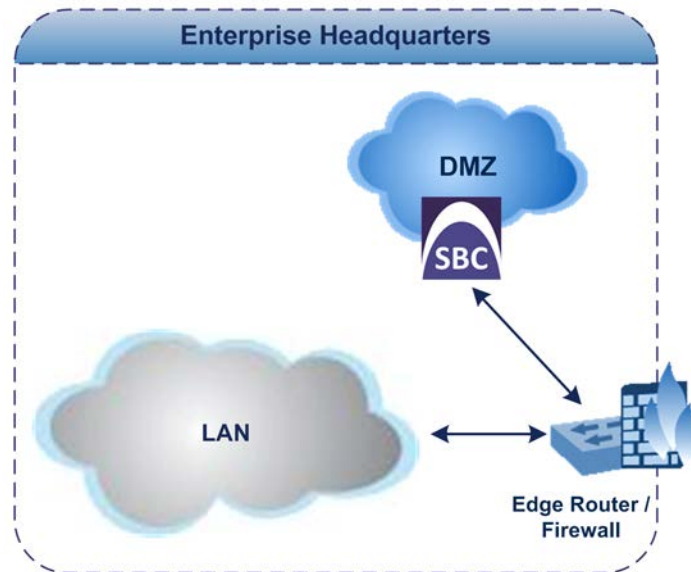
Figure 3-1: Connected to LAN through Single Logical Network Interface



3.1.2 Connected to DMZ Network using Single Network Interface

The E-SBC can be connected to the Enterprise's Demilitarized Zone network (DMZ) through a single logical network interface.

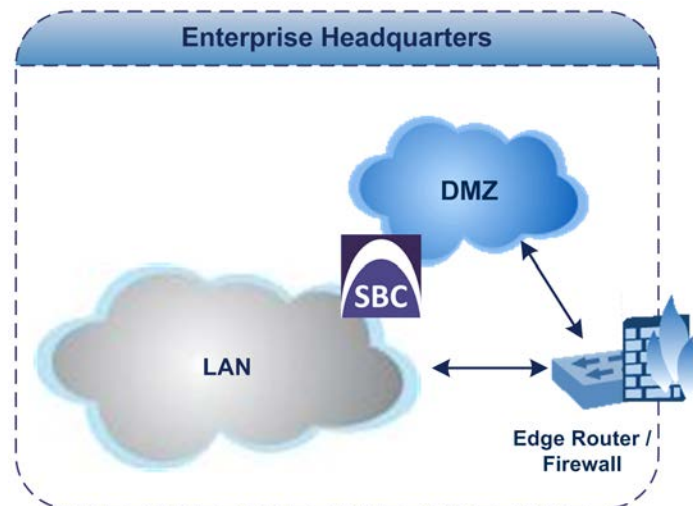
Figure 3-2: Single Logical Network Interface to Enterprise DMZ



3.1.3 Connected to LAN and DMZ using Two Network Interfaces

The E-SBC can be connected to the Enterprise network through two network interfaces – one interfacing with the DMZ network and one interfacing with the LAN.

Figure 3-3: One Logical Network Interface to Enterprise LAN and One to DMZ



3.2 E-SBC Physical LAN Port Connections

This section describes typical physical LAN port connections of the deployed E-SBC at the Enterprise. The type of physical LAN connection depends on the method used for connecting to the Enterprise's network, as discussed in Section 3.1 on page 11.

3.2.1 Connected to LAN or DMZ

If the E-SBC is connected to the Enterprise's LAN (or DMZ) with one logical network interface, the number of E-SBC physical LAN port connections can be any of the following, depending on requirements:

- One LAN port (i.e., one network cable)
- If 1+1 LAN port redundancy is required, then two LAN ports are used (i.e., two network cables)



Note: LAN port redundancy is applicable only to the following E-SBC products:

- Mediant 800 Gateway & SBC
- Mediant 1000 Gateway & SBC
- Mediant 3000
- Mediant 4000 E-SBC

3.2.2 Connected to LAN and DMZ

If the E-SBC is connected with two logical network interfaces at the Enterprise—one to the LAN and one to the DMZ—the number of E-SBC physical LAN port connections can be any of the following, depending on setup:

- E-SBC connects to a VLAN-aware switch with one LAN port (i.e., one network cable)
- E-SBC connects to a VLAN-aware switch with two LAN ports for 1+1 LAN port redundancy (i.e., two ports and network cables)
- E-SBC connects to LAN and DMZ using dedicated LAN ports (i.e., two ports and network cables)
- E-SBC connects to LAN and DMZ using dedicated LAN ports and with 1+1 LAN port redundancy (i.e., four ports and network cables)



Note: Physical network separation using different LAN ports is applicable only to the following E-SBC products:

- Mediant 800 Gateway & SBC
- Mediant 1000 Gateway & SBC (using SWX module)
- Mediant 4000 E-SBC
- Mediant Software E-SBC (**not supporting 1+1 LAN port redundancy**)

3.3 Deployments Requiring Multiple SRDs

The *SRD* represents a logical VoIP network entity. You need to implement multiple SRDs in the following deployment scenarios:

- E-SBC needs to resolve NAT traversal
- E-SBC has two logical network interfaces for SIP signaling traffic (i.e., of *Control* application type)
- Different security policies are required for different networks (e.g., using Classification rules or call admission control – configured per SRD)

4 SBC Configuration Examples

This chapter provides configuration steps for various SBC example scenarios.

Before configuring the E-SBC, you should familiarize yourself with some of the related configuration terms used in these examples – see the table below.

Table 4-1: Configuration Terms

Term	Description
<i>SRD</i>	Represents a logical VoIP network.
<i>Media Realm</i>	Defines a UDP port range for RTP (media) traffic on a specific logical IP network interface of the E-SBC.
<i>SIP Interface</i>	Defines a listening port for SIP signaling traffic on a specific logical IP network interface of the E-SBC.
<i>IP Group</i>	Represents a SIP entity with which the E-SBC does call routing. 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. The IP Groups are typically assigned to IP-to-IP call routing rules for denoting the source and destination of calls.
<i>Proxy Set</i>	Defines the destination addresses (IP address or FQDN) of the SIP entity server.
<i>IP Profile</i>	Defines a set of call behavior (e.g., required coders, fax transport type, and transcoding method) that can be associated to a specific IP Group.
<i>Classification</i>	Process that identifies the IP Group from where the call is received.

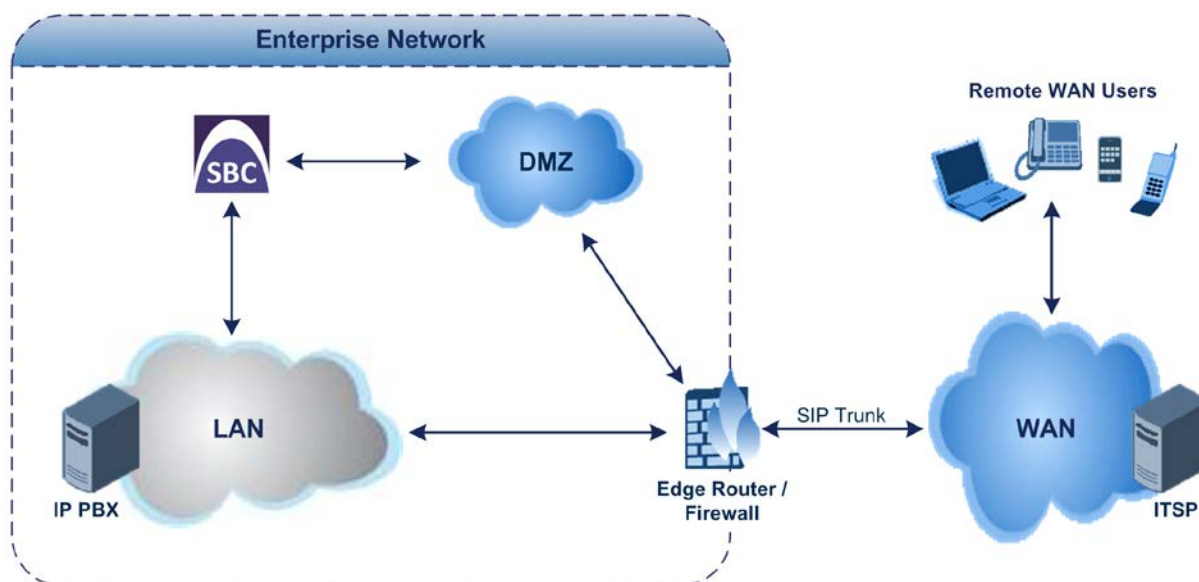
4.1 Enterprise IP PBX with SIP Trunk and WAN Users

This example scenario includes the following topology architecture:

■ **Application:**

- Enterprise LAN IP PBX at IP address, 10.33.6.100.
- WAN SIP Trunk at IP address, 212.199.200.10.
- Nomadic WAN users.
- PSTN Fallback, whereby calls from the IP PBX are re-routed to the PSTN upon a WAN failure.

Figure 4-1: Application Topology of Local IP PBX with SIP Trunk Example



■ **Topology:**

• **E-SBC Logical Network Interface Connections:**

- ◆ One logical network interfacing with the LAN, using IP address 10.33.4.176. This interface is also used for the E-SBC management interface (OAMP).
- ◆ One logical network interfacing with the DMZ / WAN, using IP address 212.199.200.90.

• **E-SBC Physical LAN Port Connections:**

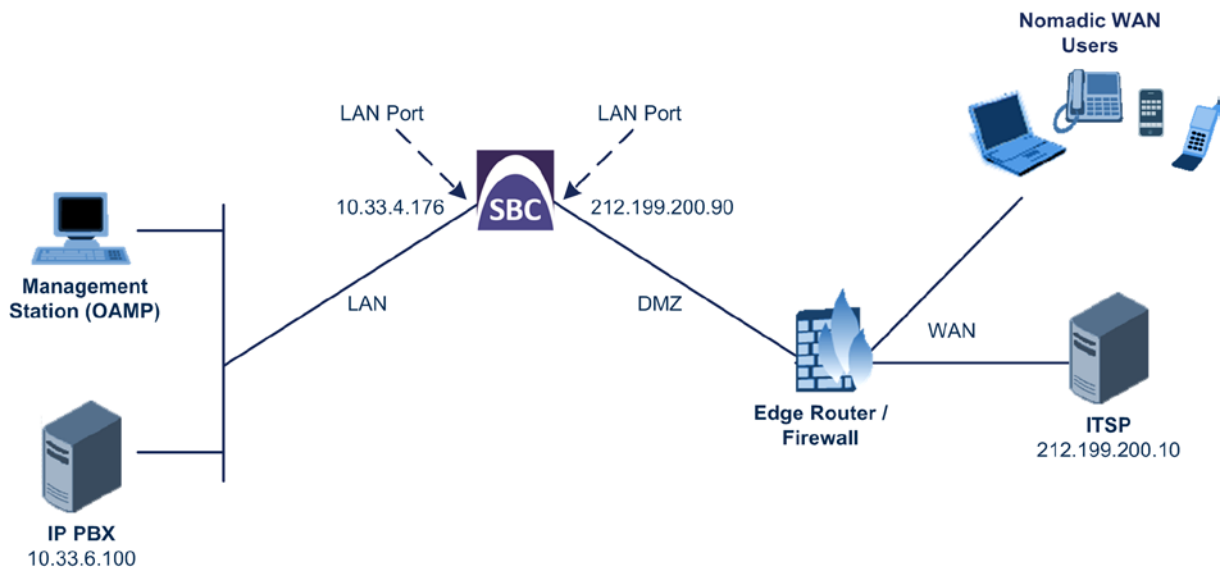
- ◆ One LAN port connected to the LAN.
- ◆ One LAN port connected to the DMZ / WAN.



Note: Regarding LAN port connections, the E-SBC could alternatively use a **single** LAN port, physically connected to a VLAN-aware switch.

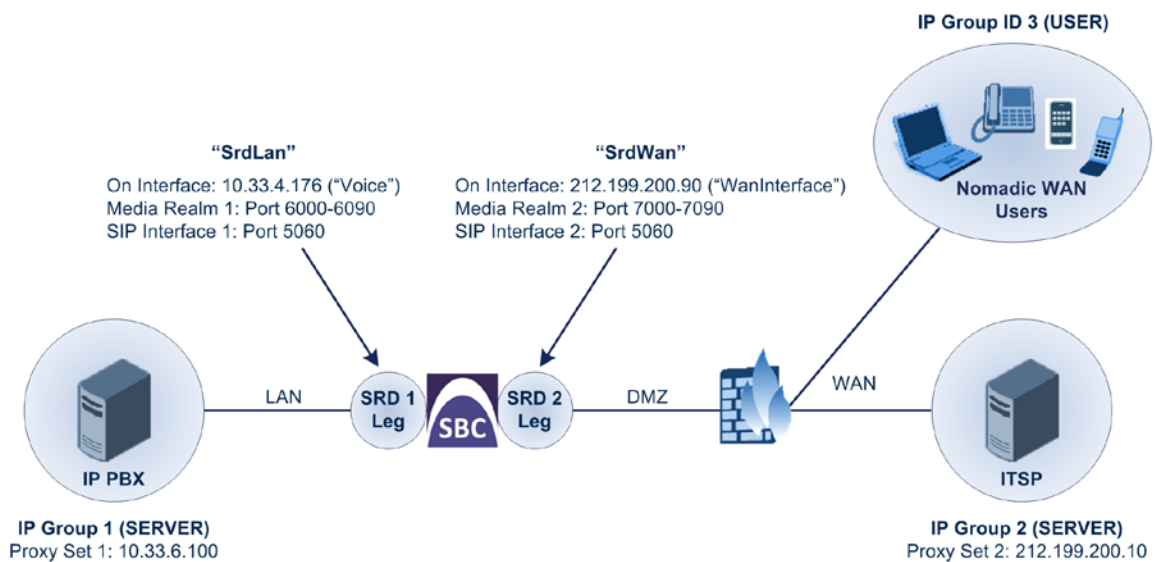
The figure below illustrates the E-SBC logical network interfaces and LAN port connections used in this example scenario:

Figure 4-2: E-SBC Logical Interfaces and Physical Port Connections



The required configuration entities used in this example are shown below:

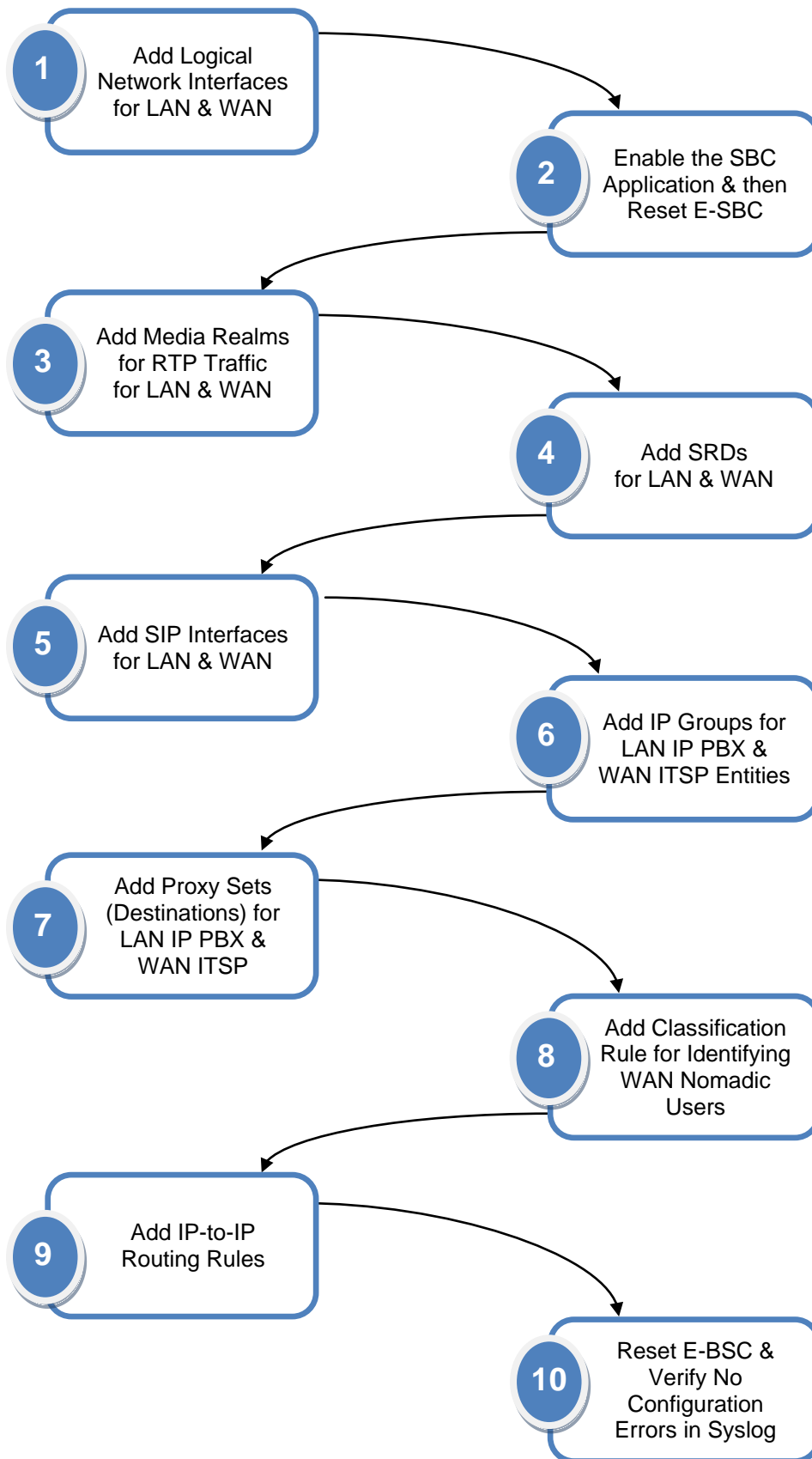
Figure 4-3: Required Configuration Entities



Note: For clarity, whenever configuring the various entities in this example (e.g., SRDs, Media Realms, SIP Interfaces, and IP Groups), table row index 1 is used for the E-SBC network interfacing with the LAN; table row index 2 is used for the E-SBC network interfacing with the WAN.

