Configuration Note

SBC Configuration Examples

Mediant™ Session Border Controllers (SBC)

Version 7.0

Table of Contents

Notice

This document provides configuration examples for the SBC application of AudioCodes' Mediant Session Border Controllers (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. Updates to this document and other documents as well as software files can be downloaded by registered customers at http://www.audiocodes.com/downloads.

This document is subject to change without notice.

Date Published: April-19-2015

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 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.

Abbreviations and Terminology

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

Throughout this document, unless otherwise specified, the term *SBC* refers to AudioCodes Mediant SBC products.

Important Notes

> **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 SBC deployment examples. However, your 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.

Document Revision Record

LTRT	Description
31624	Initial document release for Version 7.0.
31625	Multi-tenant example added; SBC Routing Policy added in Section 1.1; note updated in Section 2.9 regarding destination SIP Interface; miscellaneous formatting.

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 document provides a variety of deployment examples and corresponding configuration for AudioCodes' Mediant™ Session Border Controller (SBC) product series, Software Version 7.0. Each example includes a description of the example scenario topology as well as step-by-step procedures on how to configure the SBC. The configuration described in this document is through the SBC's Web-based management tool.

The following deployment examples are provided:

- Enterprise IP PBX with SIP Trunk and WAN Users on page 9
- Alternative Routing upon SIP Trunk Failure on page 23
- Hosted WAN IP PBX on page 39
- Call Survivability for LAN Users upon Hosted IP PBX Failure on page 49
- SIP Normalization between SIP Entity Servers on page 51
- Multi-Tenant Deployment on page 67

Notes:

- Throughout this document, callout arrows are used in configuration-related figures to indicate the required parameter configuration. Parameters without callout arrows indicate that the default value is used and thus, the parameter can be ignored.
- When you have completed all the configuration steps of an example, you **must** reset the device with a burn-to-flash memory in order for your settings to take effect. If you don't, your settings will not be maintained if the device is subsequently powered off, reset without a burn-to-flash, or crashes for whatever reason.
- It is recommended to verify that your configuration is correct by checking Syslog messages for any invalid configuration.
- 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. Thus, it is recommended to configure each configuration entity with meaningful names for easy identification.

1.1 Configuration Terminology

Before configuring the SBC, you should familiarize yourself with some of the main terminology of SBC configuration entities.

Table 1-1: Terminology of SBC Configuration Terms

Term	Description
SRD	Represents the entire VoIP network. Typically, only a single SRD is required and this is the recommended configuration topology (multiple SRDs are only required for multi-tenant deployments). The device is shipped with a default SRD (at Index 0). If you are using only one SRD, the SRD is automatically assigned to new configuration entities, for example, when adding a Proxy Set. Therefore, when using a single SRD, there is no need to even handle SRD configuration.
Media Realm	Defines a UDP port range for RTP (media) traffic on a specific logical IP network interface.

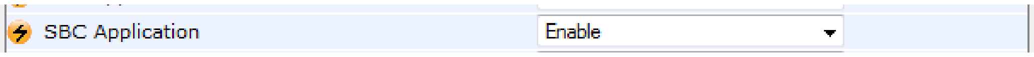
Term	Description
SIP Interface	Represents a Layer-3 network, by defining a listening port for SIP signaling traffic on a specific logical IP network interface. Multiple SIP Interfaces can be associated with a single SRD, and therefore, if your VoIP deployment includes multiple Layer-3 networks (for example, SIP Trunk, LAN IP PBX, remote WAN users), a SIP Interface would be configured for each Layer-3 network and then all assigned to the same SRD.
IP Group	Represents a SIP entity with which the SBC receives and sends calls. 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 address of the entity by associating it with a Proxy Set. IP Groups are used in IP-to-IP routing rules to denote the source and destination of the call.
Proxy Set	Defines the destination addresses (IP address or FQDN) of the SIP entity server (server-type IP Group). The Proxy Set is assigned to an IP Group belonging to the relevant SIP entity.
IP Profile	Defines a set of call behavior (e.g., required coders, fax transport type, and transcoding method) that can be associated with a specific IP Group.
Classification	Process that identifies the SIP entity (IP Group) from where the call is received.
SBC Routing Policy	SBC Routing Policy logically groups routing and manipulation (inbound and outbound) rules to create "separate" manipulation and routing tables. The SBC Routing Policy is assigned to an SRD. The SBC Routing Policy also enables Least Cost Routing (LCR) for routing rules and associates an LDAP server for LDAP-based routing. As multiple SBC Routing Policies are required only for multi-tenant deployments, for most deployments only a single SBC Routing Policy is required. When only a single SBC Routing Policy is required, handling of this configuration entity is not required as a default SBC Routing Policy is provided, which is automatically associated with all relevant configuration entities.

1.2 Enabling the SBC Application

The examples in this document are related to the SBC application. Therefore, before configuring your SBC according to the provided examples, make sure that the SBC application is enabled; otherwise, SBC functionality and SBC-specific parameters will be unavailable in the Web interface. If the SBC application is disabled, enable it as follows:

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 1-1: Enabling the SBC Application



SBC Application: Enable

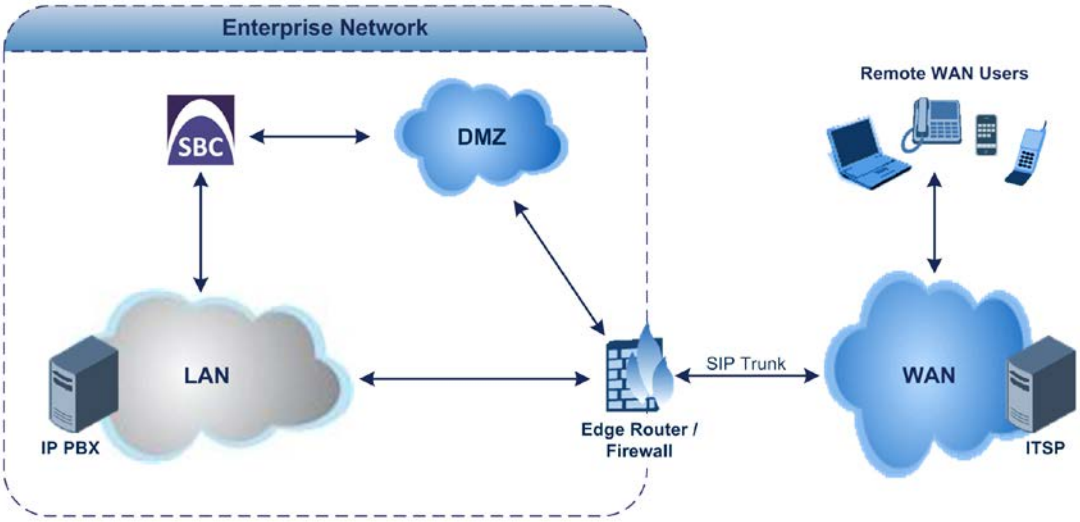
3. Click **Submit**, and then reset the SBC with a burn-to-flash memory for the setting to take effect.

2 Enterprise IP PBX with SIP Trunk and WAN Users

The example describes how to configure the SBC when interworking between an IP PBX, a SIP Trunk, and nomadic WAN users. The example scenario includes the following topology architecture:

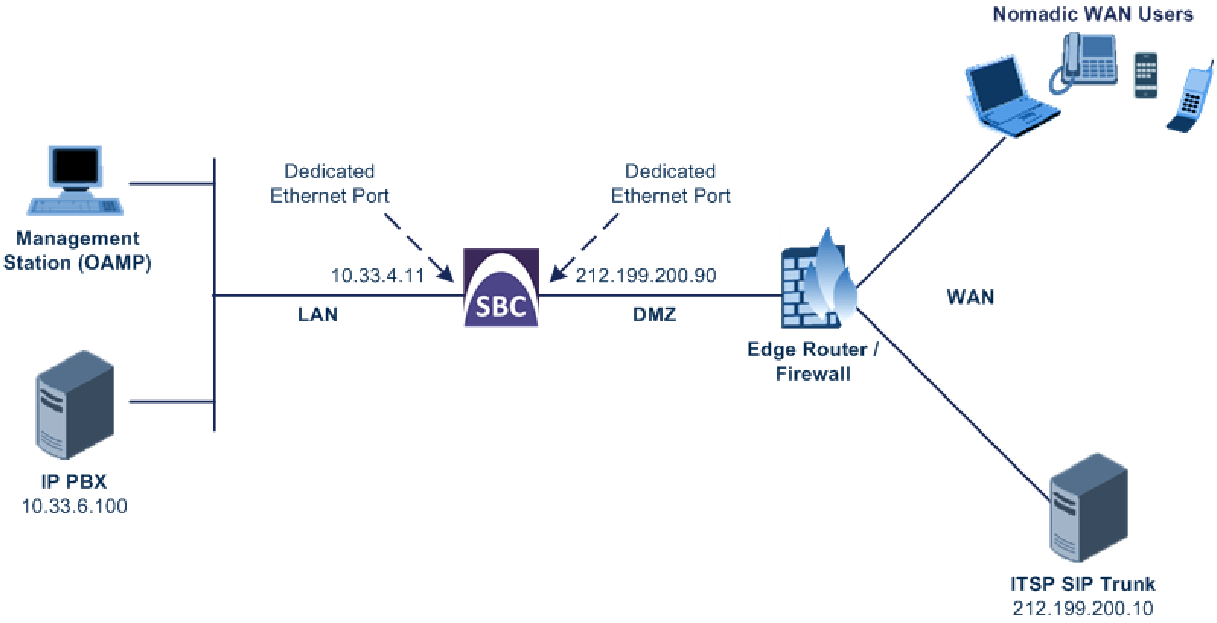
- **Application:**
  - Enterprise LAN IP PBX at IP address, 10.33.6.100
  - WAN SIP Trunk at IP address, 212.199.200.10
  - Nomadic WAN users

Figure 2-1: Enterprise IP PBX with SIP Trunk and Nomadic WAN Users



- **Topology:**
  - **SBC Logical Network Interface Connections:**
    - One logical network interfacing with the LAN, using IP address 10.33.4.11. The interface is also used for management (OAMP).
    - One logical network interfacing with the DMZ / WAN, using IP address 212.199.200.90.
  - **SBC Physical LAN Port Connections:**
    - One Ethernet port connected to the LAN.
    - One Ethernet port connected to the DMZ / WAN.

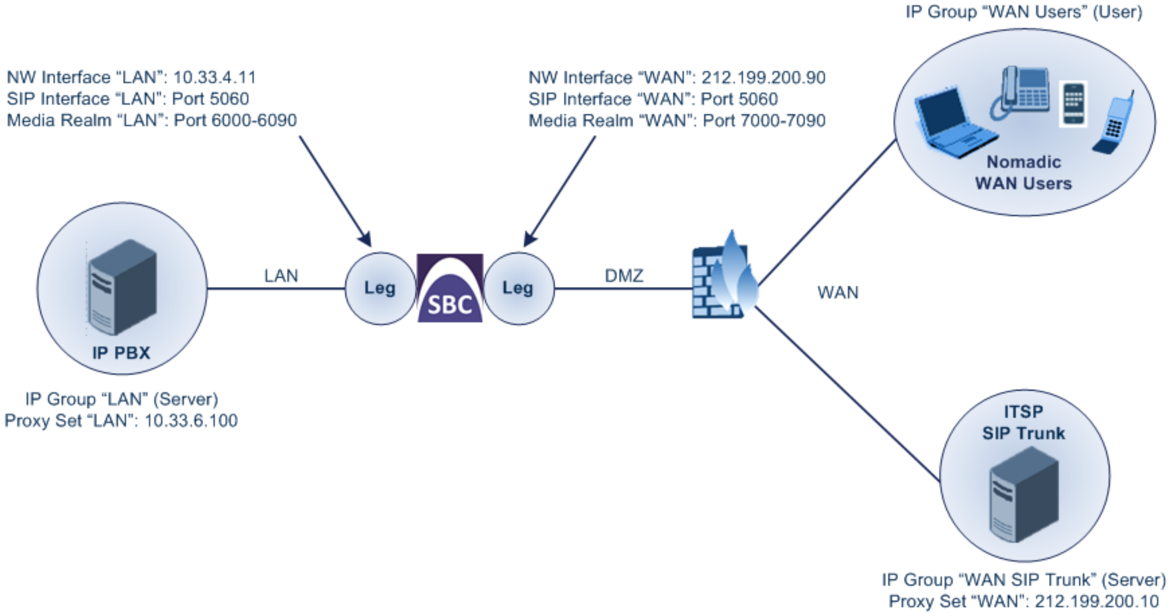
Figure 2-2: SBC Logical Interfaces and Physical Port Connections



Note: The SBC could alternatively use a **single** Ethernet port, physically connected to a VLAN-aware switch.