The configuration steps for this example scenario are summarized in the flowchart below:

Figure 4-4: Summary of Configuration Steps



4.1.1 Step 1: Add Logical IP Network Interfaces for LAN and WAN

In the example, the E-SBC uses two logical IP network interfaces:

- One logical network interfacing with the WAN, using IP address 212.199.200.90
- One logical network interfacing with the LAN, using IP address 10.33.4.176

As the network interfacing with the LAN is the same as that used for management (i.e., OAMP), which is already setup, you only need to configure the logical network interfacing with the WAN. The LAN interface is assumed to be configured for index 0:

- **Application Type:** OAMP + Media + Control
- **IP Address:** 10.33.4.176
- **Prefix Length:** 16
- **Gateway:** 10.33.0.1
- **VLAN ID:** 1
- **Interface Name:** Voice
- **Underlying Interface:** GROUP_1

This example also implements physical LAN port separation per network interface. As the E-SBC is not connected to a VLAN-aware switch, you need to configure the E-SBC to use untagged traffic. This is done by setting the Native VLAN of the port group to the same VLAN ID assigned to the network interface.

➤ **To add the logical IP network interfaces:**

1. Open the Multiple Interface Table page (**Configuration** tab > **VoIP** menu > **Network** > **IP Settings**).
2. Add an IP network interface to row index 1 for the WAN interface:
 - **Application Type:** Media + Control
 - **IP Address:** 212.199.200.90
 - **Prefix Length:** 16
 - **Gateway:** 212.199.200.1
 - **VLAN ID:** 2
 - **Interface Name:** WanInterface
 - **Underlying Interface:** GROUP_2

Figure 4-5: Logical IP Network Interfaces for LAN and WAN

Index	Application Type	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name	Primary DNS Server IP Address	Secondary DNS Server IP Address	Underlying Interface
0	OAMP + Media + Control	10.33.4.176	16	10.33.0.1	1	Voice	0.0.0.0	0.0.0.0	GROUP_1
1	Media + Control	212.199.200.90	16	212.199.200.1	2	WanInterface	0.0.0.0	0.0.0.0	GROUP_2

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



Notes:

- For this setting to take effect, a reset is required. However, this will be done later in this section.
- **Interface Name** value must be unique and set to a value other than "WAN" (reserved).
- **Underlying Interface** denotes the physical LAN port group associated with the network interface. This example uses the GROUP_1 and GROUP_2 ports.

4. Set the Native VLAN ID:
 - a. Open the Physical Ports Settings page (**Configuration** tab > **VoIP** menu > **Network** > **Physical Ports Settings**).
 - b. For GROUP_1 ports (which you assigned previously to your IP network interface "Voice"), set the following:
 - ◆ **Native VLAN:** 1
 - c. For GROUP_2 ports (which you assigned previously to your IP network interface "WanInterface"), set the following:
 - ◆ **Native VLAN:** 2

Figure 4-6: Port Native VLAN

Index	Port	Mode	Native Vlan	Speed&Duplex	Description	Group Member	Group Status
1	GE_0_1	Enable	1	Auto Negotiation	User Port #0	GROUP_1	Active
2	GE_0_2	Enable	1	Auto Negotiation	User Port #1	GROUP_1	Redundant
3	GE_7_1	Enable	2	Auto Negotiation	User Port #0	GROUP_2	Active
4	GE_7_2	Enable	2	Auto Negotiation	User Port #3	GROUP_2	Redundant

5. Click **Apply**.

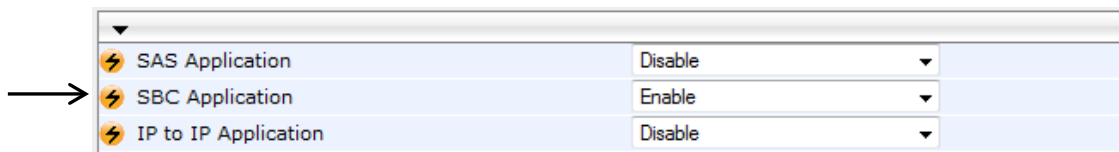
4.1.2 Step 2: Enable the SBC Application

For the E-SBC to operate as an SBC, you need to enable the SBC application. Once enabled, the SBC-specific parameters and pages become available in the Web interface.

➤ **To enable the SBC application:**

1. Open the Applications Enabling page (**Configuration** tab > **VoIP** menu > **Applications Enabling** > **Applications Enabling**).
2. From the 'SBC Application' drop-down list, select **Enable**.

Figure 4-7: Enabling the SBC Application



3. Click **Submit** to apply the changes.
4. Save your setting to flash memory ("burn") with a device reset.

4.1.3 Step 3: Add Media Realms for LAN and WAN

You need to add Media Realms for the LAN and WAN interfaces.

➤ **To add Media Realms:**

1. Open the Media Realm Table page (**Configuration** tab > **VoIP** menu > **Media** > **Media Realm Configuration**).
2. Add a Media Realm to index 1 for the LAN interface:
 - **Media Realm Name:** MediaRealmLan
 - **IPv4 Interface Name:** Voice
 - **Port Range Start:** 6000
 - **Number of Media Session Legs:** 10

Figure 4-8: Media Realm for LAN Interface

Add Record	
Index	1
Media Realm Name	MediaRealmLan
IPv4 Interface Name	Voice
IPv6 Interface Name	None
Port Range Start	6000
Number Of Media Session Legs	10
Port Range End	
Trans Rate Ratio	
Is Default	No
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

- Add a Media Realm to index 2 for the WAN interface:
 - Media Realm Name:** MediaRealmWan
 - IPv4 Interface Name:** WanInterface
 - Port Range Start:** 7000
 - Number of Media Session Legs:** 10

Figure 4-9: Media Realm for WAN Interface

Add Record	
Index	2
Media Realm Name	MediaRealmWan
IPv4 Interface Name	WanInterface
IPv6 Interface Name	None
Port Range Start	7000
Number Of Media Session Legs	10
Port Range End	
Trans Rate Ratio	
Is Default	No
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

- Click **Submit** for each configuration.

**Notes:**

- IPv4 Interface Name** value string must be identical to the Interface Name string defined in the Multiple Interface table.
- Port Range End** field value is automatically calculated when you click **Submit**.

4.1.4 Step 4: Add SRDs for LAN and WAN

You need to add SRDs for the LAN and WAN interfaces:

➤ **To add SRDs:**

1. Open the SRD Settings page (**Configuration** tab > **VoIP** menu > **Control Network** > **SRD Table**).
2. Add an SRD to index 1 for the LAN interface:
 - **SRD Name:** SrdLan
 - **Media Realm:** MediaRealmLan

Figure 4-10: SRD for LAN Interface

SRD Index	1 - SrdLan
Common Parameters	
SRD Name	SrdLan
Media Realm	MediaRealmLan
SBC Parameters	

3. Add an SRD to index 2 for the WAN interface:
 - **SRD Name:** SrdWan
 - **Media Realm:** MediaRealmWan

Figure 4-11: SRD for WAN Interface

SRD Index	2 - SrdWan
Common Parameters	
SRD Name	SrdWan
Media Realm	MediaRealmWan
SBC Parameters	

4. Click **Submit** for each configuration.



Note: **Media Realm** value string must be identical to the **Media Realm Name** string defined in the Media Realm table.

4.1.5 Step 5: Add SIP Interfaces for LAN and WAN

You need to add SIP Interfaces for the LAN and WAN interfaces:

➤ **To add SIP Interfaces:**

1. Open the SIP Interface Table page (**Configuration** tab > **VoIP** menu > **Control Network** > **SIP Interface Table**).
2. Add a SIP Interface to index 1 for the LAN interface:
 - **Network Interface:** Voice
 - **Application Type:** SBC
 - **UDP / TCP / TLS Port:** 5060 / 5060 / 5061 respectively
 - **SRD:** 1
3. Add a SIP Interface to index 2 for the WAN interface:
 - **Network Interface:** WanInterface
 - **Application Type:** SBC
 - **UDP / TCP / TLS Port:** 5060 / 5060 / 5061 respectively
 - **SRD:** 2

Figure 4-12: SIP Interfaces for LAN and WAN Interfaces

Index	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	SRD	Message Policy
1	Voice	SBC	5060	5060	5061	1	None
2	WanInterface	SBC	5060	5060	5061	2	None

4. Click **Apply**.



Notes:

- **Network Interface** value string must be identical to the Interface Name string defined in the Multiple Interface table.
- **SRD** value must correspond to the SRD index that you configured for these logical interfaces.

4.1.6 Step 6: Add IP Groups for IP PBX and ITSP Servers

You need to add an IP Group for each of the following entities:

- WAN SIP Trunk (server-type IP Group)
- LAN IP PBX (server-type IP Group)
- Nomadic WAN Users (user-type IP Group)

➤ **To add IP Groups:**

1. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **Control Network** > **IP Group Table**).
2. Add an IP Group to index 1 for the LAN IP PBX:
 - **Type:** SERVER
 - **Description:** LAN IP PBX
 - **Proxy Set ID:** 1
 - **Classify By Proxy Set:** Enable

Figure 4-13: IP Group for LAN IP PBX

	Index	1
▼ Common Parameters		
→	Type	SERVER
→	Description	LAN IP PBX
→	Proxy Set ID	1
	SIP Group Name	
	Contact User	
	SRD	0
	Media Realm	
	IP Profile ID	0
▼ Gateway Parameters		
	Always Use Route Table	No
	Routing Mode	Not Configured
	SIP Re-Routing Mode	Standard
▼ SBC Parameters		
→	Classify By Proxy Set	Enable

3. Add an IP Group to index 2 for the WAN SIP Trunk:
 - **Type:** SERVER
 - **Description:** WAN SIP Trunk
 - **Proxy Set ID:** 2
 - **Classify By Proxy Set:** Enable

Figure 4-14: IP Group for WAN SIP Trunk

Index	2
Common Parameters	
Type	SERVER
Description	WAN SIP Trunk
Proxy Set ID	2
SIP Group Name	
Contact User	
SRD	0
Media Realm	
IP Profile ID	0
Gateway Parameters	
Always Use Route Table	No
Routing Mode	Not Configured
SIP Re-Routing Mode	Standard
SBC Parameters	
Classify By Proxy Set	Enable

4. Add an IP Group to index 3 for the nomadic WAN users:
 - **Type:** USER
 - **Description:** Nomadic Users
 - **SRD:** 2
 - **Classify By Proxy Set:** Disable

Figure 4-15: IP Group for WAN Nomadic Users

Index	3
Common Parameters	
Type	USER
Description	WAN Nomadic Users
Proxy Set ID	
SIP Group Name	
Contact User	N/A
SRD	2
Media Realm	
IP Profile ID	0
Gateway Parameters	
Always Use Route Table	No
Routing Mode	Not Configured
SIP Re-Routing Mode	Standard
SBC Parameters	
Classify By Proxy Set	Disable

5. Click **Submit** for each configuration.



Note: Normally, if far-end users (FEU) are located behind a NAT device and the NAT device does not change the IP address (from that of the FEU to the public IP address of the NAT device) in the SDP body of the outgoing SIP message, the RTP packets sent by the E-SBC would not be able to reach the FEU. To resolve this issue, you can configure the E-SBC to obtain the NAT device's public IP address from the first incoming RTP packet, enabling the E-SBC to send RTP packets to the public IP address of the NAT device. This is done by setting the *DisableNAT* parameter to 0 (Enabled).

4.1.7 Step 7: Add Proxy Sets for IP PBX and ITSP Servers

You need to add a Proxy Set for each of the following server-type entities:

- WAN SIP Trunk
- LAN IP PBX

➤ To add Proxy Sets:

1. Open the Proxy Sets Table page (**Configuration** tab > **VoIP** menu > **Control Network** > **Proxy Sets Table**).
2. Add a Proxy Set to index 1 for the LAN IP PBX:
 - **Proxy Address:** 10.33.6.100
 - **SRD Index:** 1

Figure 4-16: Proxy Set for LAN IP PBX

Proxy Set ID: 1

	Proxy Address	Transport Type
1	10.33.6.100	UDP
2		
3		
4		
5		

Enable Proxy Keep Alive: Disable
 Proxy Keep Alive Time: 60
 Proxy Load Balancing Method: Disable
 Is Proxy Hot Swap: No
 Proxy Redundancy Mode: Not Configured
 SRD Index: 1
 Classification Input: IP only

3. Add a Proxy Set to index 2 for the WAN SIP Trunk:

- **Proxy Address:** 212.199.200.10
- **SRD Index:** 2

Figure 4-17: Proxy Set for WAN SIP Trunk

Proxy Set ID: 2

	Proxy Address	Transport Type
1	212.199.200.10	UDP
2		
3		
4		
5		

Enable Proxy Keep Alive: Disable
 Proxy Keep Alive Time: 60
 Proxy Load Balancing Method: Disable
 Is Proxy Hot Swap: No
 Proxy Redundancy Mode: Not Configured
 SRD Index: 2
 Classification Input: IP only

4. Click **Submit** for each configuration, and then save your settings to flash memory ("burn") with a device reset.

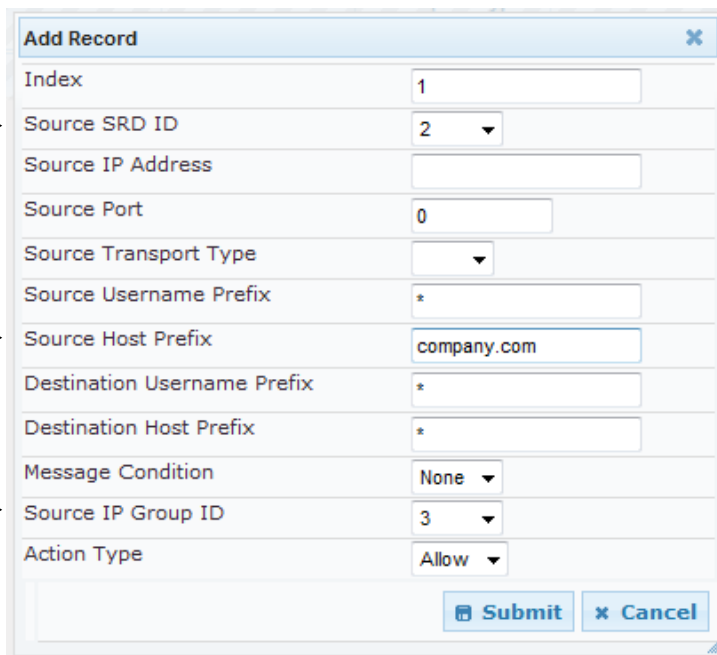
4.1.8 Step 8: Add Classification Rule for WAN Nomadic Users

For the E-SBC to identify calls from nomadic WAN users and to classify them to their IP Group, you need to add a classification rule. In the example scenario, calls received on the WAN interface (i.e., SRD 2) and with prefix host name, “company.com” will be identified as nomadic users and assigned to IP Group 3.

➤ **To add a classification rule for nomadic users:**

1. Open the Classification Table page (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **Classification Table**).
2. Add a classification rule to index 1:
 - **Source SRD:** 2
 - **Source Host Prefix:** company.com
 - **Source IP Group ID:** 3

Figure 4-18: Classification Rule for WAN Nomadic Users



Add Record	
Index	1
Source SRD ID	2
Source IP Address	
Source Port	0
Source Transport Type	
Source Username Prefix	*
Source Host Prefix	company.com
Destination Username Prefix	*
Destination Host Prefix	*
Message Condition	None
Source IP Group ID	3
Action Type	Allow
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

3. Click **Submit**.

4.1.9 Step 9: Add IP-to-IP Call Routing Rules

You need to add IP-to-IP routing rules for the following routing directions:

- Calls from the WAN SIP Trunk to the LAN IP PBX.
- Calls from the WAN nomadic users to the LAN IP PBX.
- Calls from the LAN IP PBX to the WAN nomadic users. As the WAN nomadic users in this example have a 5-digit extension number starting with the number 4, numbers dialed from the IP PBX with this prefix will be routed to the WAN users, while all other dialed numbers from the IP PBX will be routed to the SIP Trunk.
- Calls from the LAN IP PBX to the WAN SIP Trunk.

The call routing rules use the IP Groups of these entities to denote the source and destination of the route.

➤ **To add IP-to-IP call routing rules:**

1. Open the IP2IP Routing Table page (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **IP to IP Routing Table**).
2. Add a rule to row index 1 to route calls from the WAN SIP Trunk to the LAN IP PBX:
 - **Source IP Group ID:** 2
 - **Destination Type:** IP Group
 - **Destination IP Group ID:** 1
3. Add a rule to row index 2 to route calls from the WAN nomadic users to the LAN IP PBX:
 - **Source IP Group ID:** 3
 - **Destination Type:** IP Group
 - **Destination IP Group ID:** 1
4. Add a rule to row index 3 to route calls from the LAN IP PBX to the WAN users. As mentioned previously, this rule is for calls dialed to a 5-digit extension number with prefix 4:
 - **Source IP Group ID:** 1
 - **Destination Username Prefix:** 4xxxx#
 - **Destination Type:** IP Group
 - **Destination IP Group ID:** 3
5. Add a rule to row index 4 to route calls from the LAN IP PBX to the WAN SIP Trunk:
 - **Source IP Group ID:** 1
 - **Destination Type:** IP Group
 - **Destination IP Group ID:** 2

Figure 4-19: IP-to-IP Call Routing Rules

Index	Source IP Group ID	Destination Username Prefix	Destination Host	Request Type	Destination Type	Destination IP Group ID	Destination SRD ID	Destination Address	Destination Port	Alternative Route Options
1	2	*	*	All	IP Group	1	None		0	Route Row
2	3	*	*	All	IP Group	1	None		0	Route Row
3	1	4xxxx#	*	All	IP Group	3	None		0	Route Row
4	1	*	*	All	IP Group	2	None		0	Route Row

6. Click **Submit** after each configuration.



Note: **Destination Username Prefix** value "4xxxx#" denotes a 5-digit number starting with 4. For more information on using notations to represent entered values, refer to the *User's Manual*.

4.1.10 Step 10: Reset E-SBC and Verify Configuration in Syslog

Once you have completed the previous configuration steps, you must reset the E-SBC with a flash burn for your settings take effect, and then use Syslog to check the messages received at device startup.

Ensure that there are no configuration errors related to SRDs, Media Realms, or SIP interfaces.

The Syslog message below shows an example of an error indicating that the Media Realm name ("MediaRealmLa") is invalid. This could be caused by incorrect spelling of the configured Media Realm in the SRD table.

```
( lgr_psbrdif)(3 ) !! [ERROR]
PSOSBoardInterface::TranslateRealmName failed since MediaRealm
name(MediaRealmLa) is INVALID
```

4.1.11 Alternative Routing upon SIP Trunk Failure

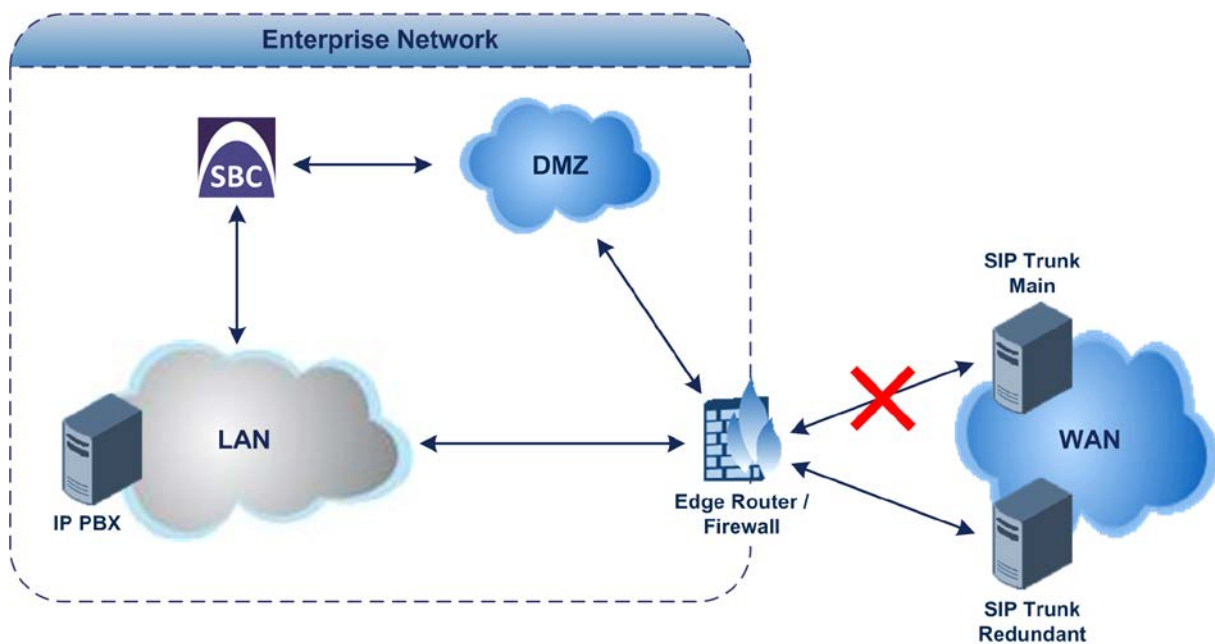
This section describes the configuration of the following optional, call survivability solutions that can be implemented upon connectivity failure with the SIP Trunk:

- PSTN Fallback, whereby external calls from the LAN IP PBX are routed to the PSTN
- SIP Trunk redundancy, whereby external calls from the LAN IP PBX are routed to a redundant SIP trunk

4.1.11.1 SIP Trunk Redundancy

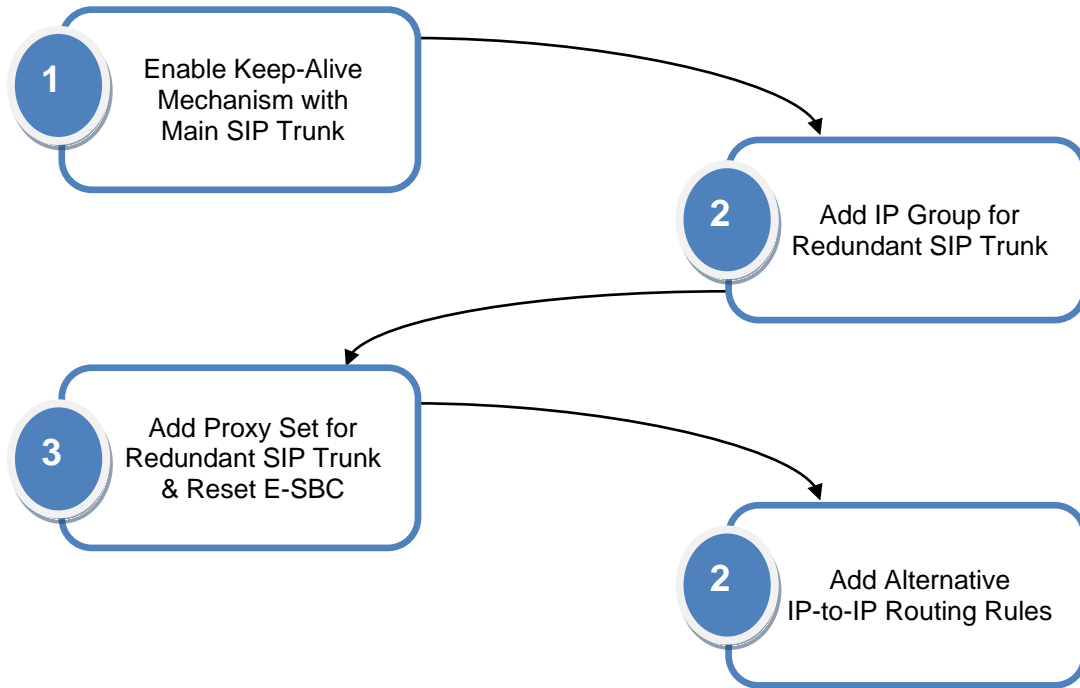
This section provides step-by-step procedures on how to configure SIP trunk redundancy. It assumes that the redundant SIP trunk is at IP address 212.199.200.12. The figure below illustrates this setup example.

Figure 4-20: SIP Trunk Redundancy Example Scenario



The configuration steps for this example scenario are summarized in the flowchart below.

Figure 4-21: Flowchart for Configuring SIP Trunk Redundancy



4.1.11.1 Step 1: Enable Keep-Alive for Main SIP Trunk

In order to detect connectivity failure with the main SIP Trunk, you need to enable the keep-alive mechanism with the main SIP Trunk.

➤ **To enable keep-alive mechanism with the main SIP Trunk:**

1. Open the Proxy Sets Table page (**Configuration** tab > **VoIP** menu > **Control Network** > **Proxy Sets Table**).
2. Select index 2 (i.e., the Proxy Set of the main SIP Trunk), and then set the following:
 - **Enable Proxy Keep Alive:** Using Options

Figure 4-22: Enabling Keep-Alive with Main SIP Trunk

Proxy Set ID		2	
	Proxy Address	Transport Type	
1	212.199.200.10	UDP	
2			
3			
4			
5			

Enable Proxy Keep Alive	Using Options
Proxy Keep Alive Time	60
Proxy Load Balancing Method	Disable
Is Proxy Hot Swap	No
Proxy Redundancy Mode	Not Configured
SRD Index	2
Classification Input	IP only

3. Click **Submit**.

4.1.11.1.2 Step 2: Add IP Group for Redundant SIP Trunk

You need to add an IP Group for the redundant SIP Trunk.

➤ **To add an IP Group for the redundant SIP Trunk:**

1. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **Control Network** > **IP Group Table**).
2. Add an IP Group to index 4 for the redundant SIP Trunk:
 - **Type:** SERVER
 - **Description:** Redundant SIP Trunk
 - **Proxy Set ID:** 4
 - **Classify By Proxy Set:** Enable

Figure 4-23: IP Group for Redundant SIP Trunk

Index	4
▼ Common Parameters	
Type	SERVER
Description	Redundant SIP Trunk
Proxy Set ID	4
SIP Group Name	
Contact User	
Domain Name in Contact	
SRD	0
Media Realm	
IP Profile ID	0
▼ Gateway Parameters	
Always Use Route Table	No
Routing Mode	Not Configured
SIP Re-Routing Mode	Standard
Enable Survivability	Disable
Serving IP Group ID	-1
▼ SBC Parameters	
Classify By Proxy Set	Enable

3. Click **Submit**.

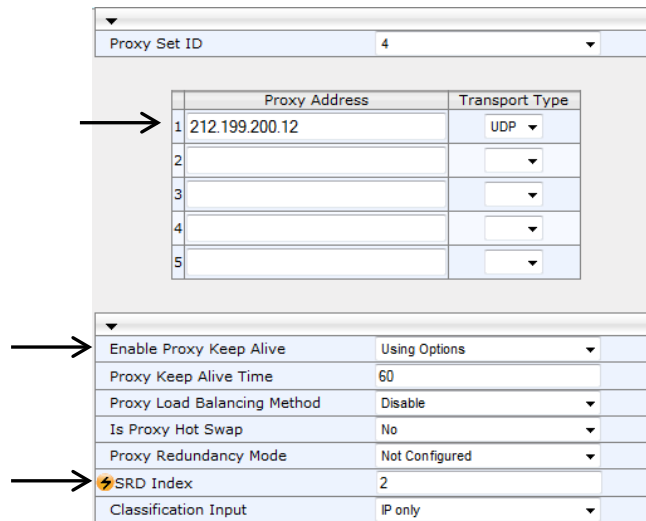
4.1.11.1.3 Step 3: Add Proxy Set for Redundant SIP Trunk

You need to add a Proxy Set for the redundant SIP Trunk.

➤ **To add a Proxy Set:**

1. Open the Proxy Sets Table page (**Configuration** tab > **VoIP** menu > **Control Network** > **Proxy Sets Table**).
2. Add a Proxy Set to index 4 for the redundant SIP Trunk:
 - **Proxy Address:** 212.199.200.12
 - **Enable Proxy Keep Alive:** Using Options
 - **SRD Index:** 2

Figure 4-24: Proxy Set for Redundant SIP Trunk



Proxy Set ID		4
Proxy Address		Transport Type
1	212.199.200.12	UDP
2		
3		
4		
5		
Enable Proxy Keep Alive		Using Options
Proxy Keep Alive Time		60
Proxy Load Balancing Method		Disable
Is Proxy Hot Swap		No
Proxy Redundancy Mode		Not Configured
SRD Index		2
Classification Input		IP only

3. Click **Submit**, and then save your settings to flash memory ("burn") with a device reset.



Note: As the redundant SIP Trunk is located in the same VoIP network as the main SIP Trunk, it uses the same SRD.

4.1.11.1.4 Step 4: Add Alternative IP-to-IP Call Routing Rules for Redundant SIP Trunk

You need to add IP-to-IP routing rules for the following routing directions:

- Calls from LAN IP PBX to redundant SIP Trunk upon failure of main SIP Trunk. This is considered an alternative routing rule and therefore, you **must** add it to the row index located immediately below the row of the LAN IP PBX to main SIP Trunk rule.
- Calls from the redundant SIP Trunk to LAN IP PBX.