A summary of the required configuration is shown below:

Figure 2-3: Summary of Required Configuration


IP Group "WAN Users" (User)
NW Interface "LAN": 10.33.4.11
SIP Interface "LAN": Port 5060
Media Realm "LAN": Port 6000-6090
NW Interface "WAN": 212.199.200.90
SIP Interface "WAN": Port 5060
Media Realm "WAN": Port 7000-7090
Nomadic WAN Users
LAN
Leg
SBC
Leg
DMZ
WAN
IP PBX
IP Group "LAN" (Server)
Proxy Set "LAN": 10.33.6.100
ITSP SIP Trunk
IP Group "WAN SIP Trunk" (Server)
Proxy Set "WAN": 212.199.200.10

Notes:

- For clarity, configuration entities configured with the name "LAN" are used for interfacing with the LAN (e.g., IP PBX) and those configured with the name "WAN" are used for the interfacing with the WAN (e.g., SIP Trunk).
- As the example uses only a single SRD, the default SRD is automatically assigned when adding configuration entities.

2.1 Step 1: Assign Ethernet Ports to Ethernet Groups

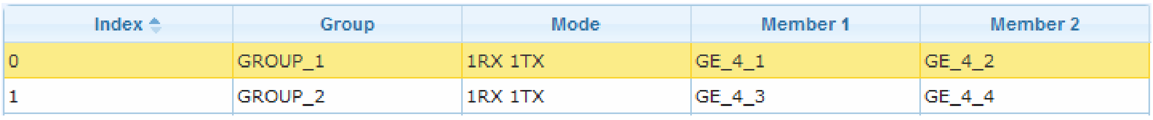
The example implements physical Ethernet port separation between the LAN and WAN networks. Therefore, you first need to assign your ports to groups (called *Ethernet Groups*). In the example, two ports are assigned to each group, providing 1+1 port redundancy:

- **LAN:** Ethernet Group 1 with ports G_4_1 and G_4_2
- **WAN:** Ethernet Group 2 with ports G_4_3 and G_4_4

➢ **To assign ports to Ethernet Groups:**

1. Open the Ethernet Group Settings table (**Configuration** tab > **VoIP** menu > **Network** > **Ethernet Groups Table**).
2. Assign the ports to Ethernet Groups:

Figure 2-4: Ports assigned to Ethernet Groups in Ethernet Group Settings Table



Index	Group	Mode	Member 1	Member 2
0	GROUP_1	1RX 1TX	GE_4_1	GE_4_2
1	GROUP_2	1RX 1TX	GE_4_3	GE_4_4

Notes:

- This step is applicable only to the following products: Mediant 500 E-SBC, Mediant 800 Gateway & E-SBC; Mediant 2600 E-SBC, Mediant 4000 SBC, Mediant 9000 SBC and Mediant VE/SE software.
- Port names depend on the product.
- To configure port speed and duplex mode, use the Physical Ports Settings table (PhysicalPortsTable).

2.2 Step 2: Assign VLAN IDs to Ethernet Groups

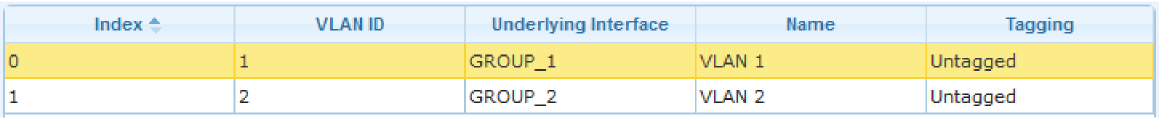
The example employs a regular switch (not a VLAN-aware switch) connected to the SBC, and therefore, to separate LAN and WAN traffic in the SBC, you need to first assign untagged VLANs to your ports (Ethernet Groups):

- **LAN:** VLAN ID 1 assigned to Ethernet Group 1
- **WAN:** VLAN ID 2 assigned to Ethernet Group 2

➢ **To assign VLANs to Ethernet Groups:**

1. Open the Ethernet Device table (**Configuration** tab > **VoIP** menu > **Network** > **Ethernet Device Table**).
2. Assign the VLANs to the Ethernet Groups:

Figure 2-5: VLANs Configured for Ethernet Groups in Ethernet Device Table



Index	VLAN ID	Underlying Interface	Name	Tagging
0	1	GROUP_1	VLAN 1	Untagged
1	2	GROUP_2	VLAN 2	Untagged

Note: The step is applicable only to the following products: Mediant 500 E-SBC, Mediant 800 Gateway & E-SBC; Mediant 2600 E-SBC, Mediant 4000 SBC, Mediant 9000 SBC and Mediant VE/SE software.

2.3 Step 3: Add Logical IP Network Interfaces for LAN and WAN

In the example, you need to add two logical IP network interfaces:

- **LAN:** IP address 10.33.4.11
- **WAN:** IP address 212.199.200.90

The example assumes that the OAMP network interface is also used for the LAN interface, which is already set up.

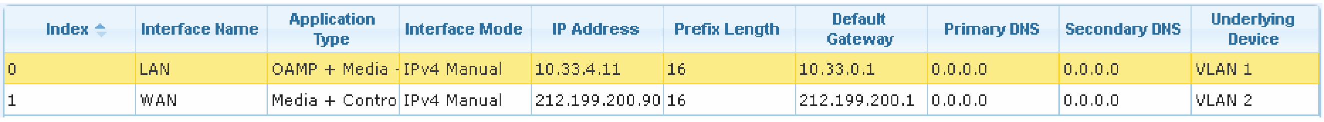
In addition, to apply your physical, Ethernet port separation between LAN and WAN traffic (configured previously), you need to assign the VLANs (*Underlying Device*) that you configured in Step 2, to the network interfaces, where:

- VLAN 1 (Ethernet Group 1) is assigned to the LAN interface
- VLAN 2 (Ethernet Group 2) is assigned to the WAN interface

➢ To add the logical IP network interfaces:

1. Open the Interface table (**Configuration** tab > **VoIP** menu > **Network** > **IP Interfaces Table**).
2. Configure LAN and WAN interfaces:

Figure 2-6: Configured Logical IP Network Interfaces for LAN and WAN in Interface Table



Index	Interface Name	Application Type	Interface Mode	IP Address	Prefix Length	Default Gateway	Primary DNS	Secondary DNS	Underlying Device
0	LAN	OAMP + Media -	IPv4 Manual	10.33.4.11	16	10.33.0.1	0.0.0.0	0.0.0.0	VLAN 1
1	WAN	Media + Contro	IPv4 Manual	212.199.200.90	16	212.199.200.1	0.0.0.0	0.0.0.0	VLAN 2

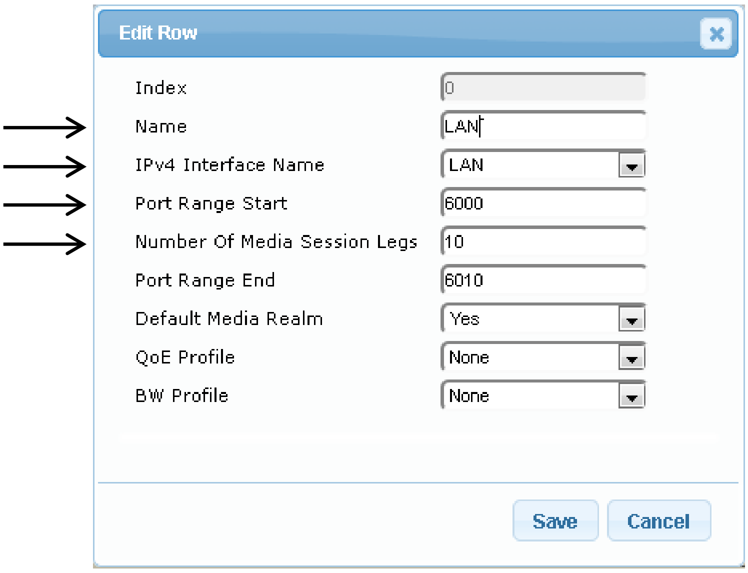
2.4 Step 4: Add Media Realms for LAN and WAN

Media Realms define a port range for media (RTP) traffic on a specified network interface. Therefore, you need to configure Media Realms for the LAN (IP PBX) and WAN (SIP Trunk and nomadic users) interfaces. You will later apply the Media Realms to your VoIP network by assigning them to SIP Interfaces (see Section 2.5).

➢ To add Media Realms:

1. Open the Media Realm table (**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:

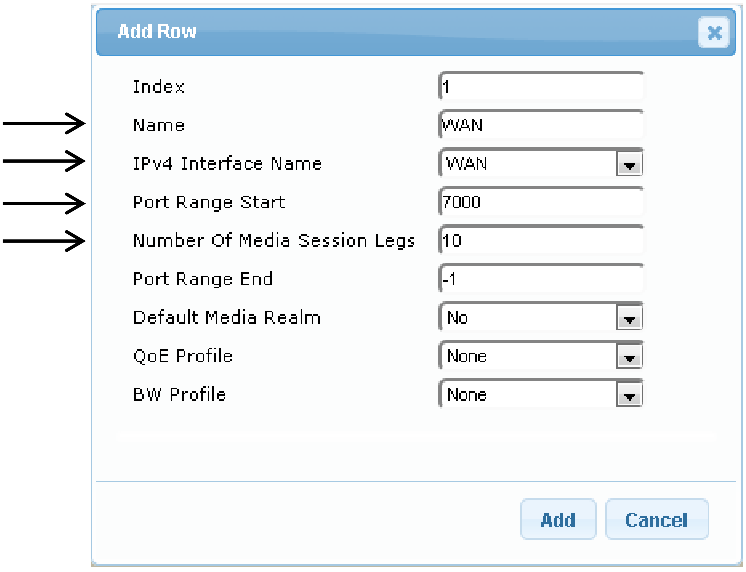
Figure 2-7: Media Realm for LAN Interface



Index	0
Name	LAN
IPv4 Interface Name	LAN
Port Range Start	6000
Number Of Media Session Legs	10
Port Range End	6010
Default Media Realm	Yes
QoE Profile	None
BW Profile	None

3. Add a Media Realm for the WAN interface:

Figure 2-8: Media Realm for WAN Interface



Index	1
Name	WAN
IPv4 Interface Name	WAN
Port Range Start	7000
Number Of Media Session Legs	10
Port Range End	-1
Default Media Realm	No
QoE Profile	None
BW Profile	None

Note: The 'Port Range End' parameter's value is automatically calculated (based on start port range and number of sessions) after you click **Add** in the dialog box.

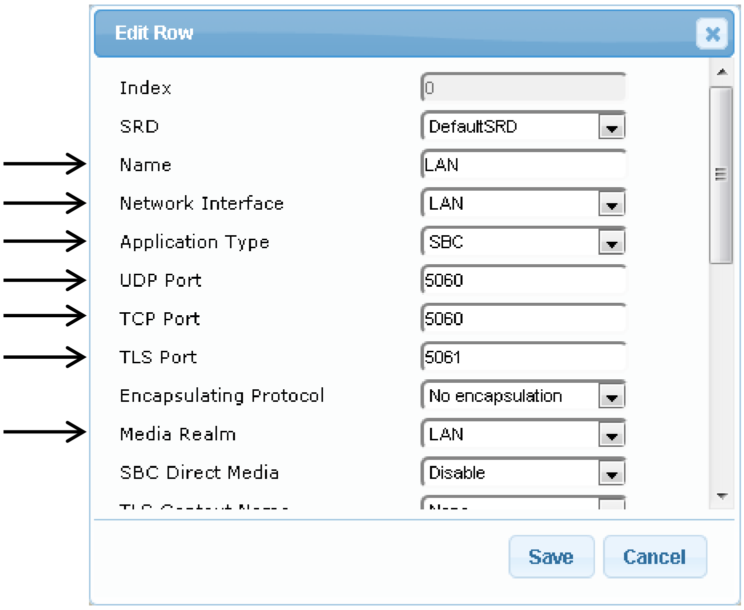
2.5 Step 5: Add SIP Interfaces for LAN and WAN

The SIP Interface represents a Layer-3 network, defining the listening port for SIP signaling traffic on a specific network interface. The SIP Interface also determines the port and network interface for media (Media Realm, configured in Section 2.4). Therefore, you need to add a SIP Interface for the LAN and WAN interfaces.

➢ To add SIP Interfaces:

1. Open the SIP Interface table (**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:

Figure 2-9: SIP Interface for LAN

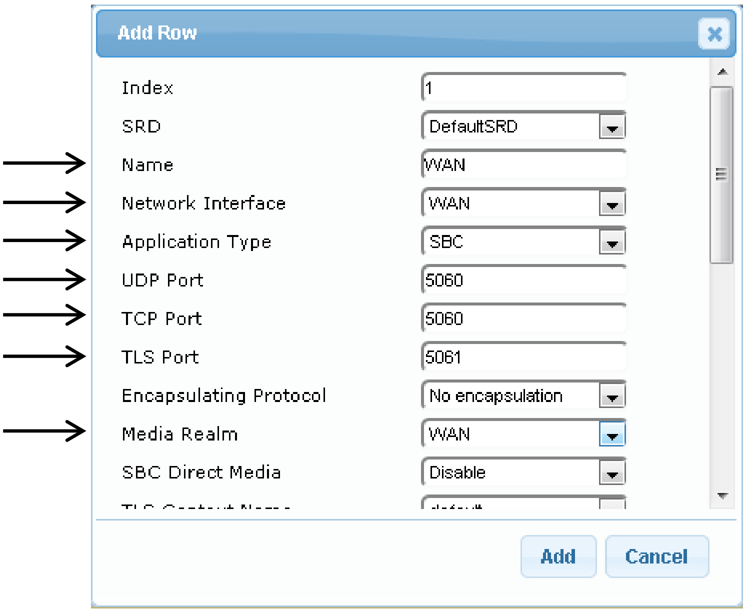


Edit Row

Index	0
SRD	DefaultSRD
Name	LAN
Network Interface	LAN
Application Type	SBC
UDP Port	5060
TCP Port	5060
TLS Port	5061
Encapsulating Protocol	No encapsulation
Media Realm	LAN
SBC Direct Media	Disable
TLS Context Name	None

3. Add a SIP Interface for the WAN interface:

Figure 2-10: SIP Interface for WAN



Add Row

Index	1
SRD	DefaultSRD
Name	WAN
Network Interface	WAN
Application Type	SBC
UDP Port	5060
TCP Port	5060
TLS Port	5061
Encapsulating Protocol	No encapsulation
Media Realm	WAN
SBC Direct Media	Disable
TLS Context Name	default

2.6 Step 6: Add Proxy Sets for IP PBX and SIP Trunk

The Proxy Set defines the actual address of SIP server entities in your network. Therefore, you need to add a Proxy Set for the following entities:

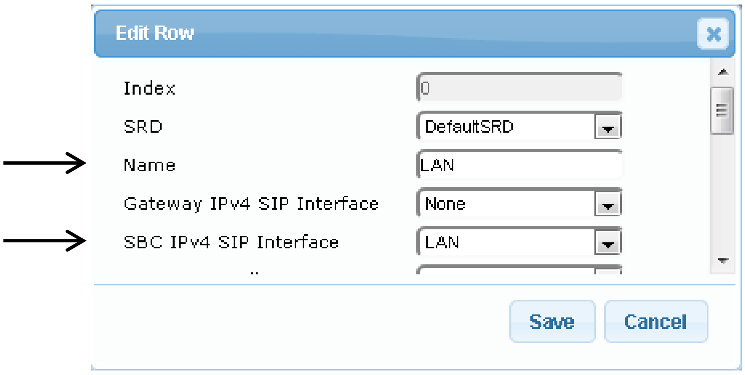
- **LAN:** IP PBX with address 10.33.6.100
- **WAN:** SIP Trunk with address 212.199.200.10

You will later apply the Proxy Sets to your VoIP network by assigning them to IP Groups, which represent these entities (see Section 2.7).

➢ **To add Proxy Sets:**

1. Open the Proxy Sets table (**Configuration** tab > **VoIP** menu > **VoIP Network** > **Proxy Sets Table**).
2. Add a Proxy Set for the LAN IP PBX. You can use the default Proxy Set (Index 0), but modify it as shown below:
   a. Add the Proxy Set:

Figure 2-11: Proxy Set for IP PBX



Edit Row

Index: 0

SRD: DefaultSRD

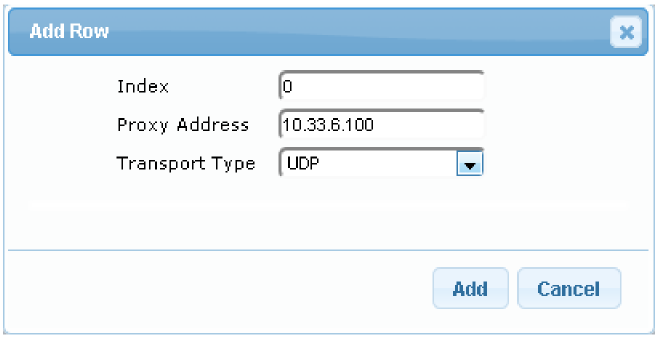
Name: LAN

Gateway IPv4 SIP Interface: None

SBC IPv4 SIP Interface: LAN

   b. Select the table row of the Proxy Set that you added, and then click the **Proxy Address Table** link located below the table.
   c. Add the IP address of the IP PBX:

Figure 2-12: Proxy Set Address for IP PBX



Add Row

Index: 0

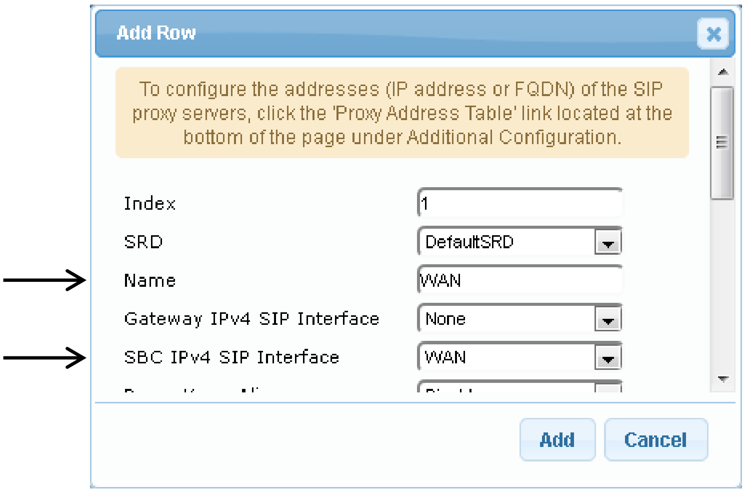
Proxy Address: 10.33.6.100

Transport Type: UDP

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

   a. Add the Proxy Set:

Figure 2-13: Proxy Set for SIP Trunk



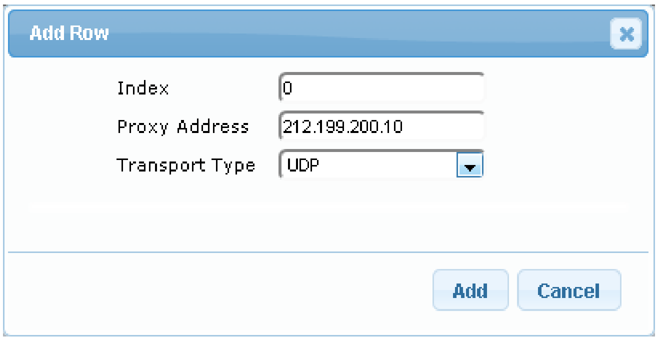
To configure the addresses (IP address or FQDN) of the SIP proxy servers, click the 'Proxy Address Table' link located at the bottom of the page under Additional Configuration.

Index	1
SRD	DefaultSRD
Name	WAN
Gateway IPv4 SIP Interface	None
SBC IPv4 SIP Interface	WAN

   b. Select the table row of the Proxy Set that you added, and then click the **Proxy Address Table** link located below the table.

   c. Add the IP address of the IP PBX:

Figure 2-14: Proxy Set Address for SIP Trunk



Index	0
Proxy Address	212.199.200.10
Transport Type	UDP

2.7 Step 7: Add IP Groups for IP PBX, SIP Trunk, and WAN Nomadic Users

The IP Group represents the SIP entity. In the example, you need to add an IP Group for the following entities:

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

For the server-type IP Groups, you need to assign their respective Proxy Sets, which define their addresses (see Section 2.6). You also need to enable the SBC to classify incoming calls to the IP Groups, based on their source IP address (i.e., Proxy Set).

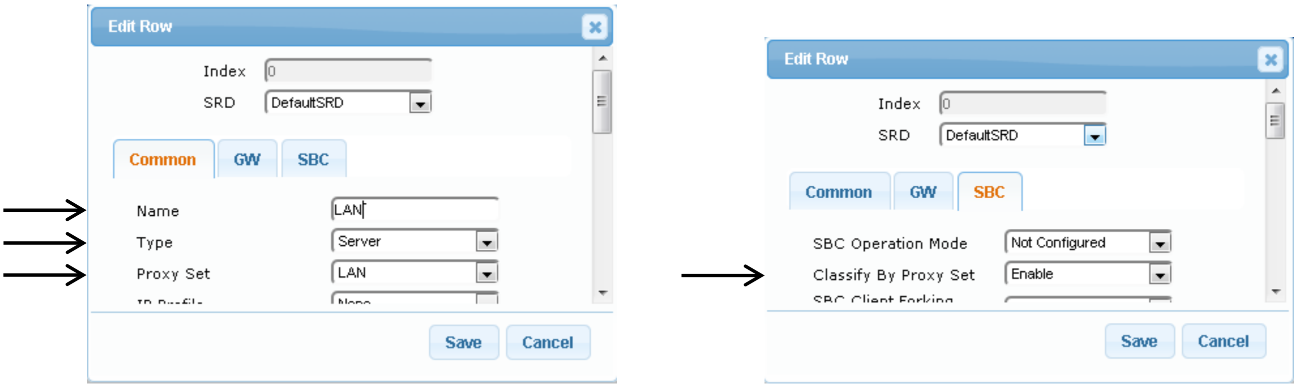
For the WAN users, a Proxy Set is not used and thus, classification by Proxy Set needs to be disabled.

> **Note:** The SBC resolves NAT issues for WAN users located behind NAT. By default, when an INVITE is received from a user behind NAT, the device sends the SIP response to the packet's source address (i.e., the public address of the NAT device), instead of to the IP address specified in the SIP Contact header. You can change this default behavior using the SIPNatDetection parameter.

➢ To add IP Groups:

1. Open the IP Group table (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group Table**).
2. Add an IP Group for the LAN IP PBX:

Figure 2-15: IP Group for LAN IP PBX

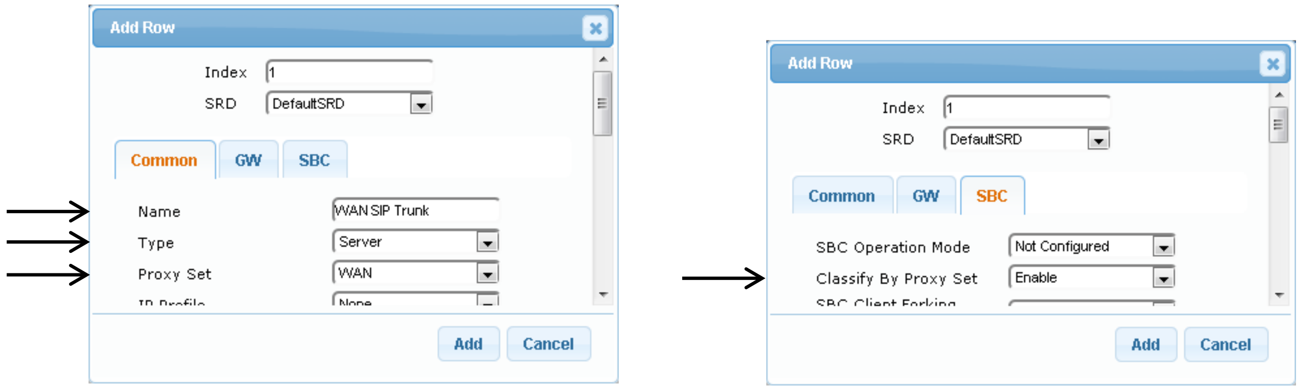


Index: 0
SRD: DefaultSRD
Name: LAN
Type: Server
Proxy Set: LAN
IP Profile: None

Index: 0
SRD: DefaultSRD
SBC Operation Mode: Not Configured
Classify By Proxy Set: Enable
SBC Client Forking

3. Add an IP Group for the WAN SIP Trunk:

Figure 2-16: IP Group for WAN SIP Trunk



Add Row

Index: 1
SRD: DefaultSRD

Name: WAN SIP Trunk
Type: Server
Proxy Set: WAN
IP Profile: None

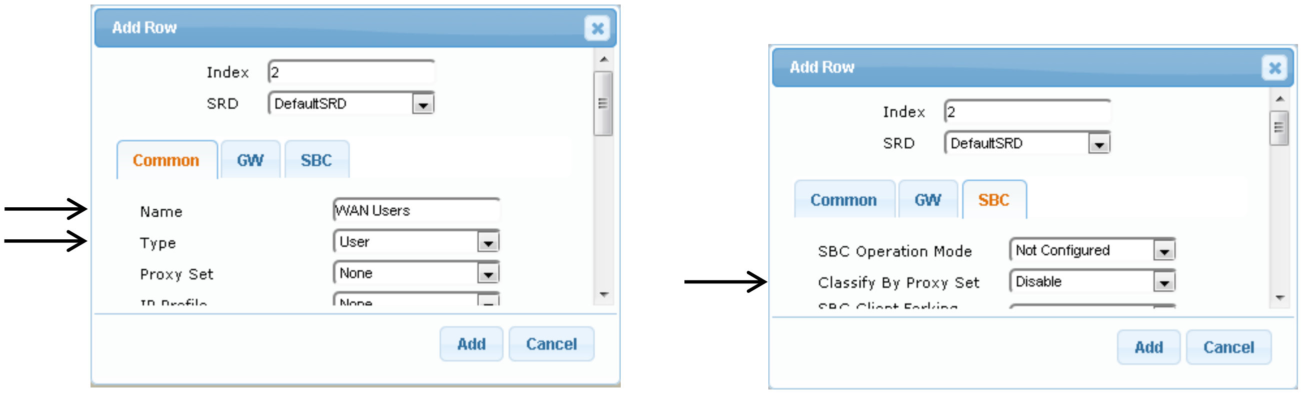
Add Row

Index: 1
SRD: DefaultSRD

SBC Operation Mode: Not Configured
Classify By Proxy Set: Enable
SBC Client Forking