➤ **To add IP-to-IP alternative call routing rules:**

1. Open the IP2IP Routing Table page (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **IP to IP Routing Table**).
2. Add a rule to row index 5 to route calls from the LAN IP PBX to the redundant SIP Trunk:
 - **Source IP Group ID:** 1
 - **Destination Type:** IP Group
 - **Destination IP Group ID:** 4
 - **Alternative Route Options:** Alt Route Consider Inputs
3. Add a rule to row index 6 to route calls from the redundant SIP Trunk to the LAN IP PBX:
 - **Source IP Group ID:** 4
 - **Destination Type:** IP Group
 - **Destination IP Group ID:** 1

Figure 4-25: IP-to-IP Call Routing Rules for Redundant SIP Trunk

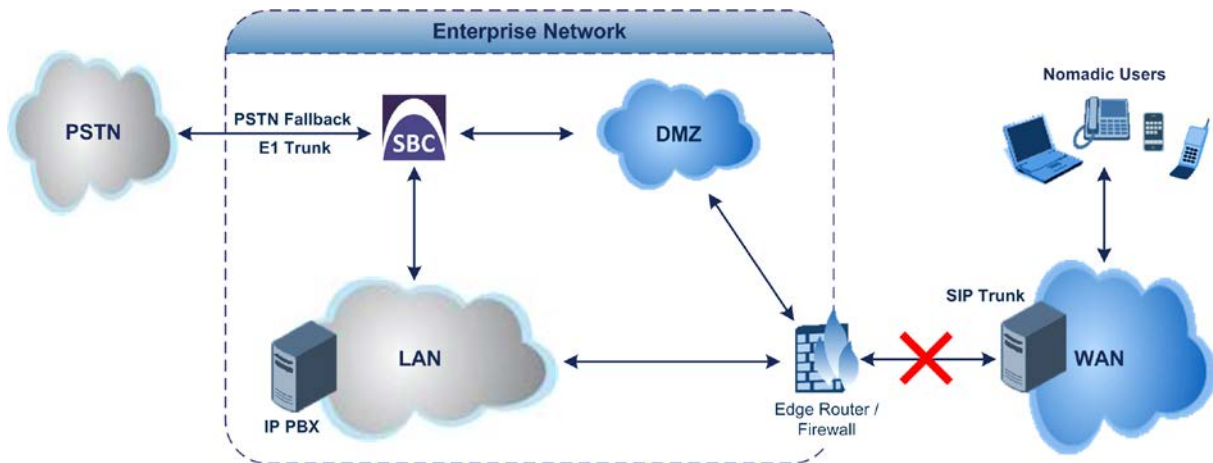
Index	Source IP Group ID	Destination Username Prefix	Destination Host	Request Type	Destination Type	Destination IP Group ID	Destination SRD ID	Destination Address	Destination Port	Alternative Route Options
1	2	*	*	All	IP Group	1	None		0	Route Row
2	3	*	*	All	IP Group	1	None		0	Route Row
3	1	4xxxx#	*	All	IP Group	3	None		0	Route Row
4	1	*	*	All	IP Group	2	None		0	Route Row
5	1	*	*	All	IP Group	4	None		0	Alt Route Co
6	4	*	*	All	IP Group	1	None		0	Route Row

4. Click **Submit** after each configuration.

4.1.11.2 Setting up PSTN Fallback

This section describes how to configure PSTN fallback. It assumes that the E-SBC provides an E1 trunk connection with the local PSTN. The figure below illustrates this setup example.

Figure 4-26: PSTN Fallback Example Scenario



Upon SIP Trunk connectivity failure, the E-SBC's PSTN Fallback feature routes external calls from the LAN IP PBX to the PSTN (instead of to the WAN SIP Trunk). The E-SBC uses a keep-alive mechanism to check connectivity with the SIP Trunk. When it detects a failure, it routes the SIP messages from the IP PBX to the IP Group of the PSTN Gateway ("GW") application, instead of to the WAN SIP Trunk IP Group.

For routing between the LAN IP PBX and PSTN, you can either use the Gateway's IP address:port, or use an IP Group to represent the Gateway (i.e., GW application). The latter method is recommended. Implementing IP Groups facilitates configuration of routing rules in both directions (i.e., IP PBX to PSTN, and PSTN to IP PBX), and provides flexibility in assigning unique call handling (behaviors) using IP Profiles.

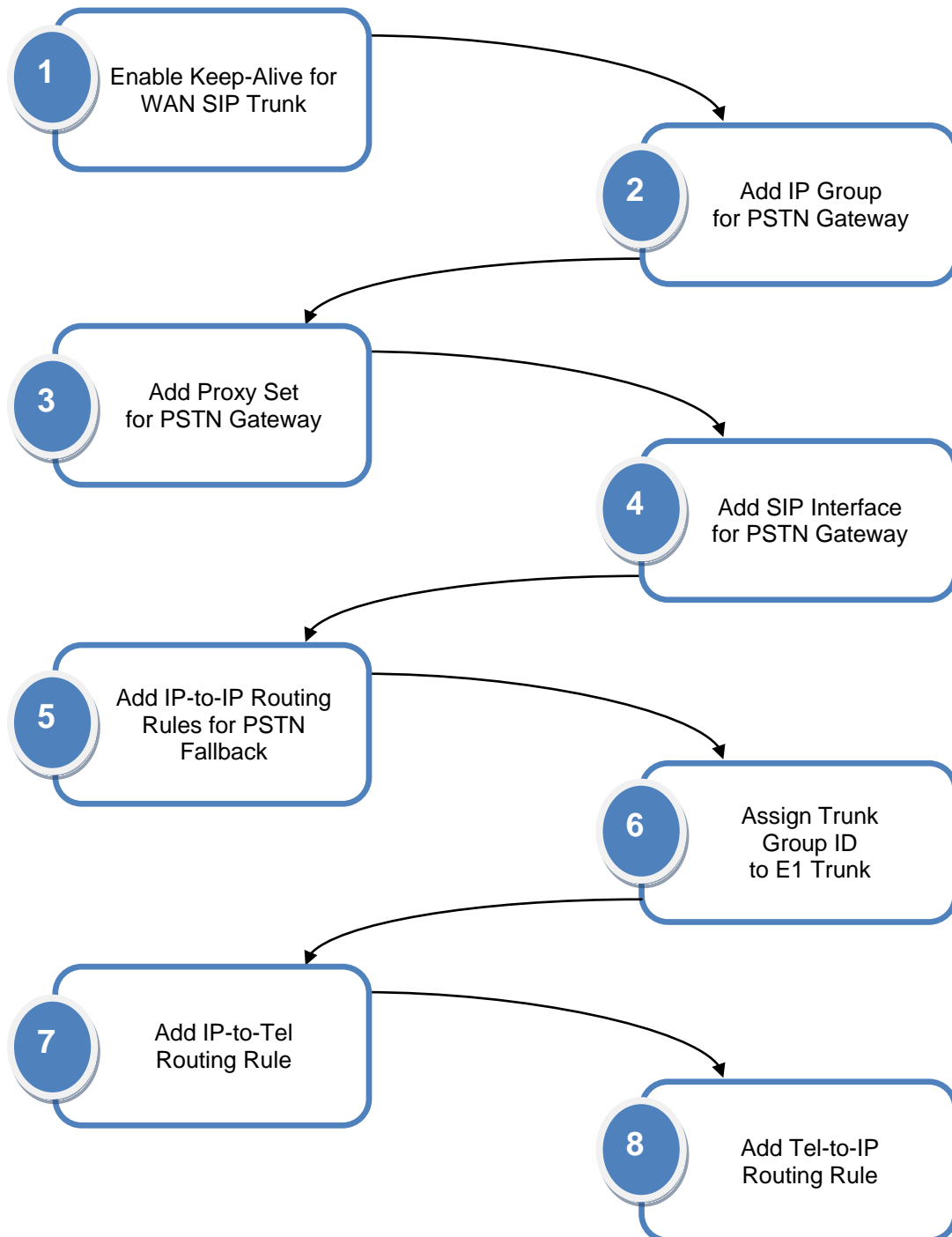
Notes:

- PSTN Fallback is applicable only to the following E-SBC products:
 - Mediant 800 MSBG
 - Mediant 800 Gateway & SBC
 - Mediant 1000 MSBG
 - Mediant 1000 Gateway & SBC
 - Mediant 3000
- For PSTN Fallback support your device must have a PSTN interface (PRI, BRI, or FXO). If not, contact your AudioCodes distributor for more information.



The configuration steps for this example scenario are summarized in the flowchart below:

Figure 4-27: Flowchart for Configuring PSTN Fallback

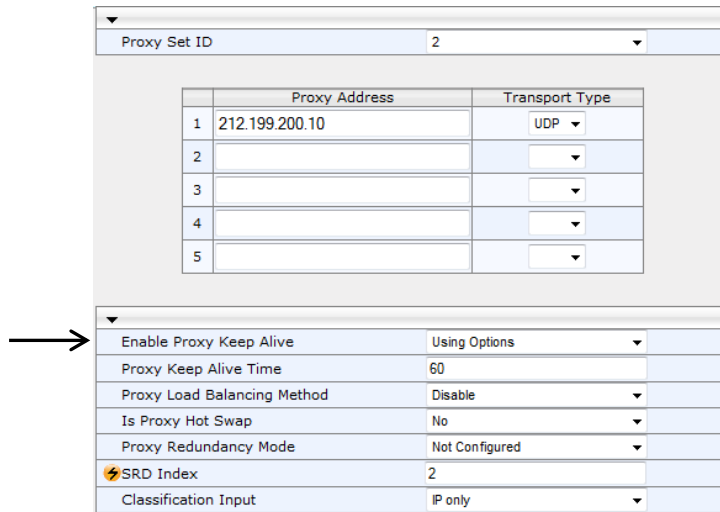


4.1.11.2.1 Step 1: Enable Keep-Alive for SIP Trunk

The E-SBC performs PSTN fallback upon a WAN failure or more specifically, when it detects an IP connectivity failure with the WAN SIP Trunk (ITSP). Therefore, you need to enable E-SBC to periodically check connectivity with this entity. To do so, you need to enable a keep-alive mechanism whereby the E-SBC periodically sends SIP OPTIONS messages to this entity.

- **To enable keep-alive mechanism with the WAN ITSP:**
- 1. Open the Proxy Sets Table page (**Configuration** tab > **VoIP** menu > **Control Network** > **Proxy Sets Table**).
- 2. Select index 2 (i.e., the Proxy Set of the WAN SIP Trunk), and then set the following:
 - **Enable Proxy Keep Alive:** Using Options

Figure 4-28: Enabling Keep-Alive for WAN SIP Trunk



Proxy Set ID		2	
Proxy Address			
Transport Type			
1	212.199.200.10	UDP	▼
2			▼
3			▼
4			▼
5			▼
▼			
Enable Proxy Keep Alive	Using Options		▼
Proxy Keep Alive Time	60		
Proxy Load Balancing Method	Disable		▼
Is Proxy Hot Swap	No		▼
Proxy Redundancy Mode	Not Configured		▼
SRD Index	2		
Classification Input	IP only		▼

- 3. Click **Submit**.

4.1.11.2.2 Step 2: Add IP Group for PSTN Gateway

You need to add an IP Group for the PSTN Gateway.

➤ **To add an IP Group for the PSTN Gateway:**

1. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **Control Network** > **IP Group Table**).
2. Add an IP Group to index 5 for the PSTN Gateway:
 - **Type:** SERVER
 - **Description:** PSTN Gateway
 - **Proxy Set ID:** 5
 - **Classify By Proxy Set:** Enable

Figure 4-29: IP Group for PSTN Gateway

Index	5
Common Parameters	
Type	SERVER
Description	PSTN Gateway
Proxy Set ID	5
SIP Group Name	
Contact User	
Domain Name in Contact	
SRD	0
Media Realm	
IP Profile ID	0
Gateway Parameters	
Always Use Route Table	No
Routing Mode	Not Configured
SIP Re-Routing Mode	Standard
SBC Parameters	
Classify By Proxy Set	Enable

3. Click **Submit**.

4.1.11.2.3 Step 3: Add Proxy Set for PSTN Gateway

You need to add a Proxy Set for the PSTN Gateway. The proxy address is the destination to where the E-SBC sends the SIP messages. This destination is the IP address of the LAN Voice interface - 10.33.4.176 - and the port of the PSTN Gateway application – 5070 – which will be defined in the SIP Interface table (see Section 4.1.11.2.4).

➤ **To add a Proxy Set for the PSTN Gateway:**

1. Open the Proxy Sets Table page (**Configuration** tab > **VoIP** menu > **Control Network** > **Proxy Sets Table**).
2. Add a Proxy Set to index 5:
 - **Proxy Address:** 10.33.4.176:5070
 - **SRD Index:** 1

Figure 4-30: Proxy Set for PSTN Gateway

Proxy Address	Transport Type
1 10.33.4.176:5070	UDP
2	
3	
4	
5	

Enable Proxy Keep Alive	Disable
Proxy Keep Alive Time	60
Proxy Load Balancing Method	Disable
Is Proxy Hot Swap	No
Proxy Redundancy Mode	Not Configured
SRD Index	1
Classification Input	IP only

3. Click **Submit**, and then save your settings to flash memory ("burn") with a device reset.

4.1.11.2.4 Step 4: Add a SIP Interface for PSTN Gateway

You need to create a SIP interface for the PSTN Gateway. This SIP interface is used for the listening port of SIP messages destined to the PSTN Gateway application.

➤ **To add a SIP Interface for PSTN Gateway:**

1. Open the SIP Interface Table page (**Configuration** tab > **VoIP** menu > **Control Network** > **SIP Interface Table**).
2. Add a SIP Interface to index 3 for the LAN interface:
 - **Network Interface:** Voice
 - **Application Type:** GW/IP2IP
 - **UDP / TCP / TLS Port:** 5070 / 5070 / 5071 respectively
 - **SRD:** 1

Figure 4-31: SIP Interface for PSTN Fallback Calls

Index	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	SRD	Message Policy
1	Voice	SBC	5060	5060	5061	1	None
2	WanInterface	SBC	5060	5060	5061	2	None
3	Voice	GW/IP2IP	5070	5070	5071	1	None

3. Click **Apply**.



Notes:

- As the SIP interface is used in the LAN VoIP network, it is assigned to SRD 1.
- **Network Interface** value string must be identical to the Interface Name string defined in the Multiple Interface table.

4.1.11.2.5 Step 5: Add IP-to-IP Call Routing Rules for PSTN Fallback Calls

You need to add IP-to-IP routing rules for PSTN Fallback for the following routing directions:

- Calls from the LAN IP PBX to PSTN Gateway, used upon SIP Trunk failure. This is considered an alternative routing rule and therefore, you **must** add it to the row index located immediately below the LAN IP PBX to main SIP Trunk routing rule entry.
- Calls from the PSTN Gateway to the LAN IP PBX.

➤ **To add an IP-to-IP call routing rule for PSTN Fallback:**

1. Open the IP2IP Routing Table page (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **IP to IP Routing Table**).
2. Add a rule to index 7 to route calls from the LAN IP PBX to the PSTN Gateway:
 - **Source IP Group ID:** 1
 - **Destination Type:** IP Group
 - **Destination IP Group ID:** 5
 - **Alternative Route Options:** Alt Route Consider Inputs
3. Add a rule to index 8 to route calls from the PSTN Gateway to LAN IP PBX:
 - **Source IP Group ID:** 5
 - **Destination Type:** IP Group
 - **Destination IP Group ID:** 1

Figure 4-32: IP-to-IP Call Routing Rule for PSTN Fallback

Index	Source IP Group ID	Destination Username	Destination Host	Request Type	Destination Type	Destination IP Group ID	Destination SRD ID	Destination Address	Destination Port	Alternative Route Options
1	2	*	*	All	IP Group	1	None		0	Route Row
2	3	*	*	All	IP Group	1	None		0	Route Row
3	1	4xxxxx#	*	All	IP Group	3	None		0	Route Row
4	1	*	*	All	IP Group	2	None		0	Route Row
7	1	*	*	All	IP Group	5	None		0	Alt Route Ig
8	5	*	*	All	IP Group	1	None		0	Route Row

4. Click **Submit**.

4.1.11.2.6 Step 6: Assign a Trunk Group for the E1 Trunk

A *Trunk Group* is a logical group of trunks (spans) and channels pertaining to these trunks. This example scenario employs an E1 trunk to connect the E-SBC to the PSTN.

➤ **To set up a Trunk Group:**

1. Configure E1 protocol settings for the trunk in the Trunk Settings page (**Configuration** tab > **VoIP** menu > **PSTN** > **Trunk Settings**). Trunk protocol configuration is not in the scope of this document. For more information, refer to the *User's Manual*.
2. Assign a Trunk Group ID to the E1 trunk:
 - a. Open the Trunk Group Table page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **Trunk Group** > **Trunk Group**).
 - b. For row index 1, set the following:
 - ◆ **Module:** Module 1 PRI
 - ◆ **From Trunk:** 1
 - ◆ **To Trunk:** 1
 - ◆ **Channels:** 1-30
 - ◆ **Phone Number:** 6000
 - ◆ **Trunk Group ID:** 2

Figure 4-33: Assigning Trunk Group ID to E1 Trunk

Group Index	Module	From Trunk	To Trunk	Channels	Phone Number	Trunk Group ID	Tel Profile ID
1	Module 1 PRI	1	1	1-30	6000	2	0



Notes:

- **Module** is applicable only to the following E-SBC products:
 - Mediant 800 MSBG
 - Mediant 800 Gateway & SBC
 - Mediant 1000 MSBG
 - Mediant 1000 Gateway & SBC
- **Phone Number** is only a logical value for enabling the Trunk Group and thus, can be any numerical value.