4. Add an IP Group for the nomadic WAN users:

Figure 2-17: IP Group for WAN Nomadic Users



Add Row

Index: 2
SRD: DefaultSRD

Name: WAN Users
Type: User
Proxy Set: None
IP Profile: None

Add Row

Index: 2
SRD: DefaultSRD

SBC Operation Mode: Not Configured
Classify By Proxy Set: Disable
SBC Client Forking

2.8 Step 8: Add Classification for WAN Nomadic Users

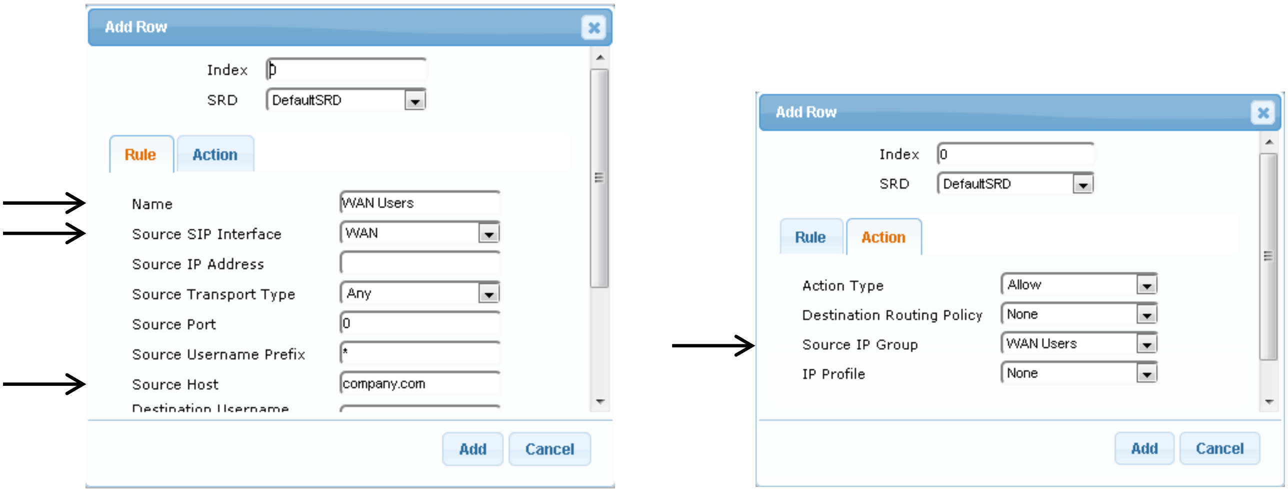
For the SBC to identify calls from WAN nomadic users and classify them to their IP Group (configured in Section 2.7), you need to add a classification rule. Remember that for the IP PBX and SIP trunk, you configured classification by Proxy Set (see Section 2.7).

In the example, calls received on the WAN interface (i.e., SIP Interface configured as "WAN") and whose prefix host name is “company.com”, will be identified as nomadic users and assigned to IP Group "WAN Users".

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

1. Open the Classification table (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **Classification Table**).
2. Add a Classification rule:

Figure 2-18: Classification Rule for WAN Nomadic Users



Index	0
SRD	DefaultSRD
Name	WAN Users
Source SIP Interface	WAN
Source IP Address	
Source Transport Type	Any
Source Port	0
Source Username Prefix	*
Source Host	company.com
Destination Username	

Index	0
SRD	DefaultSRD
Action Type	Allow
Destination Routing Policy	None
Source IP Group	WAN Users
IP Profile	None

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

For call routing between the SIP entities, you need to add IP-to-IP routing rules for the following call directions:

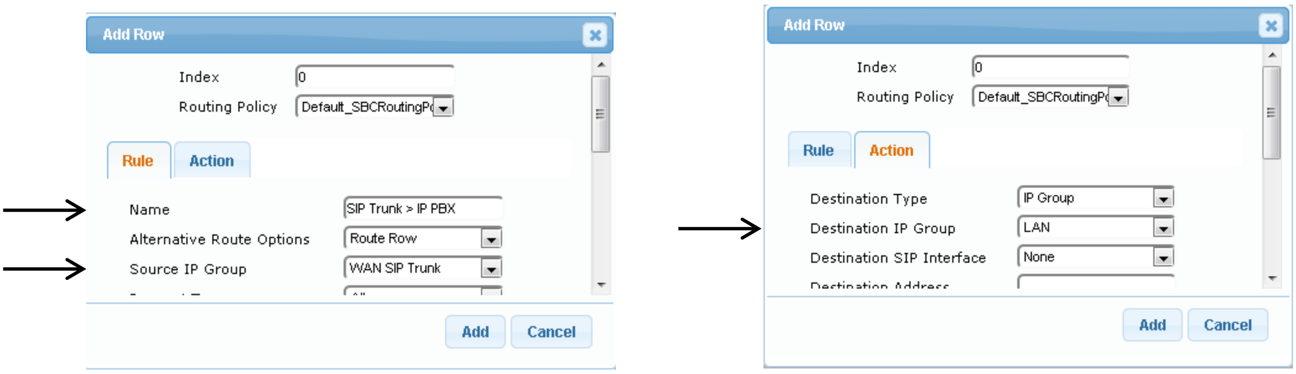
- Calls from the WAN SIP Trunk to the LAN IP PBX.
- Calls from the LAN IP PBX to the WAN SIP Trunk.
- Calls from the WAN nomadic users to the LAN IP PBX.
- Calls from the LAN IP PBX to the WAN nomadic users. As the WAN nomadic users in the example use a 5-digit extension number starting with the number 4 (e.g., 40011), numbers dialed from the IP PBX with the prefix "4" will be routed to the WAN users; all other dialed numbers from the IP PBX will be routed to the SIP Trunk.

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

➢ To add IP-to-IP call routing rules:

1. Open the IP-to-IP Routing table (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **IP-to-IP Routing Table**).
2. Add a rule to route calls from the WAN SIP Trunk to the LAN IP PBX:

Figure 2-19: Call Routing Rule from WAN SIP Trunk to LAN IP PBX

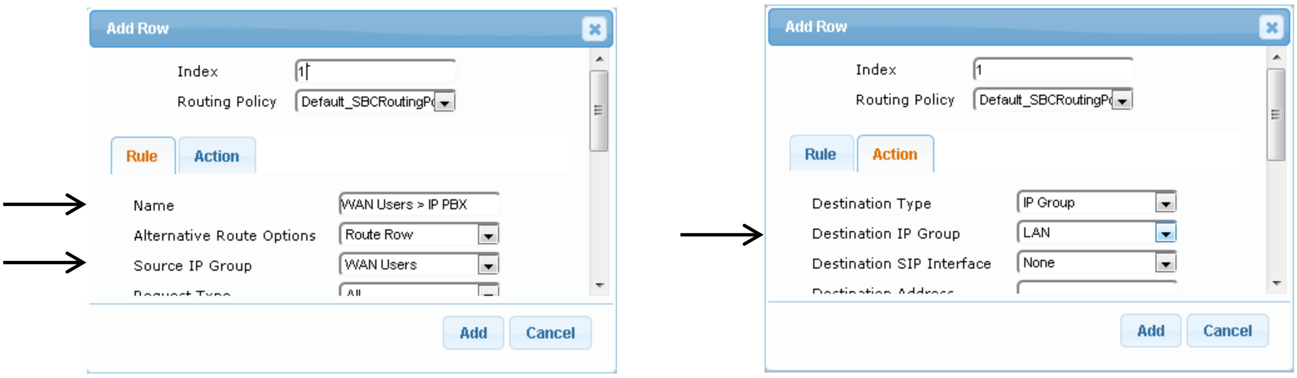


Index: 0
Routing Policy: Default_SBCRoutingP
Name: SIP Trunk > IP PBX
Alternative Route Options: Route Row
Source IP Group: WAN SIP Trunk

Index: 0
Routing Policy: Default_SBCRoutingP
Destination Type: IP Group
Destination IP Group: LAN
Destination SIP Interface: None
Destination Address:

3. Add a rule to route calls from WAN nomadic users to the LAN IP PBX:

Figure 2-20: Call Routing Rule from WAN Users to LAN IP PBX

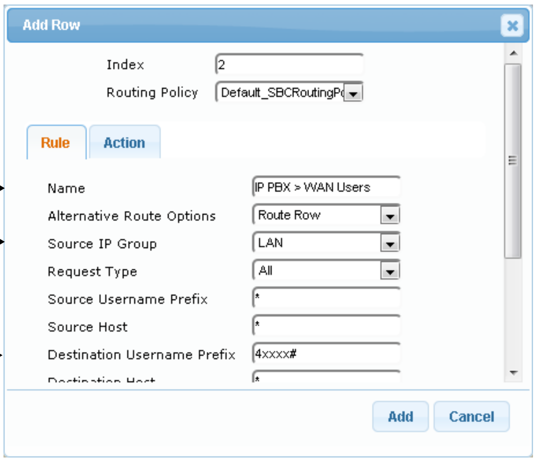


Index: 1
Routing Policy: Default_SBCRoutingP
Name: WAN Users > IP PBX
Alternative Route Options: Route Row
Source IP Group: WAN Users
Request Type: All

Index: 1
Routing Policy: Default_SBCRoutingP
Destination Type: IP Group
Destination IP Group: LAN
Destination SIP Interface: None
Destination Address:

4. Add a rule to route calls from the LAN IP PBX to the WAN users:

Figure 2-21: Call Routing Rule from LAN IP PBX to WAN Users

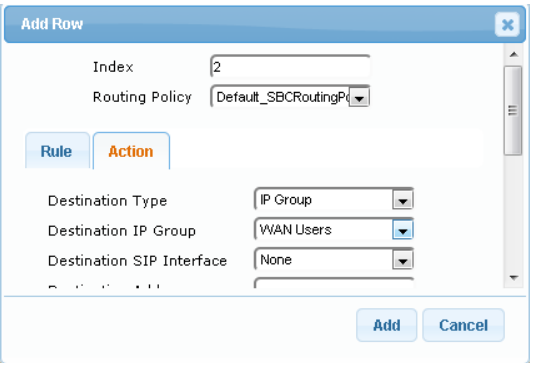


Add Row

Index: 2
Routing Policy: Default_SBCRoutingP

Rule | Action

Name: IP PBX > WAN Users
Alternative Route Options: Route Row
Source IP Group: LAN
Request Type: All
Source Username Prefix: *
Source Host: *
Destination Username Prefix: 4xxxx#
Destination Host: *



Add Row

Index: 2
Routing Policy: Default_SBCRoutingP

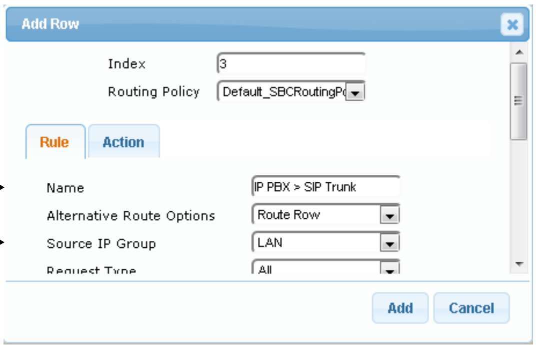
Rule | Action

Destination Type: IP Group
Destination IP Group: WAN Users
Destination SIP Interface: None

Note: The value "4xxxx#" configured in the 'Destination Username Prefix' parameter denotes a 5-digit number starting with 4. The *x* denotes a digit and the #, the end of the number. For more information on dialing notations, refer to the *User's Manual*.

5. Add a rule to route calls from the LAN IP PBX to the WAN SIP Trunk:

Figure 2-22: Call Routing Rule from LAN IP PBX to WAN SIP Trunk

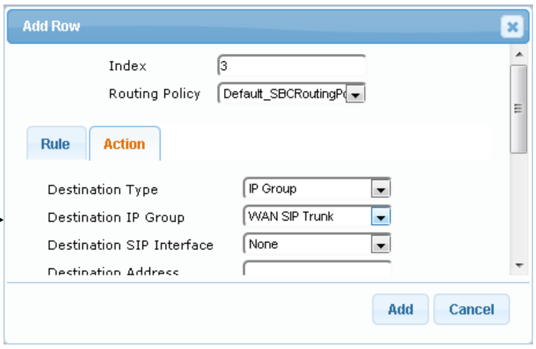


Add Row

Index: 3
Routing Policy: Default_SBCRoutingP

Rule | Action

Name: IP PBX > SIP Trunk
Alternative Route Options: Route Row
Source IP Group: LAN
Request Type: All



Add Row

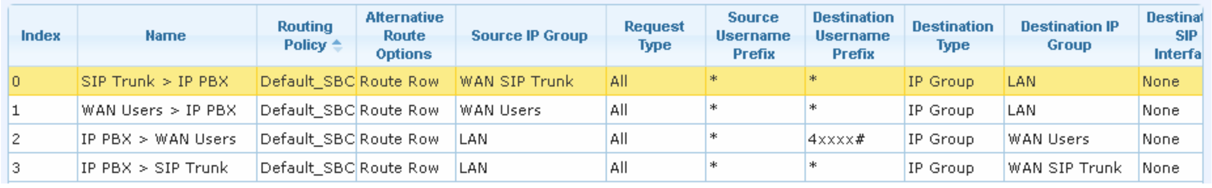
Index: 3
Routing Policy: Default_SBCRoutingP

Rule | Action

Destination Type: IP Group
Destination IP Group: WAN SIP Trunk
Destination SIP Interface: None
Destination Address

Once you have configured the IP-to-IP routing rules, the IP-to-IP Routing table should appear populated as shown below:

Figure 2-23: Configured IP-to-IP Routing Rules in the IP-to-IP Routing Table



Index	Name	Routing Policy	Alternative Route Options	Source IP Group	Request Type	Source Username Prefix	Destination Username Prefix	Destination Type	Destination IP Group	Destinat SIP Interfa
0	SIP Trunk > IP PBX	Default_SBC	Route Row	WAN SIP Trunk	All	*	*	IP Group	LAN	None
1	WAN Users > IP PBX	Default_SBC	Route Row	WAN Users	All	*	*	IP Group	LAN	None
2	IP PBX > WAN Users	Default_SBC	Route Row	LAN	All	*	4xxxx#	IP Group	WAN Users	None
3	IP PBX > SIP Trunk	Default_SBC	Route Row	LAN	All	*	*	IP Group	WAN SIP Trunk	None

Note: A destination SIP Interface is not specified for the routing rules. The 'Destination SIP Interface' parameter is applicable only if the 'Destination Type' parameter is configured to any value other than **IP Group**. When the 'Destination Type' parameter is configured to **IP Group**, the SIP Interface is determined as follows:

- Server-type IP Groups: SIP Interface that is assigned to the Proxy Set associated with the IP Group.
- User-type IP Groups: SIP Interface is determined during user registration with the device.

3 Alternative Routing upon SIP Trunk Failure

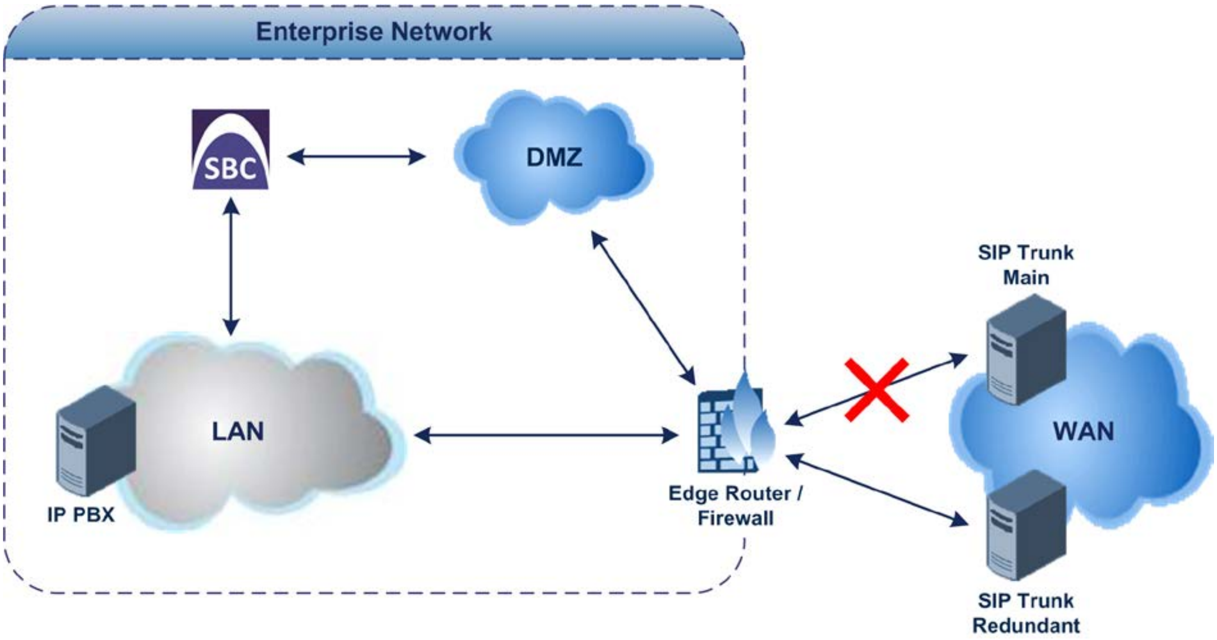
The alternative routing examples described in this section are based on the same main topology setup as described in the previous example (see Section 2). Two alternative routing examples are provided for call survivability solutions upon connectivity failure with the WAN SIP Trunk:

- SIP Trunk redundancy, whereby calls from the LAN IP PBX are routed to a redundant SIP trunk upon connectivity failure with the primary SIP Trunk.
- PSTN Fallback, whereby calls from the LAN IP PBX are routed to the PSTN upon connectivity failure with the SIP Trunk.

3.1 SIP Trunk Redundancy

The example describes how to configure SIP trunk redundancy, whereby upon primary SIP Trunk connectivity failure, calls from the LAN IP PBX are routed to a redundant SIP Trunk. The example assumes that the IP address of the redundant SIP Trunk is 212.199.200.12. The figure below illustrates the setup example.

Figure 3-1: SIP Trunk Redundancy Example Scenario



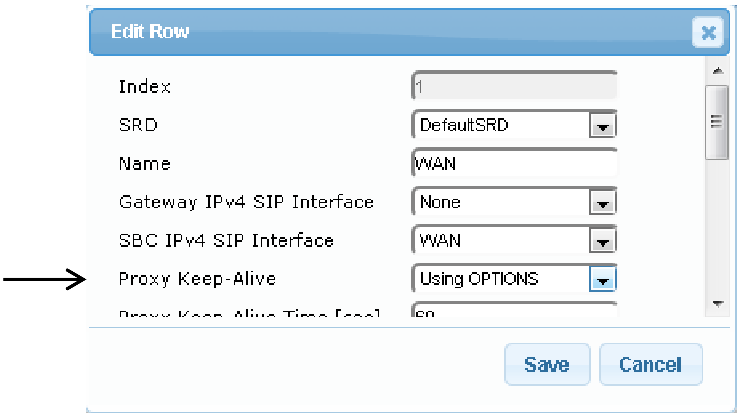
3.1.1 Step 1: Enable Keep-Alive for Proxy Set of Main SIP Trunk

For the device to detect connectivity failure, you need to enable the keep-alive mechanism with the main SIP Trunk. The keep-alive mechanism periodically checks connectivity with the SIP Trunk by sending SIP OPTIONS messages.

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

1. Open the Proxy Sets table (**Configuration** tab > **VoIP** menu > **V Network** > **Proxy Sets Table**).
2. Edit Proxy Set "WAN", which you configured for the WAN SIP Trunk (in the previous example), to enable proxy keep-alive using SIP OPTIONS messages:

Figure 3-2: Enabling Keep-Alive with Main SIP Trunk



Index	1
SRD	DefaultSRD
Name	WAN
Gateway IPv4 SIP Interface	None
SBC IPv4 SIP Interface	WAN
Proxy Keep-Alive	Using OPTIONS
Proxy Keep-Alive Time [sec]	60

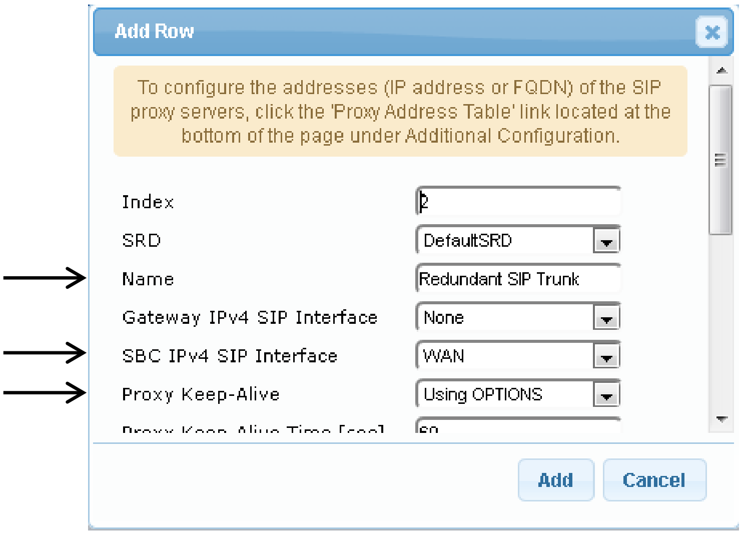
3.1.2 Step 2: Add a Proxy Set for Redundant SIP Trunk

The Proxy Set defines the address of the redundant SIP Trunk. In the example, the address of the SIP Trunk is 212.199.200.12.

➢ **To add a Proxy Set:**

1. Open the Proxy Sets table (**Configuration** tab > **VoIP** menu > **VoIP Network** > **Proxy Sets Table**).
2. Add a Proxy Set for the redundant SIP Trunk:
   a. Add the Proxy Set:

Figure 3-3: Proxy Set for Redundant SIP Trunk



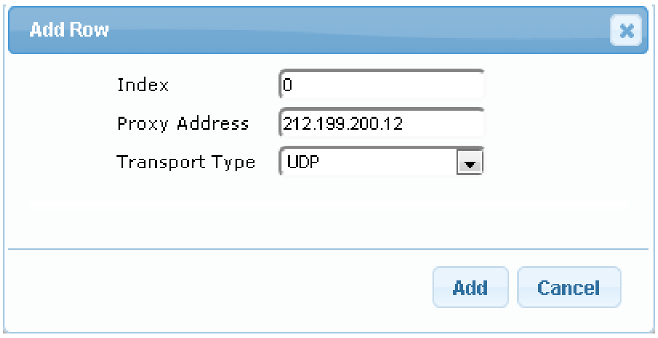
Add Row

To configure the addresses (IP address or FQDN) of the SIP proxy servers, click the 'Proxy Address Table' link located at the bottom of the page under Additional Configuration.

Index	2
SRD	DefaultSRD
Name	Redundant SIP Trunk
Gateway IPv4 SIP Interface	None
SBC IPv4 SIP Interface	WAN
Proxy Keep-Alive	Using OPTIONS
Proxy Keep-Alive Time [sec]	60

   b. Select the table row of the Proxy Set that you added, and then click the **Proxy Address Table** link located below the table.
   c. Add the IP address of the redundant SIP Trunk:

Figure 3-4: Proxy Set Address for Redundant SIP Trunk



Add Row

Index	0
Proxy Address	212.199.200.12
Transport Type	UDP

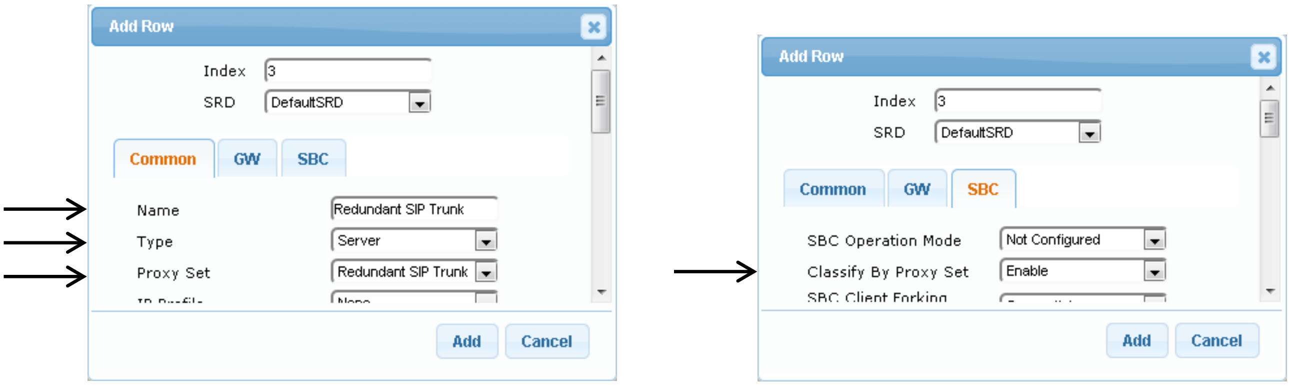
3.1.3 Step 3: Add an IP Group for Redundant SIP Trunk

You need to add an IP Group for the redundant SIP Trunk and assign the Proxy Set that you configured in the previous step to it. Calls received from the SIP Trunk are classified to this IP Group based on the Proxy Set.