3. Click **Submit**.

4.1.11.2.7 Step 7: Add IP to Trunk Group Routing Rule

You need to define an IP-to-Trunk Group routing rule to route calls destined to the PSTN Gateway application to the Trunk Group of the E1 trunk.

➤ **To add an IP-to-Trunk Group call routing rule:**

1. Open the Inbound IP Routing Table page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **Routing** > **IP to Trunk Group Routing**).
2. Add a rule to row index 1:
 - **Dest. Phone Prefix:** * (indicates all)
 - **Trunk Group ID:** 2

Figure 4-34: IP-to-Trunk Group Call Routing Rule

	Dest. Host Prefix	Source Host Prefix	Dest. Phone Prefix	Source Phone Prefix	Source IP Address	Trunk Group ID	IP Profile ID	Source IP Group ID
→ 1			*			2	0	-1

3. Click **Submit**.

4.1.11.2.8 Step 8: Add Tel-to-IP Routing Rule

In order to receive calls from the PSTN, you need to add a rule to route calls from the PSTN Trunk Group to the SBC application

➤ **To add a Trunk-to-IP routing rule for PSTN fallback:**

1. Open the Outbound IP Routing Table page (**Configuration** tab > **VoIP** menu > **GW and IP to IP** > **Routing** > **Tel to IP Routing**).
2. Add a rule to row index 1:
 - **Src. Trunk Group ID:** 2
 - **Dest. IP Address:** 10.33.4.176:5060

Figure 4-35: Trunk-to-IP Call Routing Rule

	Src. Trunk Group ID	Dest. Phone Prefix	Source Phone Prefix	Dest. IP Address	Port	Transport Type
→ 2		*	*	10.33.4.176	5060	Not Configured ▼

3. Click **Submit**.

4.2 Hosted IP PBX

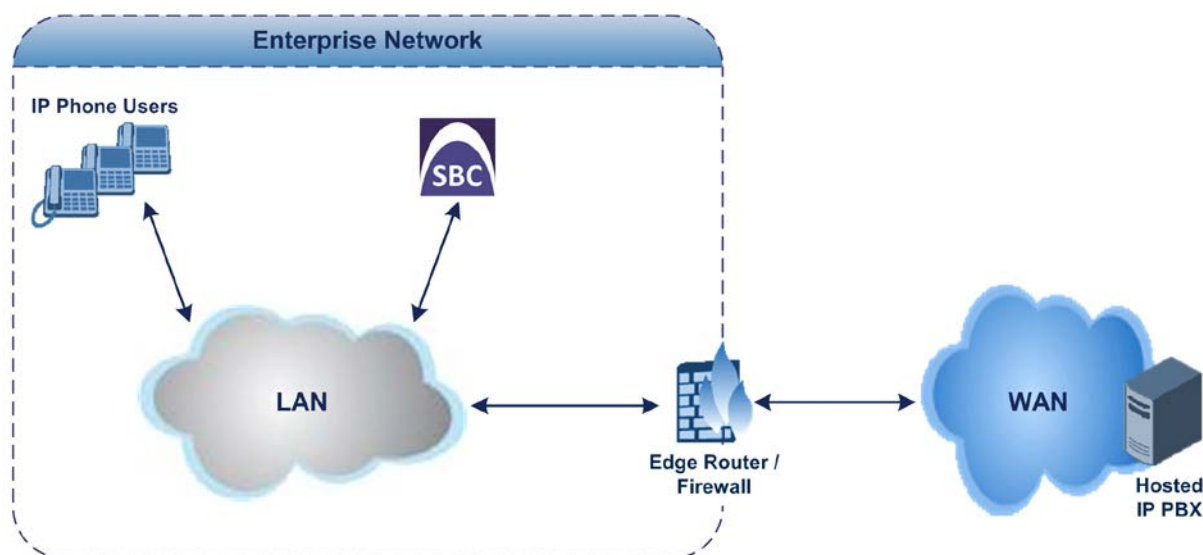
This example scenario includes the following topology architecture:

■ **Application:**

- Enterprise LAN IP Phone users, located behind NAT.
- Hosted WAN IP PBX at IP address, 212.199.200.10.
- Call Survivability in case of hosted IP PBX failure (e.g., WAN disconnection), whereby the E-SBC maintains call routing between the LAN users, by using its User Registration database. During normal operation, LAN users register with the hosted IP PBX and the E-SBC updates these registrations in its registration database. If PSTN connectivity is required during IP PBX failure, you can also setup PSTN Fallback as described in the previous example (see Section 4.1.11.2).

The figure below illustrates the application of this example scenario:

Figure 4-36: Hosted IP PBX Example - Application Topology



■ **Topology:**

• **E-SBC Logical Network Interface Connection:**

This example employs one logical network interface using IP address 10.33.4.176. This interface is used for communicating with the LAN and WAN. Two SRDs are required to resolve NAT traversal. As the E-SBC uses only one logical interface, it separates the traffic between the LAN and WAN using different logical ports defined by each SRD. The IP phones communicate with the E-SBC using port 5060 and the edge router will forward the messages from the hosted IP PBX to the E-SBC using port 5070.

• **NAT Traversal:**

When the E-SBC sends messages to the hosted IP PBX, it uses the public IP address of the edge router (instead of 10.33.4.176).



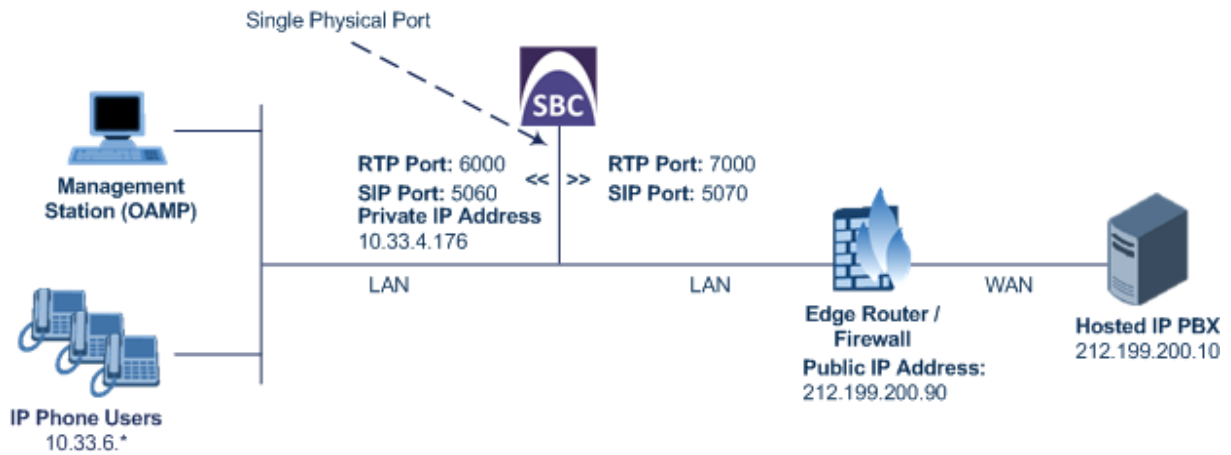
Note: You must configure port forwarding on the edge router to forward messages from the WAN to the E-SBC. Based on this example scenario, for SIP messages you need to set the SIP interface port to 5070.

- **E-SBC Physical LAN Port Connections:**

The E-SBC is connected through a single LAN port to the Enterprise LAN.

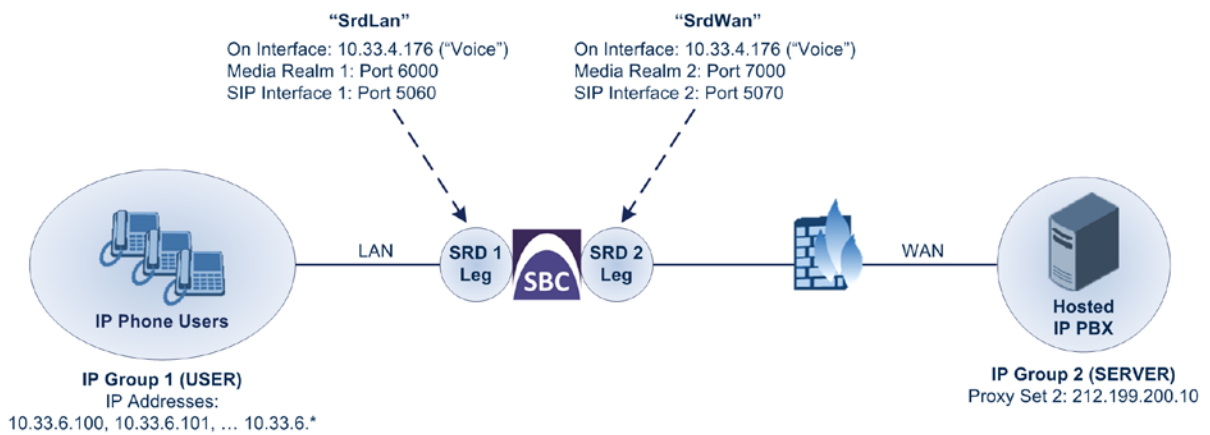
The figure below illustrates the E-SBC logical network interfaces and LAN port connection of this example scenario:

Figure 4-37: E-SBC Logical Interfaces and Physical Port Connection Example



The main configuration entities used in this example are shown below:

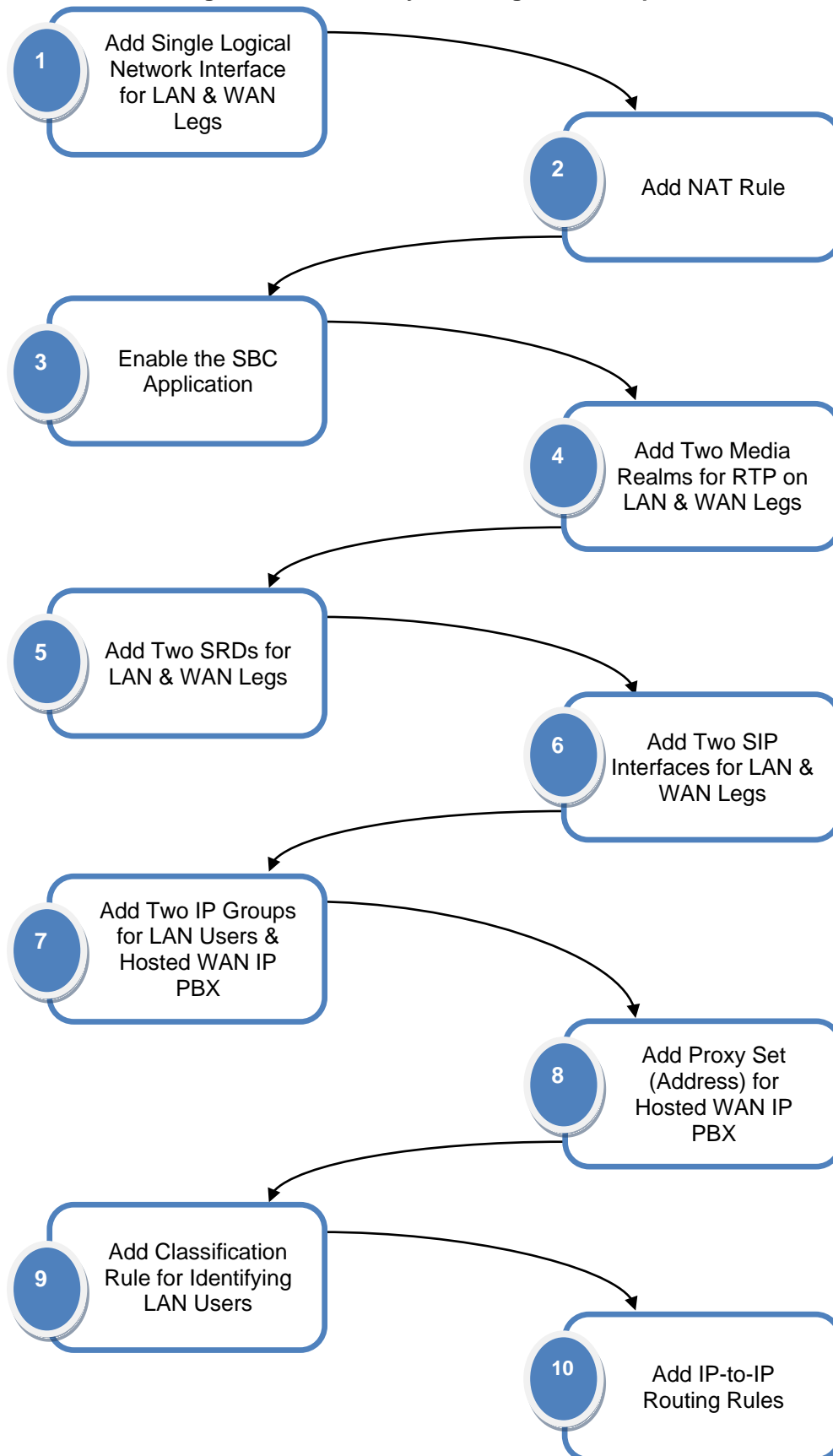
Figure 4-38: Required Configuration Entities



Note: For clarity, whenever configuring the various entities in this example (e.g., SRDs, Media Realms, SIP Interfaces, and IP Groups), table row index 1 is used for the E-SBC logical network interfacing with the LAN users; table row index 2 is used for the E-SBC logical network interfacing with the hosted WAN IP PBX.

The configuration steps for the example scenario are summarized in the flowchart below:

Figure 4-39: Summary of Configuration Steps



4.2.1 Step 1: Add a Logical IP Network Interface for LAN and WAN

As this example employs only one logical network interface (10.33.4.176) for the LAN and WAN and this same interface is also used for management (i.e., OAMP) which is already set up, additional configuration is unnecessary.

Figure 4-40: Logical IP Network Interface for LAN and WAN

Index	Application Type	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name	Primary DNS Server IP Address	Secondary DNS Server IP Address	Underlying Interface
0	OAMP + Media + Control	10.33.4.176	16	10.33.0.1	1	Voice	0.0.0.0	0.0.0.0	GROUP_1

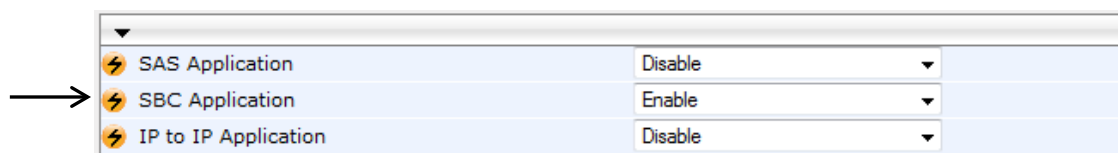
4.2.2 Step 2: Enable the SBC Application

For the E-SBC to operate as an SBC, you need to enable the SBC application. Once enabled, the SBC-specific parameters and pages become available in the Web interface.

➤ **To enable the SBC application:**

1. Open the Applications Enabling page (**Configuration** tab > **VoIP** menu > **Applications Enabling** > **Applications Enabling**).
2. From the 'SBC Application' drop-down list, select **Enable**.

Figure 4-41: Enabling the SBC Application



3. Click **Submit** to apply the changes.
4. Save your setting to flash memory ("burn") with a device reset.

4.2.3 Step 3: Add Media Realms for LAN and WAN

Add two Media Realms – one will be used for the LAN SRD and one for the WAN SRD.

➤ **To add Media Realms:**

1. Open the Media Realm Table page (**Configuration** tab > **VoIP** menu > **Media** > **Media Realm Configuration**).
2. Add a Media Realm to index 1 for the LAN interface:
 - **Media Realm Name:** MediaRealmLan
 - **IPv4 Interface Name:** Voice
 - **Port Range Start:** 6000
 - **Number of Media Session Legs:** 10

Figure 4-42: Media Realm for LAN Interface

Index	1
Media Realm Name	MediaRealmLan
IPv4 Interface Name	Voice
IPv6 Interface Name	None
Port Range Start	6000
Number Of Media Session Legs	10
Port Range End	
Trans Rate Ratio	
Is Default	No

3. Add a Media Realm to row index 2 for the WAN IP PBX interface:
 - **Media Realm Name:** MediaRealmWan
 - **IPv4 Interface Name:** Voice
 - **Port Range Start:** 7000
 - **Number of Media Session Legs:** 10

Figure 4-43: Media Realm for WAN Interface

Index	2
Media Realm Name	MediaRealmWan
IPv4 Interface Name	Voice
IPv6 Interface Name	None
Port Range Start	7000
Number Of Media Session Legs	10
Port Range End	
Trans Rate Ratio	
Is Default	No

4. Click **Submit** for each configuration.
5. Save your setting to flash memory ("burn") with a device reset.



Notes:

- **IPv4 Interface Name** value string must be identical to the Interface Name string defined in the Multiple Interface table.
- **Port Range End** field value is automatically calculated when you click **Submit**. For example, the first session uses port 6000; the second session uses port 6010, and so on.