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

1. Open the IP Group table (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group Table**).
2. Add an IP Group for the redundant SIP Trunk:

Figure 3-5: IP Group for Redundant SIP Trunk (Common Tab)



Index: 3
SRD: DefaultSRD
Name: Redundant SIP Trunk
Type: Server
Proxy Set: Redundant SIP Trunk
IP Profile: None

Index: 3
SRD: DefaultSRD
SBC Operation Mode: Not Configured
Classify By Proxy Set: Enable
SBC Client Forking

3.1.4 Step 4: Add Alternative IP-to-IP Call Routing Rules

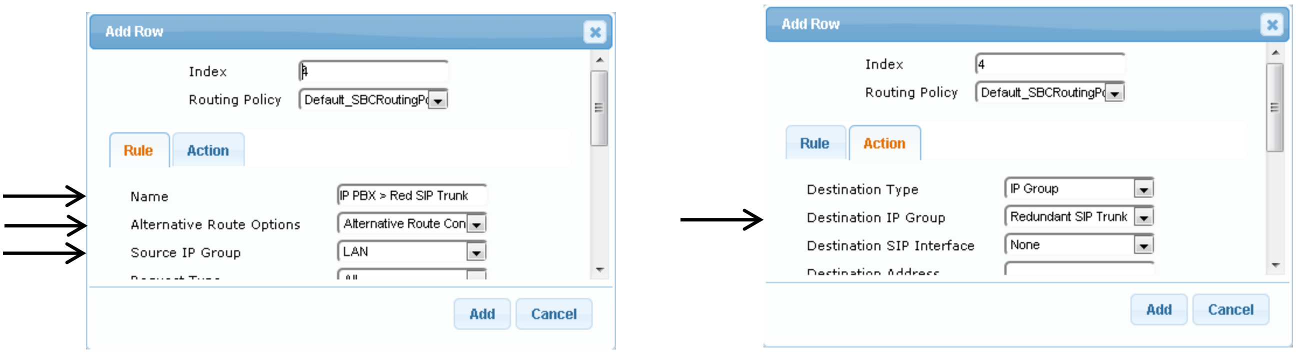
For alternative routing upon main SIP Trunk connectivity failure, you need to add IP-to-IP routing rules for the following routing directions:

- Calls from LAN IP PBX to redundant SIP Trunk upon failure of main SIP Trunk.
- Calls from the redundant SIP Trunk to LAN IP PBX.

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

1. Open the IP-to-IP Routing table (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **IP-to-IP Routing Table**).
2. Add a rule to route calls from the LAN IP PBX to the redundant SIP Trunk:

Figure 3-6: Call Routing Rule from LAN IP PBX to Redundant SIP Trunk



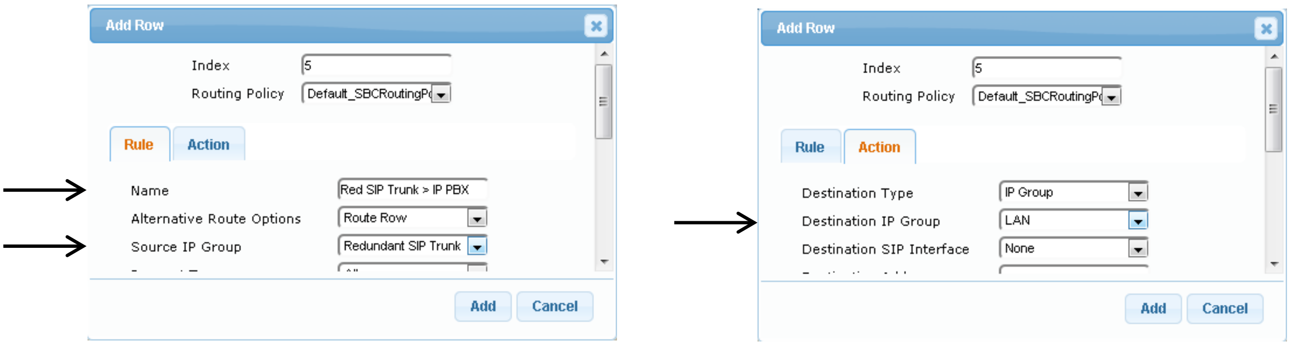
Index: 4
Routing Policy: Default_SBCRoutingP
Name: IP PBX > Red SIP Trunk
Alternative Route Options: Alternative Route Con
Source IP Group: LAN
Request Type: All

Index: 4
Routing Policy: Default_SBCRoutingP
Destination Type: IP Group
Destination IP Group: Redundant SIP Trunk
Destination SIP Interface: None
Destination Address

> **Note:** You must add the alternative routing rule to the table index row that is **immediately below** the row of the LAN IP PBX to main SIP Trunk routing rule, and set the 'Alternative Route Options' parameter to **Alternative Route Consider Inputs**.

3. Add a rule to route calls from the redundant SIP Trunk to the LAN IP PBX (normal routing row):

Figure 3-7: Call Routing Rule from Redundant SIP Trunk to LAN IP PBX

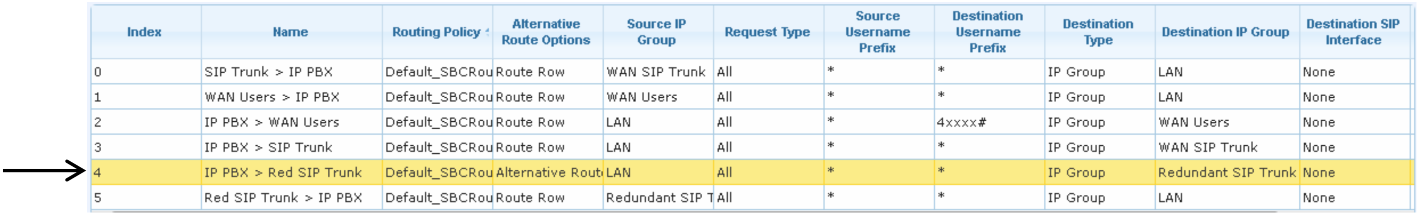


Index	5
Routing Policy	Default_SBCRoutingP
Name	Red SIP Trunk > IP PBX
Alternative Route Options	Route Row
Source IP Group	Redundant SIP Trunk

Index	5
Routing Policy	Default_SBCRoutingP
Destination Type	IP Group
Destination IP Group	LAN
Destination SIP Interface	None

Once you have configured the IP-to-IP routing rules, the IP-to-IP Routing table should appear populated with the alternative routing rule, as shown below:

Figure 3-8: Alternative Call Routing Rule for Redundant SIP Trunk in IP-to-IP Routing Table



Index	Name	Routing Policy	Alternative Route Options	Source IP Group	Request Type	Source Username Prefix	Destination Username Prefix	Destination Type	Destination IP Group	Destination SIP Interface
0	SIP Trunk > IP PBX	Default_SBCRou	Route Row	WAN SIP Trunk	All	*	*	IP Group	LAN	None
1	WAN Users > IP PBX	Default_SBCRou	Route Row	WAN Users	All	*	*	IP Group	LAN	None
2	IP PBX > WAN Users	Default_SBCRou	Route Row	LAN	All	*	4xxxx#	IP Group	WAN Users	None
3	IP PBX > SIP Trunk	Default_SBCRou	Route Row	LAN	All	*	*	IP Group	WAN SIP Trunk	None
4	IP PBX > Red SIP Trunk	Default_SBCRou	Alternative Rout	LAN	All	*	*	IP Group	Redundant SIP Trunk	None
5	Red SIP Trunk > IP PBX	Default_SBCRou	Route Row	Redundant SIP T	All	*	*	IP Group	LAN	None

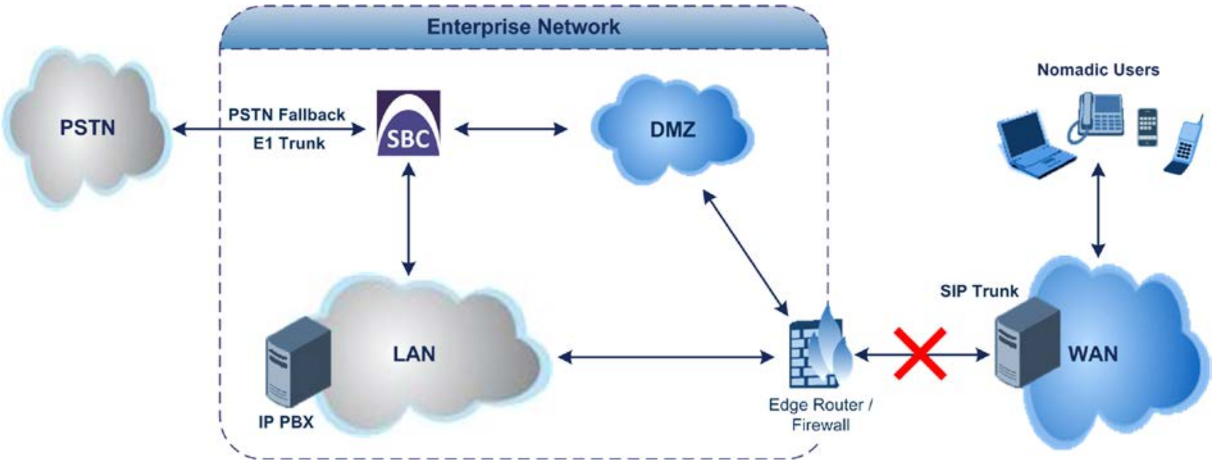
3.2 PSTN Fallback

The example describes how to configure PSTN fallback, whereby upon SIP Trunk connectivity failure, calls from the LAN IP PBX are routed to the PSTN instead of the WAN SIP trunk. The example assumes that the SBC is connected to the local PSTN by an E1 trunk.

> **Note:** The example is applicable only to hybrid SBCs, which also provide optional PSTN interfaces.

The figure below illustrates the topology:

Figure 3-9: PSTN Fallback Example Scenario



You can configure PSTN Fallback using one of two methods, each with its advantages and disadvantages, as listed in the table below. Choose the preferred configuration method based on this criterion.

Table 3-1: Configuration Methods for PSTN Fallback

PSTN Fallback Configuration Method	Advantages	Disadvantages
Optimized Configuration (No Gateway Interface Required)	▪ Quick-and-easy configuration ▪ Each call utilizes only one DSP session	Only partial SBC functionality and features can be applied to the call
Gateway interface configured	All SBC functionality and features (e.g., CAC) can be applied to the call	▪ Complex configuration ▪ Each call utilizes two DSP sessions

3.2.1 PSTN Fallback – Optimized Configuration

The example describes how to configure PSTN fallback using the optimized configuration method.

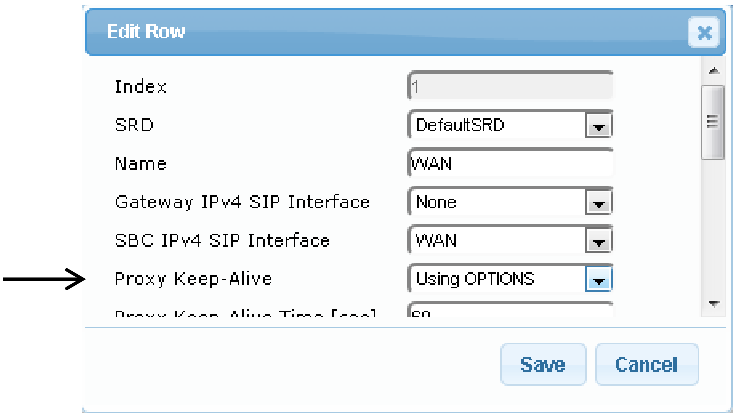
3.2.1.1 Step 1: Enable Keep-Alive for SIP Trunk

The SBC performs PSTN fallback upon connectivity failure with the SIP Trunk. For the device to detect connectivity failure, you need to enable the keep-alive mechanism with the SIP Trunk. The keep-alive mechanism periodically checks connectivity with the SIP Trunk by sending SIP OPTIONS messages.

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

1. Open the Proxy Sets table (**Configuration** tab > **VoIP** menu > **V Network** > **Proxy Sets Table**).
2. Edit Proxy Set "WAN", which you configured for the WAN SIP Trunk (in the previous example – see Section 2.6), to enable proxy keep-alive using SIP OPTIONS messages:

Figure 3-10: Enabling Keep-Alive with Main SIP Trunk



Index	1
SRD	DefaultSRD
Name	WAN
Gateway IPv4 SIP Interface	None
SBC IPv4 SIP Interface	WAN
Proxy Keep-Alive	Using OPTIONS
Proxy Keep-Alive Time [sec]	60

3.2.1.2 Step 2: Add an Alternative IP-to-IP Call Routing Rule for PSTN Fallback

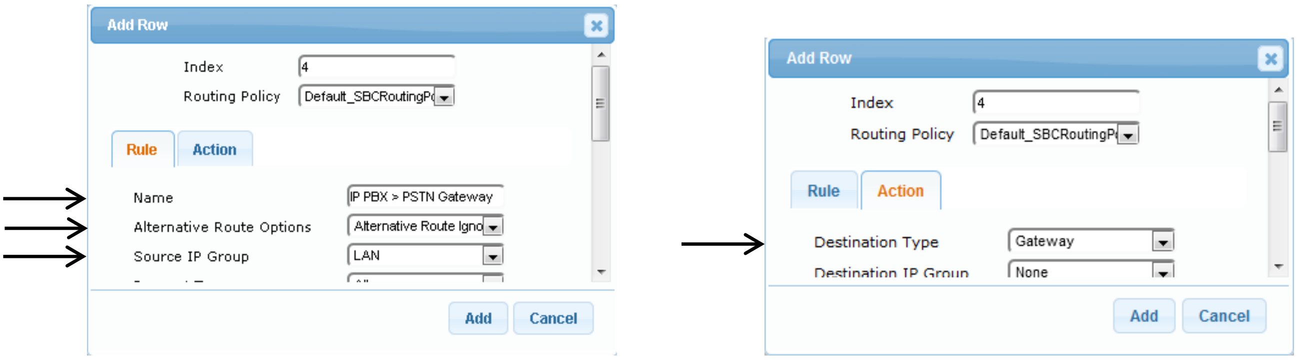
For alternative routing upon SIP Trunk connectivity failure, you need to add an alternative IP-to-IP routing rule to re-route calls from the LAN IP PBX to the PSTN Gateway, instead of to the SIP Trunk. In this configuration method, the destination type is configured to **Gateway**.

Note: You must add the alternative routing rule to the table index row that is immediately below the row of the LAN IP PBX to SIP Trunk routing rule, and set the 'Alternative Route Options' parameter to **Alternative Route Consider Inputs**.

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

1. Open the IP-to-IP Routing table (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **IP-to-IP Routing Table**).
2. Add a rule to route calls from the LAN IP PBX to the PSTN:

Figure 3-11: Call Routing Rule from LAN IP PBX to PSTN Gateway



Add Row

Index: 4
Routing Policy: Default_SBCRoutingPo

Rule | Action

Name: IP PBX > PSTN Gateway
Alternative Route Options: Alternative Route Igno
Source IP Group: LAN

Add Row

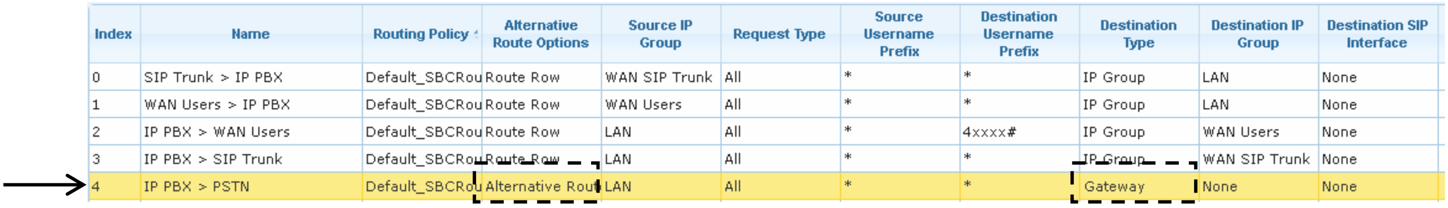
Index: 4
Routing Policy: Default_SBCRoutingPo

Rule | Action

Destination Type: Gateway
Destination IP Group: None

The figure below shows the IP-to-IP Routing table with the configured alternative routing rule:

Figure 3-12: IP-to-IP Call Routing Rule for PSTN Fallback



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
0	SIP Trunk > IP PBX	Default_SBCRou	Route Row	WAN SIP Trunk	All	*	*	IP Group	LAN	None
1	WAN Users > IP PBX	Default_SBCRou	Route Row	WAN Users	All	*	*	IP Group	LAN	None
2	IP PBX > WAN Users	Default_SBCRou	Route Row	LAN	All	*	4xxxx#	IP Group	WAN Users	None
3	IP PBX > SIP Trunk	Default_SBCRou	Route Row	LAN	All	*	*	IP Group	WAN SIP Trunk	None
4	IP PBX > PSTN	Default_SBCRou	Alternative Rout	LAN	All	*	*	Gateway	None	None

3.2.1.3 Step 3: Assign a Trunk Group to the E1 Trunk

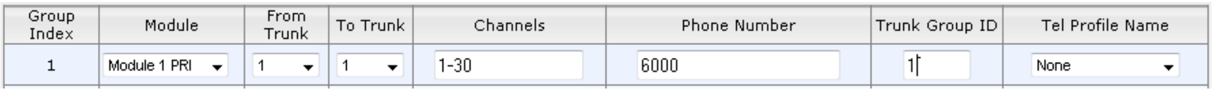
The example includes an E1 trunk that is connected between the SBC and PSTN. To route calls to the trunk, you first need to configure the trunk with a Trunk Group ID. A Trunk Group is a logical group of trunks (spans) as well as channels pertaining to these trunks.

The example assumes that you have already configured the E1 protocol settings for the trunk. The main trunk settings are done in the Trunk Settings page (**Configuration** tab > **VoIP** menu > **PSTN** > **Trunk Settings**). For more information, refer to the *User's Manual*.

➢ **To assign a Trunk Group to the E1 trunk:**

1. Open the Trunk Group table (**Configuration** tab > **VoIP** menu > **Gateway** > **Trunk Group** > **Trunk Group**).
2. Assign Trunk Group ID 1 to the trunk:

Figure 3-13: Assigning Trunk Group ID to E1 Trunk



Group Index	Module	From Trunk	To Trunk	Channels	Phone Number	Trunk Group ID	Tel Profile Name
1	Module 1 PRI	1	1	1-30	6000	1	None

Note: The 'Phone Number' parameter is only a logical value for enabling the Trunk Group and thus, can be any numerical value.

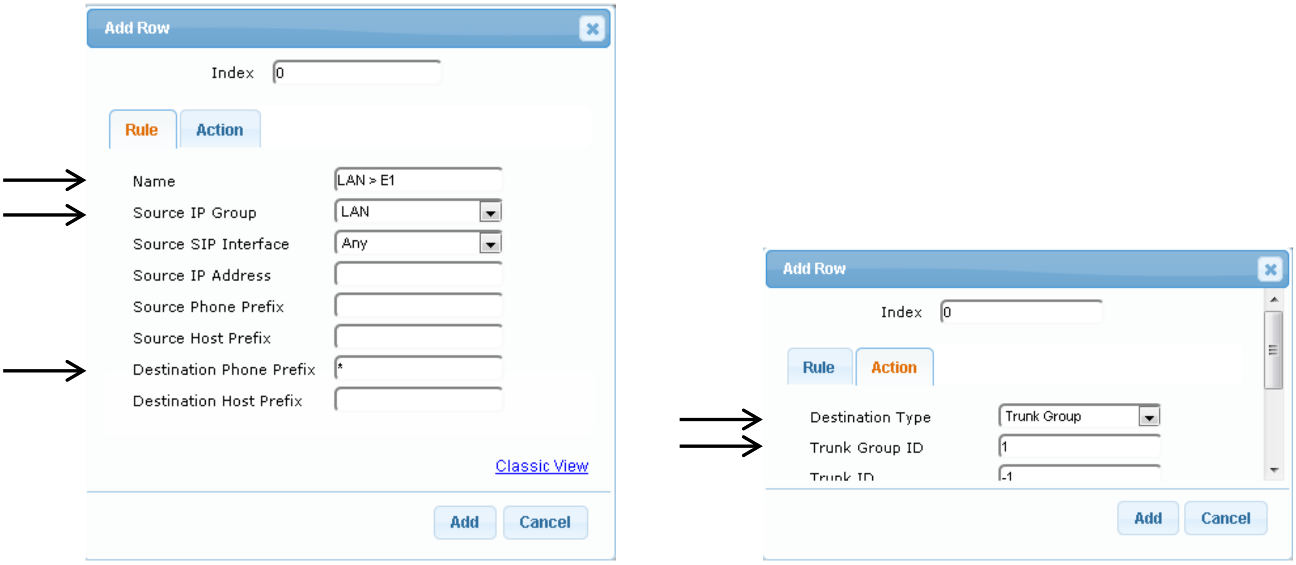
3.2.1.4 Step 4: Add an IP-to-Trunk Group Routing Rule

For call routing from the IP PBX to the E1 trunk, you need to configure an IP-to-Trunk Group routing rule. In other words, you need to route calls from the IP Group of the IP PBX ("LAN") to the Trunk Group that you configured for the E1 trunk (i.e., ID 1).

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

1. Open the IP to Trunk Group Routing table (**Configuration** tab > **VoIP** menu > **Gateway** > **Routing** > **IP to Trunk Group Routing**).
2. Add a rule to route calls from the IP PBX to the Trunk Group:

Figure 3-14: IP-to-Trunk Group Call Routing Rule



Index: 0

Name: LAN > E1
Source IP Group: LAN
Source SIP Interface: Any
Source IP Address:
Source Phone Prefix:
Source Host Prefix:
Destination Phone Prefix: *
Destination Host Prefix:

Index: 0

Destination Type: Trunk Group
Trunk Group ID: 1
Trunk ID: -1

Note: The asterisk (*) value of the 'Destination Phone Prefix' parameter denotes all dialed calls.

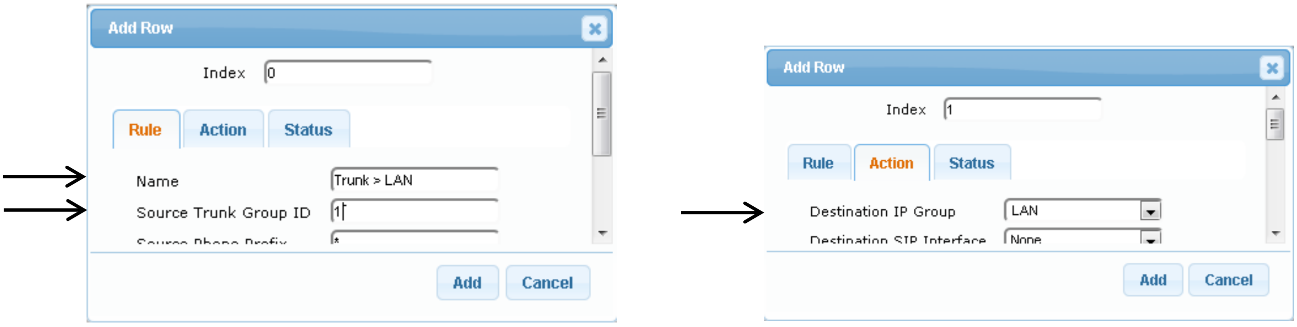
3.2.1.5 Step 5: Add a Tel-to-IP Routing Rule

To receive calls from the PSTN, you need to add a rule to route calls received on the E1 trunk (i.e., Trunk Group ID 1) to the IP PBX.

➢ To add a Tel-to-IP routing rule:

1. Open the Tel to IP Routing table (**Configuration** tab > **VoIP** menu > **Gateway** > **Routing** > **Tel to IP Routing**).
2. Add a rule to route calls from the Trunk Group to the SBC LAN:

Figure 3-15: Tel-to-IP Call Routing Rule



Index: 0

Name: Trunk > LAN
Source Trunk Group ID: 1
Source Phone Prefix: *

Index: 1

Destination IP Group: LAN
Destination SIP Interface: None

3.2.2 PSTN Fallback through the Gateway Application

This method uses the Gateway application to send the call to the PSTN. In other words, the initial SBC call is first routed to the interface of the Gateway application, and only then routed to the PSTN.

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., Gateway 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.

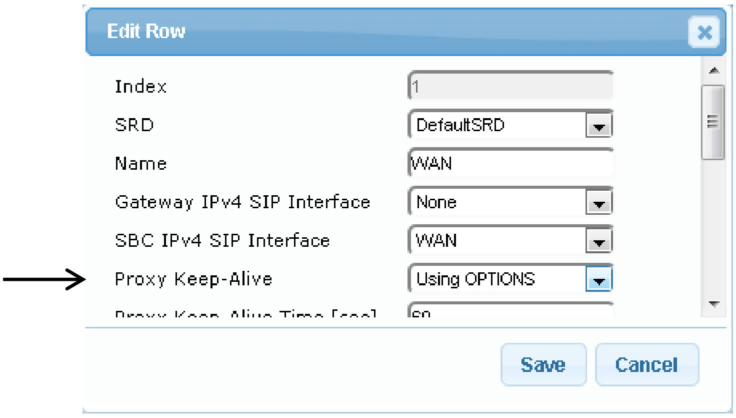
3.2.2.1 Step 1: Enable Keep-Alive for SIP Trunk

The SBC performs PSTN fallback upon connectivity failure with the SIP Trunk. For the device to detect connectivity failure with the SIP Trunk, you need to enable the keep-alive mechanism with the SIP Trunk. The keep-alive mechanism periodically checks connectivity by sending SIP OPTIONS messages.