4.2.4 Step 4: Add SRDs for LAN and WAN

The example scenario uses two SRDs on the single, logical LAN interface. Two SRDs are used to overcome NAT traversal, as explained in Section 3.3.

As the E-SBC uses only one logical interface, it separates the traffic between the LAN and WAN using different logical ports defined by each SRD. The IP phones communicate with the E-SBC using port 5060 and the edge router will forward the messages from the hosted IP PBX to the E-SBC using port 5070.



Notes: As the LAN users reside on the same LAN network, to reduce bandwidth usage, the media (RTP) path can be enabled to flow directly between the two call parties without traversing the E-SBC. In this setup, only the SIP signaling traverses the E-SBC to the WAN IP PBX. This is referred to as *anti-tromboning*.

➤ To add SRDs:

1. Open the SRD Settings page (**Configuration** tab > **VoIP** menu > **Control Network** > **SRD Table**).
2. Add an SRD to index 1 for the LAN users interface:
 - **SRD Name:** SrdLan
 - **Media Realm:** MediaRealmLan
 - **Internal SRD Media Anchoring:** Don't Anchor Media Anchoring

Figure 4-44: SRD for LAN Interface

SRD Index	1 - SrdLan
Common Parameters	
SRD Name	SrdLan
Media Realm	MediaRealmLan
SBC Parameters	
Internal SRD Media Anchoring	Don't Anchor Media
Block Unregistered Users	No
Max Number Of Registered Users	-1
Enable Un-Authenticated Registrations	Yes

3. Add an SRD to index 2 for the hosted IP PBX interface:
 - **SRD Name:** SrdWan
 - **Media Realm:** MediaRealmWan

Figure 4-45: SRD for WAN Interface

SRD Index	2 - SrdWan
Common Parameters	
SRD Name	SrdWan
Media Realm	MediaRealmWan
SBC Parameters	

4. Click **Submit** for each configuration.



Note: **Media Realm** value string must be identical to the **Media Realm Name** string defined in the Media Realm table.

4.2.5 Step 5: Add SIP Interfaces for LAN and WAN

Add two SIP Interfaces – one will be used for the LAN SRD and one for the WAN SRD.

➤ **To add SIP Interfaces:**

1. Open the SIP Interface Table page (**Configuration** tab > **VoIP** menu > **Control Network** > **SIP Interface Table**).
2. Add a SIP Interface to index 1 for the LAN interface:
 - **Network Interface:** Voice
 - **Application Type:** SBC
 - **UDP / TCP / TLS Port:** 5060 / 5060 / 5061
 - **SRD:** 1
3. Add a SIP Interface to index 2 for the WAN interface:
 - **Network Interface:** Voice
 - **Application Type:** SBC
 - **UDP / TCP / TLS Port:** 5070 / 5070 / 5071
 - **SRD:** 2

Figure 4-46: SIP Interfaces for LAN and WAN Interfaces

Index	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	SRD	Message Policy
1	Voice	SBC	5060	5060	5061	1	None
2	Voice	SBC	5070	5070	5071	2	None

4. Click **Apply** for each configuration.

4.2.6 Step 6: Configure a NAT Translation Rule

As the E-SBC is located behind NAT, you need to configure it for NAT traversal. The E-SBC NAT traversal mechanism replaces the source IP address of SIP messages sent from its WAN SRD to a public IP address.

When the E-SBC is configured with two network interfaces (e.g., one LAN and one WAN), only one NAT rule is required and without specifying ports. This rule is defined with only the network interface representing the WAN, and with a public IP address.

As this example uses only one network interface (e.g., "Voice"), you need to specify ports in order to differentiate between the SRDs (WAN and LAN). Thus, the E-SBC will only replace the source IP address for messages sent from the WAN SRD (e.g., 2) and not from the LAN SRD.

You need to add the following NAT rules for SIP messages:

- NAT rule for SIP messages with source port 5070 (defined for the WAN SIP interface in Section 4.2.5)
- NAT rule for SIP messages with SDP source port 7000-7090 (defined for the WAN Media Realm in Section 4.2.3)

➤ **To add NAT translation rules:**

1. Open the NAT Translation Table page (**Configuration** tab > **VoIP** menu > **Control Network** > **NAT Translation Table**).
2. Add a NAT rule to row index 1 for SIP messages:
 - **Source Interface Name:** Voice
 - **Target IP Address:** 212.199.200.90
 - **Source/Target Start/End Port:** 5070
3. Add a NAT rule to row index 2 for RTP packets:
 - **Source Interface Name:** Voice
 - **Target IP Address:** 212.199.200.90
 - **Source/Target Start Port:** 7000
 - **Source/Target End Port:** 7090

Figure 4-47: NAT Translation Rule

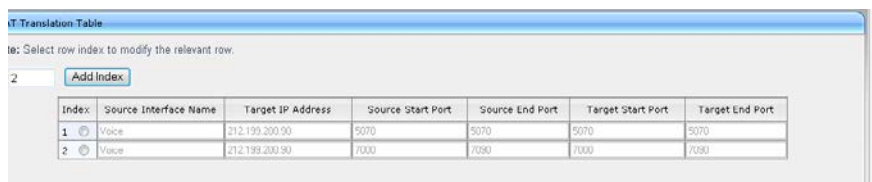


Table: Select row index to modify the relevant row.

2

Index	Source Interface Name	Target IP Address	Source Start Port	Source End Port	Target Start Port	Target End Port
1	Voice	212.199.200.90	5070	5070	5070	5070
2	Voice	212.199.200.90	7000	7090	7000	7090

4. Click **Apply** for each configuration.

4.2.7 Step 7: Add IP Groups for LAN Users and Hosted IP PBX

You need to configure an IP Group for each of the following entities:

- Hosted WAN IP PBX (Server-type IP Group)
- LAN users (User-type IP Group)

➤ **To add IP Groups:**

1. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **Control Network** > **IP Group Table**).
2. Add an IP Group to index 1 for the LAN users:
 - **Type:** USER
 - **Description:** LAN Users
 - **SRD:** 1
 - **Classify By Proxy Set:** Disable

Figure 4-48: IP Group for LAN Users

Index	1
Common Parameters	
Type	USER
Description	LAN Users
Proxy Set ID	
SIP Group Name	
Contact User	N/A
SRD	1
Media Realm	
IP Profile ID	0
Gateway Parameters	
Always Use Route Table	No
Routing Mode	Not Configured
SIP Re-Routing Mode	Standard
SBC Parameters	
Classify By Proxy Set	Disable

3. Add an IP Group to index 2 for the hosted WAN IP PBX:
 - **Type:** SERVER
 - **Description:** WAN IP PBX
 - **Proxy Set ID:** 2
 - **Classify By Proxy Set:** Enable

Figure 4-49: IP Group for Hosted IP PBX

Index	2
Common Parameters	
Type	SERVER
Description	WAN IP PBX
Proxy Set ID	2
SIP Group Name	
Contact User	
SRD	0
Media Realm	
IP Profile ID	0
Gateway Parameters	
Always Use Route Table	No
Routing Mode	Not Configured
SIP Re-Routing Mode	Standard
SBC Parameters	
Classify By Proxy Set	Enable

4. Click **Submit** for each configuration.
5. Save your setting to flash memory ("burn") with a device reset.

4.2.8 Step 8: Add Proxy Set for Hosted IP PBX Server

You need to define the destination address of the hosted WAN IP PBX. This is done by using a Proxy Set as described below.

➤ **To add a Proxy Set:**

1. Open the Proxy Sets Table page (**Configuration** tab > **VoIP** menu > **Control Network** > **Proxy Sets Table**).
2. Add a Proxy Set to index 2 for the hosted WAN IP PBX:
 - **Proxy Address:** 212.199.200.10
 - **SRD Index:** 2

Figure 4-50: Proxy Set for Hosted WAN IP PBX

	Proxy Address	Transport Type
1	212.199.200.10	UDP
2		
3		
4		
5		

Enable Proxy Keep Alive	Disable
Proxy Keep Alive Time	60
Proxy Load Balancing Method	Disable
Is Proxy Hot Swap	No
Proxy Redundancy Mode	Not Configured
SRD Index	2
Classification Input	IP only

3. Click **Submit**, and then save your setting to flash memory ("burn") with a device reset.

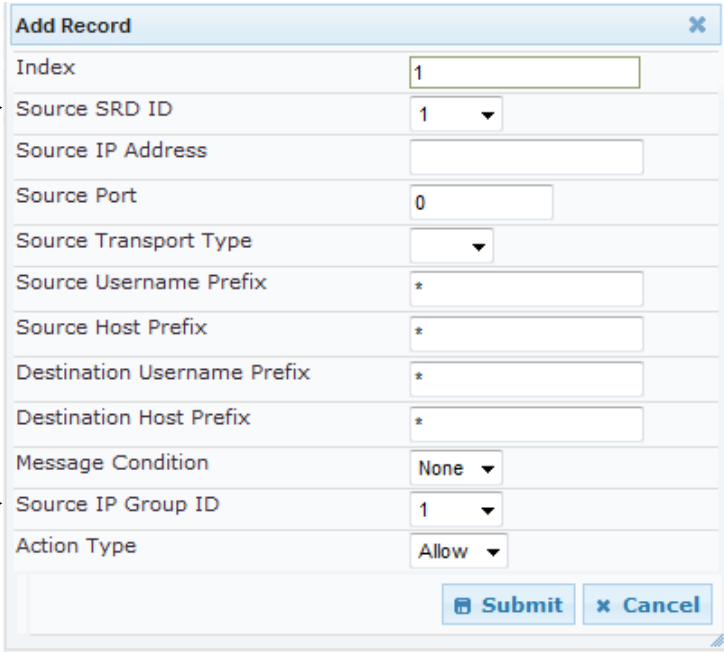
4.2.9 Step 9: Add Classification Rule for LAN Users

For the E-SBC to identify calls from LAN users and to classify them to their IP Group, you need to add a classification rule. In the example, calls received on SRD 1 will be identified as LAN users and assigned to IP Group 1. Note that other classification methods (e.g., using source prefix number) can be used to classify the calls.

➤ **To add a classification rule for LAN users:**

1. Open the Classification Table page (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **Classification Table**).
2. Add a classification rule to index 1:
 - **Source SRD:** 1
 - **Source IP Group ID:** 1

Figure 4-51: Classification Rule for LAN Users



Add Record	
Index	1
Source SRD ID	1
Source IP Address	
Source Port	0
Source Transport Type	
Source Username Prefix	*
Source Host Prefix	*
Destination Username Prefix	*
Destination Host Prefix	*
Message Condition	None
Source IP Group ID	1
Action Type	Allow
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

3. Click **Submit**.

4.2.10 Step 10: Add IP-to-IP Call Routing Rules

You need to add routing rules for the following routing capabilities:

- Routing calls from the LAN users to hosted IP PBX
- Routing calls from the hosted IP PBX to the LAN users

The configuration of the call routing rules use the IP Groups of these entities to denote the source and destination of the route.

➤ **To add IP-to-IP call routing rules:**

1. Open the IP2IP Routing Table page (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **IP to IP Routing Table**).
2. Add a rule to row index 1, to route calls from the LAN users to the Hosted IP PBX:
 - **Source IP Group ID:** 1
 - **Destination Type:** IP Group
 - **Destination IP Group ID:** 2
3. Add a rule to row index 2, to route calls from the hosted IP PBX to the LAN users:
 - **Source IP Group ID:** 2
 - **Destination Type:** IP Group
 - **Destination IP Group ID:** 1

Figure 4-52: IP-to-IP Call Routing Rules

Index	Source IP Group ID	Destination Username Prefix	Destination Host	Request Type	Destination Type	Destination IP Group ID	Destination SRD ID	Destination Address	Destination Port	Alternative Route Options
1	1	*	*	All	IP Group	2	None		0	Route Row
2	2	*	*	All	IP Group	1	None		0	Route Row

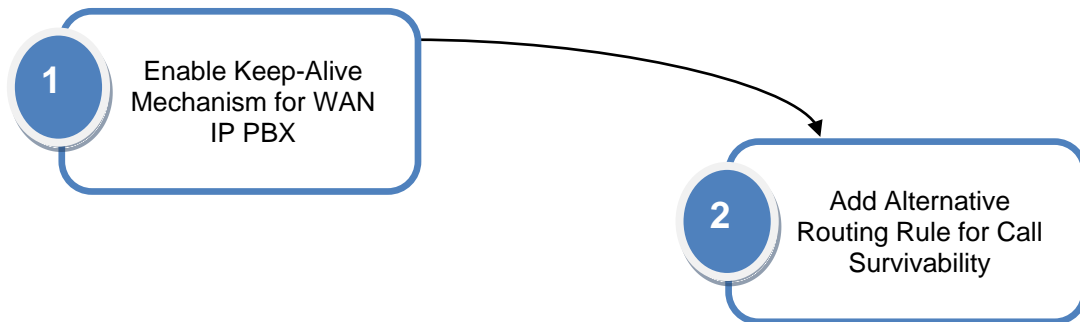
4. Click **Submit** for each configuration.

4.2.11 Call Survivability for LAN Users

During normal operation when connectivity with the hosted IP PBX exists, the LAN users register with the IP PBX through the E-SBC. During this process, the E-SBC also adds these registered users to its internal Registration database. Upon IP PBX failure, the E-SBC maintains call continuity between the LAN users, using this database.

The procedure for configuring call survivability is described in this subsection and summarized in the flowchart below:

Figure 4-53: Flowchart for Configuring Call Survivability



4.2.11.1 Step 1: Enable Keep-Alive for WAN IP PBX

The E-SBC performs call survivability upon a WAN failure or more specifically, when it detects an IP connectivity failure with the hosted WAN IP PBX. Therefore, you need to enable E-SBC to periodically check connectivity with this entity. To do so, you need to enable a keep-alive mechanism whereby the E-SBC periodically sends SIP OPTIONS messages to this entity.

➤ **To enable keep-alive mechanism with the WAN IP PBX:**

1. Open the Proxy Sets Table page (**Configuration** tab > **VoIP** menu > **Control Network** > **Proxy Sets Table**).
2. Select index 2 (i.e., the Proxy Set of the WAN IP PBX), and then set the following:
 - **Enable Proxy Keep Alive:** Using Options

Figure 4-54: Enabling Keep-Alive for WAN IP PBX

Proxy Set ID		Proxy Address		Transport Type
1	212.199.200.10			UDP
2				
3				
4				
5				

Enable Proxy Keep Alive	Using Options
Proxy Keep Alive Time	60
Proxy Load Balancing Method	Disable
Is Proxy Hot Swap	No
Proxy Redundancy Mode	Not Configured
SRD Index	2
Classification Input	IP only

3. Click **Submit**.

4.2.11.2 Step 2: Add Alternative IP-to-IP Call Routing Rule for Call Survivability

You need to add an alternative IP-to-IP call routing rule that is used when connectivity with the hosted IP PBX fails. This rule **must** be added to the row index located immediately below the row of the LAN users to hosted IP PBX rule.

➤ **To add an IP-to-IP call routing rule for call survivability:**

1. Open the IP2IP Routing Table page (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **IP to IP Routing Table**).
2. Add a rule to the row (i.e., index 2) located immediately below the main rule for routing calls to the hosted IP PBX:
 - **Source IP Group ID:** 1
 - **Destination Type:** IP Group
 - **Destination IP Group ID:** 1
 - **Alternative Route Options:** Alt Route Consider Inputs

Figure 4-55: IP-to-IP Call Routing Rule for LAN User Survivability

Index	Source IP Group ID	Destination Username Prefix	Destination Host	Request Type	Destination Type	Destination IP Group ID	Destination SRD ID	Destination Address	Destination Port	Alternative Route Options
1	1	*	*	All	IP Group	2	None		0	Route Row
2	1	*	*	All	IP Group	1	None		0	Alt Route Cons
3	2	*	*	All	IP Group	1	None		0	Route Row

3. Click **Submit**.



Notes:

- When you add the alternative routing rule to index 2, the previous rule of index 2 (for routing calls from the hosted IP PBX to the LAN users) is shifted down to row index 3.
- When the E-SBC detects the return of network connectivity with the hosted IP PBX, it uses the main routing rule (i.e., index 1) instead of the alternative rule.

4.2.12 Step 11: Reset E-SBC and Verify Configuration in Syslog

Once you have completed the previous configuration steps, you must reset the E-SBC with a flash burn for your settings take effect, and then use Syslog to check the messages received at device startup.

Ensure that there are no configuration errors related to SRDs, Media Realms, or SIP interfaces.

The Syslog message below shows an example of an error indicating that the Media Realm name ("MediaRealmLa") is invalid. This could be caused by incorrect spelling of the configured Media Realm in the SRD table.

```
( lgr_psbrdif)(3 ) !! [ERROR]
PSOSBoardInterface::TranslateRealmName failed since MediaRealm
name(MediaRealmLa) is INVALID
```

4.3 SIP Normalization between SIP Entity Servers

This example scenario includes the following topology architecture:

■ **Application:**

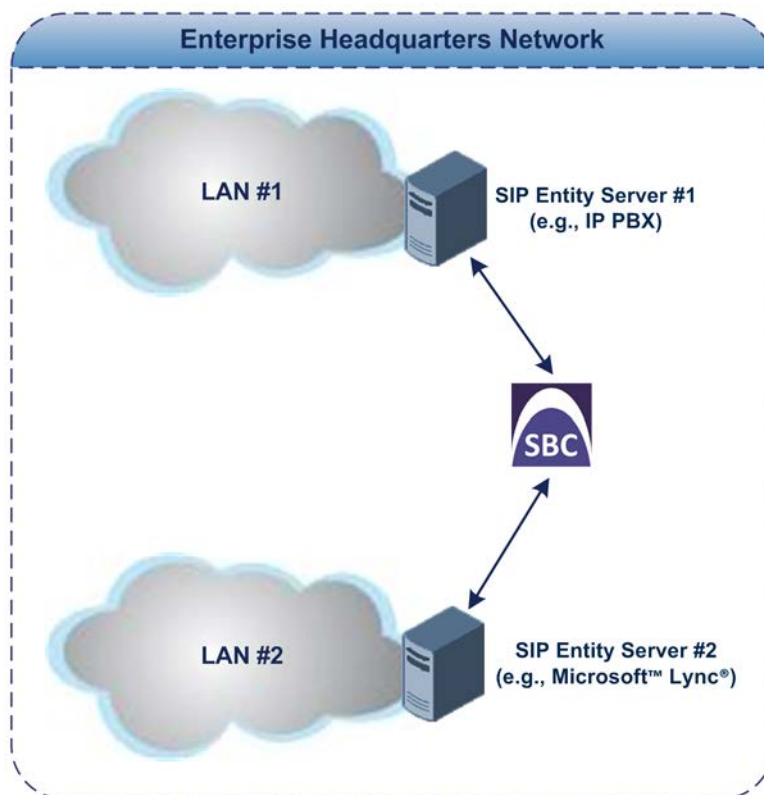
- Enterprise LAN users in LAN #1 served by SIP entity server #1:
 - ◆ Voice coder: G.711
 - ◆ SIP transport protocol: UDP
- Enterprise LAN users in LAN #2 served by SIP entity server #2:
 - ◆ Voice coder: G.729
 - ◆ SIP transport protocol: TCP

■ **SIP Normalization:**

- Voice transcoding between G.711 and G.729.
- SIP transport protocol translation between UDP and TCP.
- Manipulation on SIP INVITE messages from SIP entity server #1 so that the caller ID sent to SIP entity server #2 displays the calling party's user name (i.e., extension number) and host name "itsp" (e.g., 4410@itsp.com).

The figure below illustrates the application of this example scenario:

Figure 4-56: SIP Normalization Example - Application Topology



■ **Topology:**

- **E-SBC Logical Network Interface Connection:**

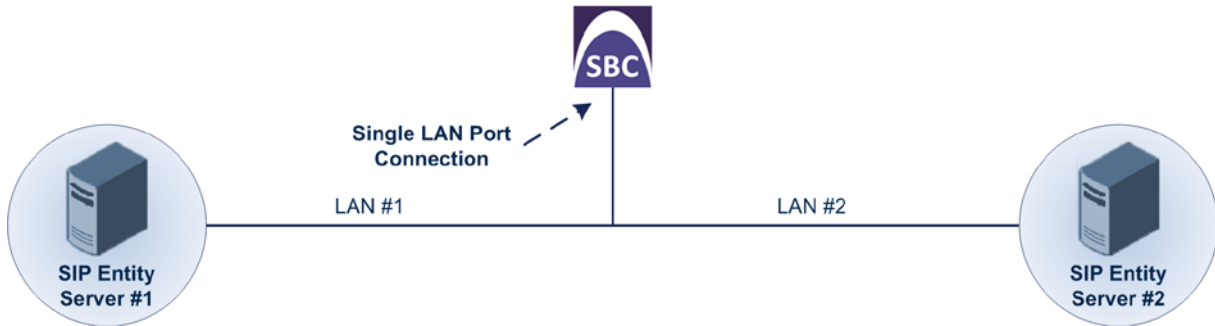
The E-SBC communicates with the SIP entity servers using a single IP network interface.

- **E-SBC Physical LAN Port Connection:**

The E-SBC uses a single LAN port to connect to the LAN.

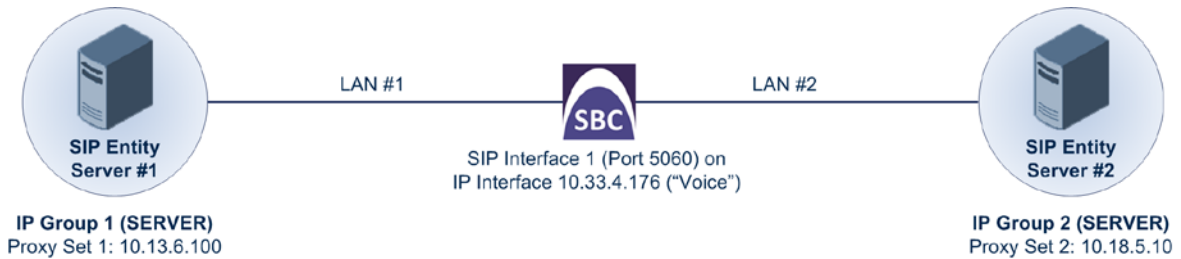
The figure below shows the E-SBC's logical network interface and LAN port connection of this example scenario:

Figure 4-57: E-SBC Physical Port Connection and Logical Interface



The main configuration entities used in this example are shown below.

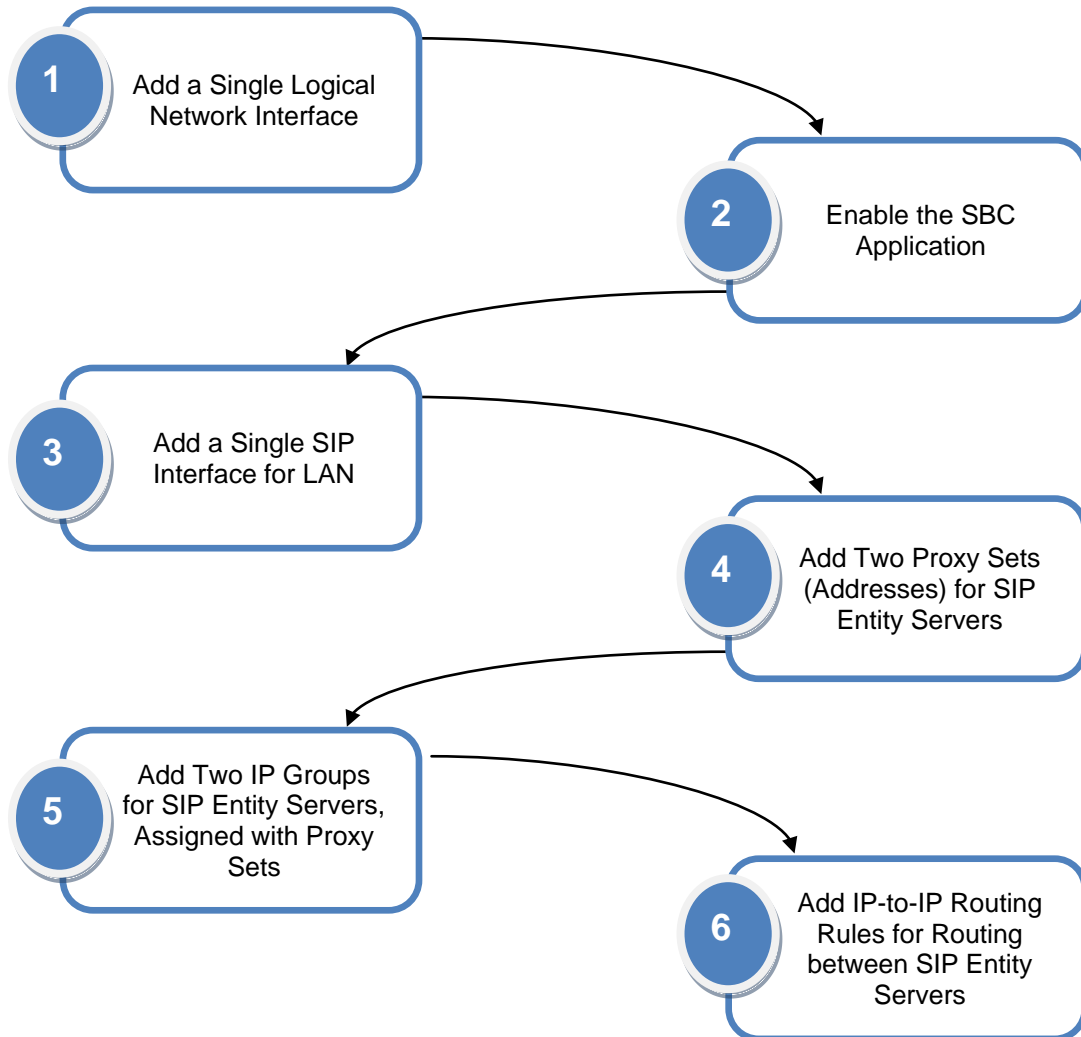
Figure 4-58: Required Configuration Entities



Note: For clarity, whenever configuring the various entities in this example (e.g., Media Realms, Proxy Sets, and IP Groups), table row index 1 is used for the E-SBC network interfacing with SIP Entity Server #1; row index 2 is used for the E-SBC network interfacing with SIP Entity Server #2.

The configuration steps for the example scenario are summarized in the flowchart below:

Figure 4-59: Summary of Configuration Steps



4.3.1 Step 1: Add a Logical IP Network Interface for LAN

As this example employs only one logical network interface (10.33.4.176) for the LAN, and this same interface is also used for management (i.e., OAMP), which is already set up, additional configuration is unnecessary.

Figure 4-60: Logical IP Network Interface for LAN and WAN

Index	Application Type	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name	Primary DNS Server IP Address	Secondary DNS Server IP Address	Underlying Interface
0	OAMP + Media + Control	10.33.4.176	16	10.33.0.1	1	Voice	0.0.0.0	0.0.0.0	GROUP_1

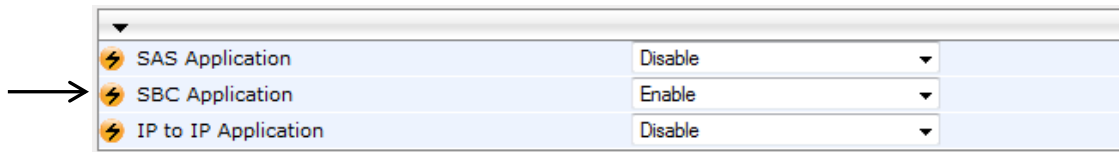
4.3.2 Step 2: Enable the SBC Application

For the E-SBC to operate as an SBC, you need to enable the SBC application. Once enabled, the SBC-specific parameters and pages become available in the Web interface.

➤ To enable the SBC application:

1. Open the Applications Enabling page (**Configuration** tab > **VoIP** menu > **Applications Enabling** > **Applications Enabling**).
2. From the 'SBC Application' drop-down list, select **Enable**.

Figure 4-61: Enabling the SBC Application



3. Click **Submit** to apply the changes.
4. Save your setting to flash memory ("burn") with a device reset.

4.3.3 Step 3: Add a SIP Interface for LAN

You need to create a SIP Interface for the LAN, which interfaces with both SIP entity servers. This SIP Interface is associated with the logical IP network interface, 10.33.4.176 ("Voice").

➤ To add a SIP Interface:

1. Open the SIP Interface Table page (**Configuration** tab > **VoIP** menu > **Control Network** > **SIP Interface Table**).
2. Add a SIP Interface to index 1 for the LAN interface:
 - **Network Interface:** Voice
 - **Application Type:** SBC
 - **UDP / TCP / TLS Port:** 5060 / 5060 / 5061 respectively
 - **SRD:** 0 (default)

Figure 4-62: SIP Interfaces for LAN Interface

Index	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	SRD	Message Policy
1	Voice	SBC	5060	5060	5061	0	None

3. Click **Apply**.



Note: **Network Interface** value string must be identical to the Interface Name string defined in the Multiple Interface table.

4.3.4 Step 4: Add IP Groups for SIP Entity Servers

For each SIP entity server, you need to add an IP Group, as described below.

➤ **To add IP Groups:**

1. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **Control Network** > **IP Group Table**).
2. Add an IP Group to index 1 for SIP Entity Server #1:
 - **Type:** SERVER
 - **Description:** SIP Entity 1
 - **Proxy Set ID:** 1
 - **Classify By Proxy Set:** Enable

Figure 4-63: IP Group for SIP Entity Server #1

Index	1
Common Parameters	
Type	SERVER
Description	SIP Entity 1
Proxy Set ID	1
SIP Group Name	
Contact User	
Domain Name in Contact	
SRD	0
Media Realm	
IP Profile ID	0
Gateway Parameters	
Always Use Route Table	No
Routing Mode	Not Configured
SIP Re-Routing Mode	Standard
SBC Parameters	
Classify By Proxy Set	Enable

3. Add an IP Group to index 2 for the SIP Entity Server #2:
 - **Type:** SERVER
 - **Description:** SIP Entity 2
 - **Proxy Set ID:** 2
 - **Classify By Proxy Set:** Enable

Figure 4-64: IP Group for SIP Entity Server #2

Index	2
▼ Common Parameters	
Type	SERVER
Description	SIP Entity 2
Proxy Set ID	2
SIP Group Name	
Contact User	
Domain Name in Contact	
SRD	0
Media Realm	
IP Profile ID	0
▼ Gateway Parameters	
Always Use Route Table	No
Routing Mode	Not Configured
SIP Re-Routing Mode	Standard
▼ SBC Parameters	
Classify By Proxy Set	Enable

4. Click **Submit** for each configuration.

4.3.5 Step 5: Add Proxy Sets for SIP Entity Servers

For each SIP entity server, you need to add a Proxy Set, as described below.

➤ **To add Proxy Sets to SIP entity servers:**

1. Open the Proxy Sets Table page (**Configuration** tab > **VoIP** menu > **Control Network** > **Proxy Sets Table**).
2. Add a Proxy Set to index 1 for the SIP Entity Server #1:
 - **Proxy Address:** 10.13.6.100
 - **Transport Type:** UDP

Figure 4-65: Proxy Set for SIP Entity Server #1

Proxy Set ID: 1

	Proxy Address	Transport Type
1	10.13.6.100	UDP
2		
3		
4		
5		

Enable Proxy Keep Alive: Disable
 Proxy Keep Alive Time: 60
 Proxy Load Balancing Method: Disable
 Is Proxy Hot Swap: No
 Proxy Redundancy Mode: Not Configured
 SRD Index: 0
 Classification Input: IP only

3. Add a Proxy Set to index 2 for SIP Entity Server #2:
 - **Proxy Address:** 10.18.5.10
 - **Transport Type:** TCP

Figure 4-66: Proxy Set for SIP Entity Server #2

Proxy Set ID: 2

	Proxy Address	Transport Type
1	10.18.5.10	TCP
2		
3		
4		
5		

Enable Proxy Keep Alive: Disable
 Proxy Keep Alive Time: 60
 Proxy Load Balancing Method: Disable
 Is Proxy Hot Swap: No
 Proxy Redundancy Mode: Not Configured
 SRD Index: 0
 Classification Input: IP only

4. Click **Submit** for each configuration.

4.3.6 Step 6: Add IP-to-IP Call Routing Rules

You need to add routing rules for the following:

- Routing calls from SIP Entity Server #1 to SIP Entity Server #2
- Routing calls from SIP Entity Server #2 to SIP Entity Server #1

The configuration of the call routing rules use the IP Groups of these entities to denote the source and destination of the route.

➤ **To add IP-to-IP call routing rules:**

1. Open the IP2IP Routing Table page (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **IP to IP Routing Table**).
2. Add a rule to index 1 to route calls from SIP Entity Server #1 to SIP Entity Server #2:
 - **Source IP Group ID:** 1
 - **Destination Type:** IP Group
 - **Destination IP Group ID:** 2
3. Add a rule to index 2 to route calls from SIP Entity Server #2 to SIP Entity Server #1:
 - **Source IP Group ID:** 2
 - **Destination Type:** IP Group
 - **Destination IP Group ID:** 1

Figure 4-67: IP-to-IP Call Routing Rules

Index	Source IP Group ID	Destination Username Prefix	Destination Host	Request Type	Destination Type	Destination IP Group ID	Destination SRD ID	Destination Address	Destination Port	Alternative Route Options
1	1	*	*	All	IP Group	2	None		0	Route Row
2	2	*	*	All	IP Group	1	None		0	Route Row

4. Click **Submit** for each configuration.

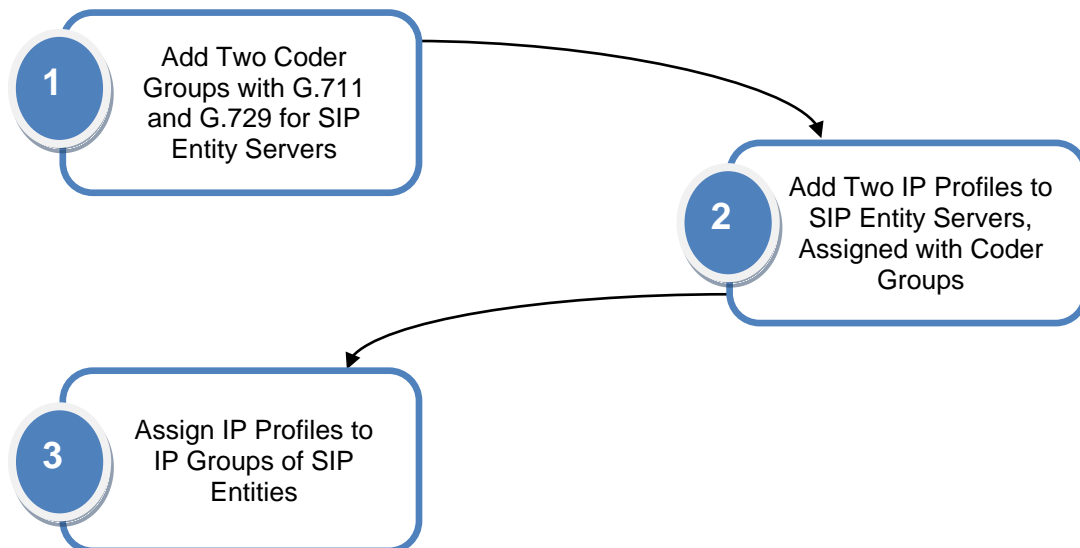
4.3.7 Voice Transcoding

As the two SIP entity servers support different voice codecs, you need to configure the E-SBC for transcoding. In the example, the codec support is as follows:

- SIP Entity Server #1 uses G.711
- SIP Entity Server #2 uses G.729

The procedure for configuring transcoding is described in this subsection and summarized in the flowchart below:

Figure 4-68: Flowchart for Configuring Transcoding



4.3.7.1 Step 1: Add Coder Groups for SIP Entities

For each SIP entity server, you need to add a Coder Group to define the required voice coder.

➤ **To add Coder Groups for the SIP entity servers:**

1. Open the Coder Group Settings page (**Configuration** tab > **VoIP** menu > **Coders And Profiles** > **Coders Group Settings**).
2. Add a Coder Group to index 1 for SIP Entity Server #1:
 - **Coder Name:** G.711A-law

Figure 4-69: Coder for SIP Entity Server #1

▼				
Coder Group ID				1 ▼
Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression
G.711A-law ▼	20 ▼	64 ▼	8	Disabled ▼

3. Add a Coder Group to index 1 for SIP Entity Server #2:
 - **Coder Name:** G.729

Figure 4-70: Coder for SIP Entity Server #2

▼				
Coder Group ID				2 ▼
Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression
G.729 ▼	20 ▼	8 ▼	18	Disabled ▼

4. Click **Submit** for each configuration.

4.3.7.2 Step 2: Add IP Profiles for SIP Entities

For each SIP entity server, you need to add an IP Profile configured with the required voice coder (i.e., Coder Group) that you previously added.

➤ **To add IP Profiles for the SIP entity servers:**

1. Open the IP Profile Settings page (**Configuration** tab > **VoIP** menu > **Coders And Profiles** > **IP Profile Settings**).
2. Add an IP Profile to index 1 for SIP Entity Server #1:
 - **Profile Name:** SIP Entity 1
 - **Extension Coders Group ID:** 1

Figure 4-71: IP Profile for SIP Entity Server #1

Profile ID	1
Profile Name	SIP Entity 1
Common Parameters	
RTP IP DiffServ	46
SBC	
Transcoding Mode	Only if Required
Extension Coders Group ID	Coders Group 1

3. Add an IP Profile to index 2 for SIP Entity Server #2:
 - **Profile Name:** SIP Entity 2
 - **Extension Coders Group ID:** 2

Figure 4-72: IP Profile for SIP Entity Server #2

Profile ID	2
Profile Name	SIP Entity 2
Common Parameters	
RTP IP DiffServ	46
SBC	
Transcoding Mode	Only if Required
Extension Coders Group ID	Coders Group 2

4. Click **Submit** for each configuration.

4.3.7.3 Step 3: Assign IP Profiles to SIP Entity IP Groups

To associate the voice coders with the SIP entity servers, you need to assign the previously configured IP Profiles to the IP Groups of these SIP entities.

➤ **To assign the IP Profiles to the IP Groups of SIP entity servers:**

1. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **Control Network** > **IP Group Table**).
2. Select index 1 (the IP Group of SIP Entity Server #1), and then set the following:

- Profile ID: 1

Figure 4-73: Assigning IP Profile to IP Group of SIP Entity Server #1

▼	
Index	1
▼ Common Parameters	
Type	SERVER
Description	SIP Entity 1
Proxy Set ID	1
SIP Group Name	
Contact User	
Domain Name in Contact	
SRD	0
Media Realm	
IP Profile ID	1
▼ Gateway Parameters	
Always Use Route Table	No
Routing Mode	Not Configured
SIP Re-Routing Mode	Standard
▼ SBC Parameters	
Classify By Proxy Set	Enable

3. Select index 2 (the IP Group of SIP Entity Server #2), and then set the following:

- Profile ID: 2

Figure 4-74: Assigning IP Profile to IP Group of SIP Entity Server #2

▼	
Index	2
▼ Common Parameters	
Type	SERVER
Description	SIP Entity 2
Proxy Set ID	2
SIP Group Name	
Contact User	
Domain Name in Contact	
SRD	0
Media Realm	
IP Profile ID	2
▼ Gateway Parameters	
Always Use Route Table	No
Routing Mode	Not Configured
SIP Re-Routing Mode	Standard
▼ SBC Parameters	
Classify By Proxy Set	Enable

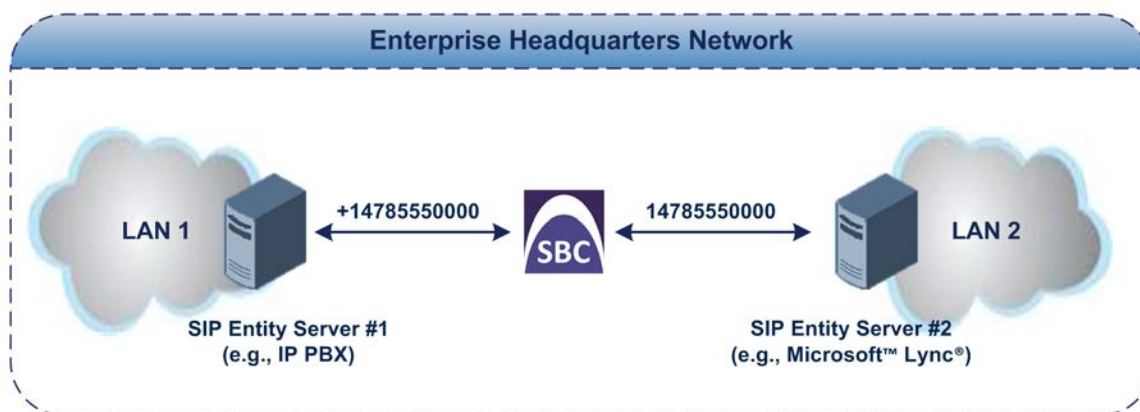
4. Click **Submit** for each configuration.

4.3.8 Number Manipulation

As SIP Entity Server #1 employs the E.164 number format while SIP Entity Server #2 does not, the E-SBC needs to perform number normalization when routing between these entities. For example, 14785551234 to +14785551234

The following number manipulation rules need to be configured:

- Calls received from SIP Entity Server #1 with destination number prefix "+": remove this prefix in the source and destination URI.
- Calls received from SIP Entity Server #2 with destination number prefix "1": add "+" to the prefix in the source and destination URI.



➤ **To add number manipulation rules:**

1. Open the IP to IP Inbound Manipulation page (**Configuration** tab > **VoIP** menu > **SBC** submenu > **Manipulations SBC** submenu > **IP to IP Inbound**).
2. For row index 1, add the following manipulation rule for calls from IP Group 1:
 - **Source IP Group:** 1
 - **Destination Username Prefix:** +
 - **Request Type:** INVITE
 - **Manipulated URI:** Destination
 - **Remove From Left:** 1
3. For row index 2, add the following manipulation rule for calls from IP Group 1:
 - **Source IP Group:** 1
 - **Destination Username Prefix:** +
 - **Request Type:** INVITE
 - **Manipulated URI:** Source
 - **Remove From Left:** 1
4. For row index 3, add the following manipulation rule for calls from IP Group 2:
 - **Source IP Group:** 2
 - **Destination Username Prefix:** 1
 - **Request Type:** INVITE
 - **Manipulated URI:** Destination
 - **Prefix to Add:** +

5. For row index 4, add the following manipulation rule:
 - **Source IP Group:** 2
 - **Destination Username Prefix:** 1
 - **Request Type:** INVITE
 - **Manipulated URI:** Source
 - **Prefix to Add:** +

Figure 4-75: Destination Number Manipulation Rules

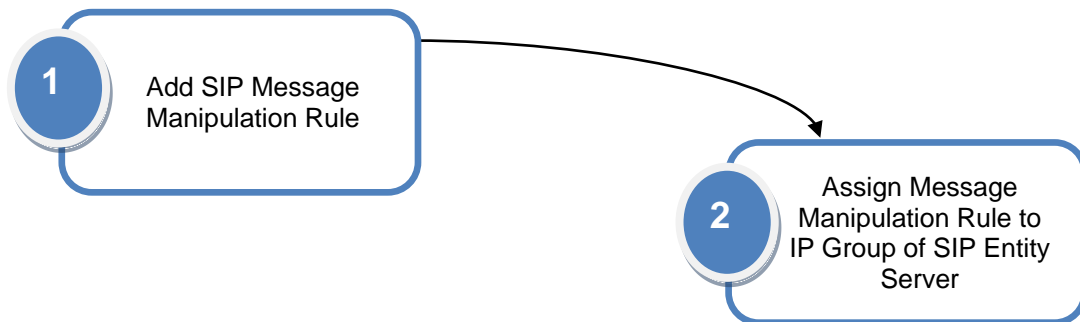
Source IP Group	Source Username Prefix	Source Host	Destination Username Prefix	Destination Host	Request Type	Manipulated URI	Remove From Left	Remove From Right	Leave From Right	Prefix to Add
1	*	*	+	*	INVITE	Destination	1	0	255	
1	*	*	+	*	INVITE	Source	1	0	255	
2	*	*	1	*	INVITE	Destination	0	0	255	+
2	*	*	1	*	INVITE	Source	0	0	255	+

6. Click **Apply** for each configuration.

4.3.9 SIP Message Manipulation

The procedure for configuring SIP message manipulation is described in this subsection and summarized in the flowchart below:

Figure 4-76: Flowchart for Configuring SIP Message Manipulation



4.3.9.1 Step 1: Add a SIP Message Manipulation Rule

In this example, the E-SBC needs to manipulate SIP INVITE messages received from SIP Entity Server #1 so that the caller ID sent to SIP Entity Server #2 displays the calling party's user name (i.e., extension number) and the host name, "itsp" (e.g., 4410@itsp.com). This is done by adding a SIP P-Asserted-Identity header that contains the user part value of the From header.

```

From: <sip:1000@10.8.5.41>;tag=1c1286571572
To: <sip:FEU8-999-1@WANWAN>
Call-ID: 128652844814102010161846@212.25.26.70
CSeq: 1 INVITE
Contact: <sip:FEU3-998-2@212.25.26.70:5060>
Supported: em,100rel,timer,replaces,path,resource-priority,sdp-anat
Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
User-Agent: Audiocodes-Sip-Gateway-Mediant/v.6.40A.004
P-Asserted-Identity: sip:1000@itsp.com
  
```


➤ **To add a SIP message manipulation rule:**

1. Open the Message Manipulations page (**Configuration** tab > **VoIP** menu > **SBC** > **Manipulations SBC** > **Message**).
2. For row index 1, add the following manipulation rule:
 - **Manipulation Set ID:** 1
 - **Message Type:** invite
 - **Action Subject:** header.p-asserted-identity
 - **Action Type:** Add (default)
 - **Action Value:** '<sip:' + header.from.url.user + '@itsp.com>'
 - **Row Rule:** Use Current Condition (default)

Figure 4-77: SIP Message Manipulation Rule

Index	Manipulation Set ID	Message Type	Condition	Action Subject	Action Type	Action Value	Row Role
1	1	invite		header.p-asserted-identity	Add	'<sip:' + header.from.url.user + '@itsp.com>'	Use Current Condition

3. Click **Submit**.



Note: In the **Action Value** field, the value "header.from.url.user" adds the From header's user part to the P-Asserted-Identity header's user part, and the value "@itsp.com" adds itsp.com to the P-Asserted-Identity header's host part.

4.3.9.2 Step 2: Assign Manipulation Rule to IP Group of SIP Entity Server #2

As the SIP message manipulation rule must be done on the INVITE messages received from SIP Entity Server #2, you need to assign this rule to the IP Group of SIP Entity Server #2 for incoming messages.

- **To assign the SIP message manipulation rule to SIP Entity Server #2:**
- 1. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **Control Network** > **IP Group Table**).
- 2. Select index 1 (the IP Group of SIP Entity Server #2), and then set the following:
 - **Inbound Message Manipulation Set:** 1

Figure 4-78: Assigning Manipulation Rule to IP Group of SIP Entity Server #2

Index	2
▼ Common Parameters	
Type	SERVER
Description	SIP Entity 2
Proxy Set ID	2
SIP Group Name	
Contact User	
Domain Name in Contact	
⚡ SRD	0
⚡ Media Realm	
IP Profile ID	2
▼ Gateway Parameters	
Always Use Route Table	No
Routing Mode	Not Configured
SIP Re-Routing Mode	Standard
▼ SBC Parameters	
Classify By Proxy Set	Enable
Max Number Of Registered Users	-1
→ Inbound Message Manipulation Set	1

3. Click **Submit**.

Reader's Notes



Deployment Guide