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

1. Open the Proxy Sets table (**Configuration** tab > **VoIP** menu > **V Network** > **Proxy Sets Table**).
2. Edit Proxy Set "WAN", which you configured for the WAN SIP Trunk (in the previous example – see Section 2.6), to enable proxy keep-alive using SIP OPTIONS messages:

Figure 3-16: Enabling Keep-Alive with Main SIP Trunk



Edit Row

Index	1
SRD	DefaultSRD
Name	WAN
Gateway IPv4 SIP Interface	None
SBC IPv4 SIP Interface	WAN
Proxy Keep-Alive	Using OPTIONS
Proxy Keep-Alive Time [sec]	60

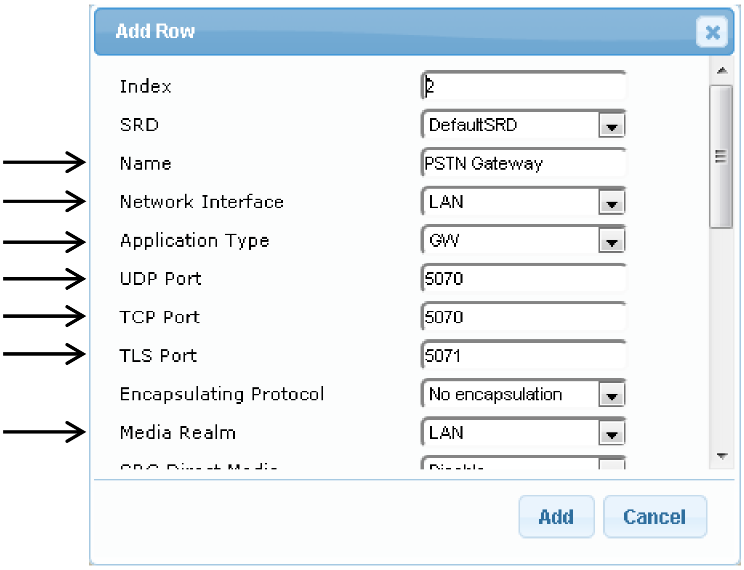
3.2.2.2 Step 2: Add a SIP Interface for PSTN Gateway

You need to add a SIP Interface for the Gateway application. The SIP Interface is used for the listening port of SIP messages destined to the Gateway application.

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

1. Open the SIP Interface table (**Configuration** tab > **VoIP** menu > **VoIP Network** > **SIP Interface Table**).
2. Add a SIP Interface for the Gateway application:

Figure 3-17: SIP Interface for Gateway Application



Index	2
SRD	DefaultSRD
Name	PSTN Gateway
Network Interface	LAN
Application Type	GW
UDP Port	5070
TCP Port	5070
TLS Port	5071
Encapsulating Protocol	No encapsulation
Media Realm	LAN
SBC Direct Media	Disable

Notes:

- As the SIP Interface is for the LAN, it is assigned the "LAN" interface.
- The 'Application Type' parameter defines that it's for the Gateway application.

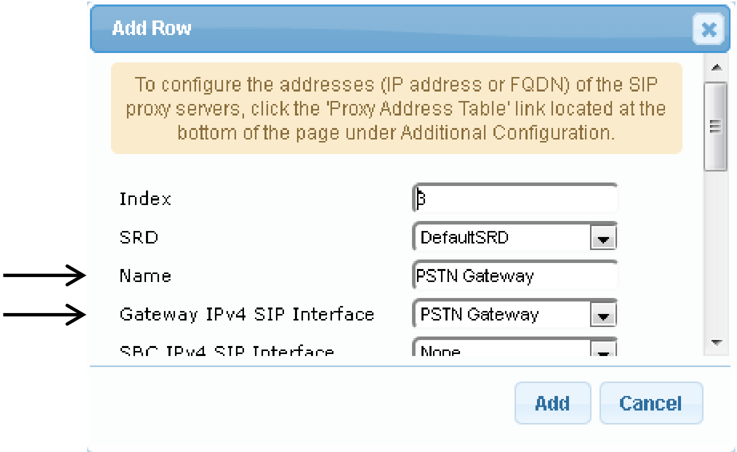
3.2.2.3 Step 3: Add a Proxy Set for PSTN Gateway

You need to add a Proxy Set for the PSTN Gateway. The proxy's address is the IP address of the LAN interface (i.e., 10.33.4.11). In other words, the SBC will route the call to this address.

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

1. Open the Proxy Sets table (**Configuration** tab > **VoIP** menu > **VoIP Network** > **Proxy Sets Table**).
2. Add a Proxy Set for the PSTN Gateway:
   a. Add the Proxy Set:

Figure 3-18: Proxy Set for PSTN Gateway

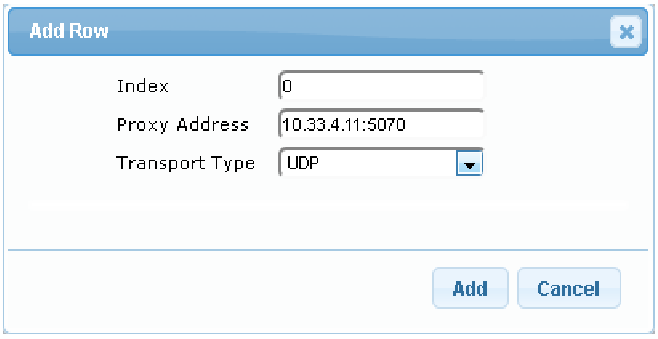


To configure the addresses (IP address or FQDN) of the SIP proxy servers, click the 'Proxy Address Table' link located at the bottom of the page under Additional Configuration.

Index: 3
SRD: DefaultSRD
Name: PSTN Gateway
Gateway IPv4 SIP Interface: PSTN Gateway
SBC IPv4 SIP Interface: None

   b. Select the table row of the Proxy Set that you added, and then click the **Proxy Address Table** link located below the table.
   c. Add the IP address of the PSTN Gateway:

Figure 3-19: Proxy Set Address for PSTN Gateway



Index: 0
Proxy Address: 10.33.4.11:5070
Transport Type: UDP

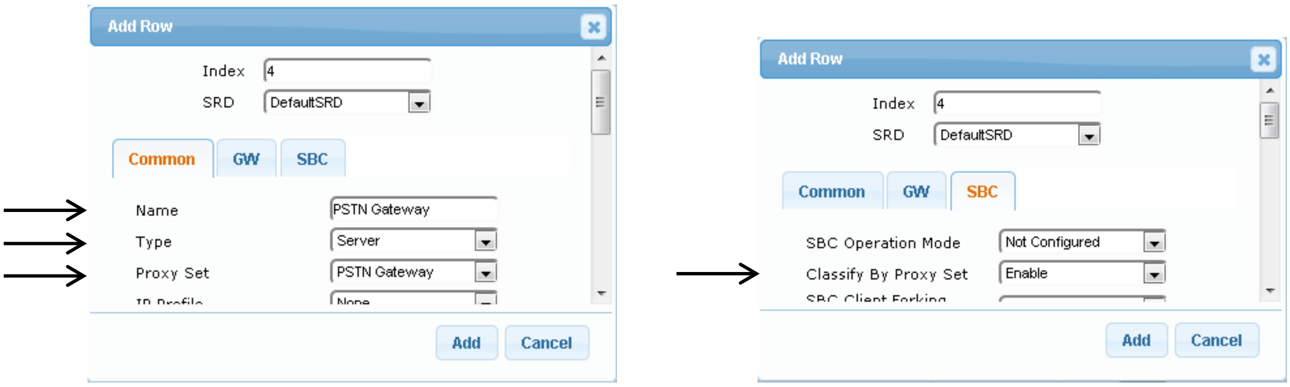
3.2.2.4 Step 4: Add an IP Group for PSTN Gateway

To route the initial SBC call to the Gateway application, 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 (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group Table**).
2. Add an IP Group for the PSTN Gateway:

Figure 3-20: IP Group for PSTN Gateway



Index 4
SRD DefaultSRD
Name PSTN Gateway
Type Server
Proxy Set PSTN Gateway
IP Profile None

Index 4
SRD DefaultSRD
SBC Operation Mode Not Configured
Classify By Proxy Set Enable
SBC Client Forking

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

For alternative routing upon SIP Trunk connectivity failure, you need to add IP-to-IP routing rules for the following routing directions:

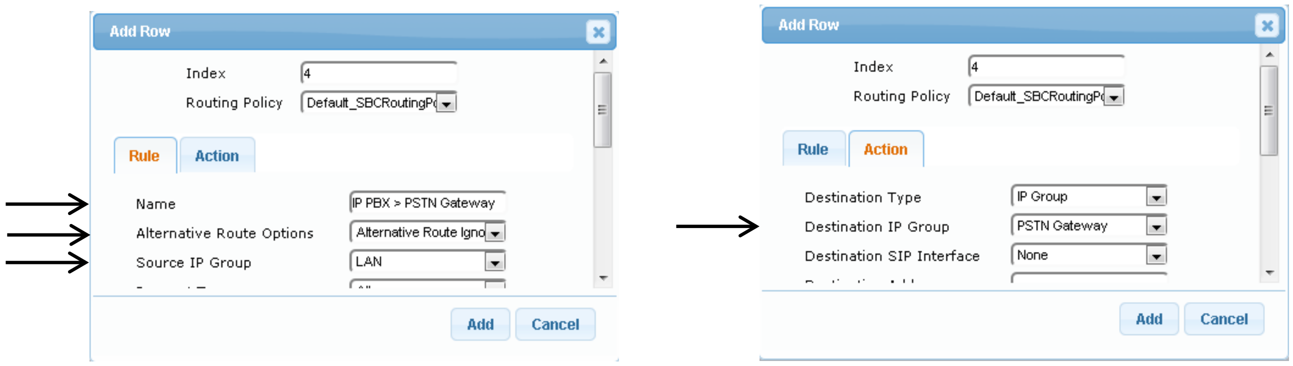
- Calls from the LAN IP PBX to PSTN Gateway, upon SIP Trunk connectivity failure.
- Calls from the PSTN Gateway to the LAN IP PBX.

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

1. Open the IP-to-IP Routing table (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **IP-to-IP Routing Table**).
2. Add a rule to route calls from the LAN IP PBX to the PSTN Gateway:

Note: You must add the alternative routing rule to the table index row that is **immediately below** the row of the LAN IP PBX to SIP Trunk routing rule, and set the 'Alternative Route Options' parameter to **Alternative Route Consider Inputs**.

Figure 3-21: Call Routing Rule from LAN IP PBX to PSTN Gateway

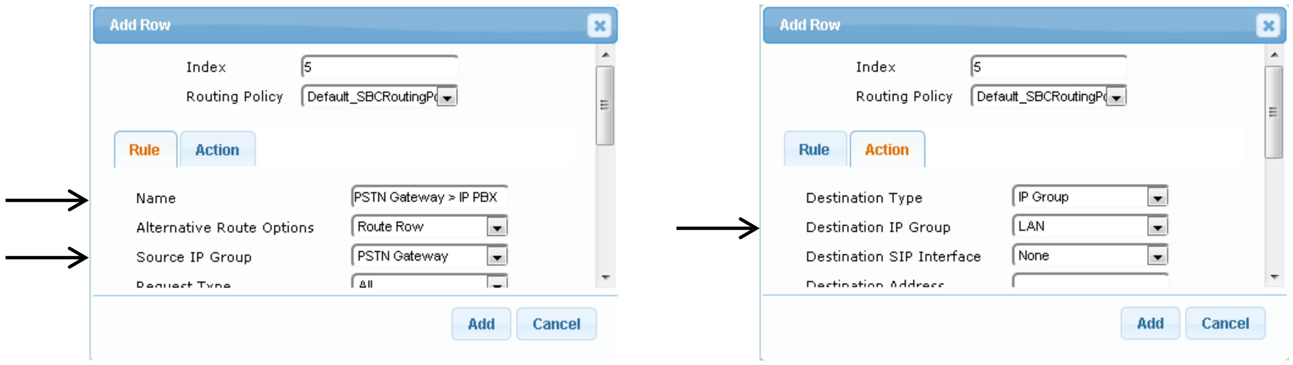


Index	4
Routing Policy	Default_SBCRoutingP
Name	IP PBX > PSTN Gateway
Alternative Route Options	Alternative Route Igno
Source IP Group	LAN

Index	4
Routing Policy	Default_SBCRoutingP
Destination Type	IP Group
Destination IP Group	PSTN Gateway
Destination SIP Interface	None

3. Add a rule to route calls from the PSTN Gateway to LAN IP PBX:

Figure 3-22: Call Routing Rule from PSTN Gateway to LAN IP PBX

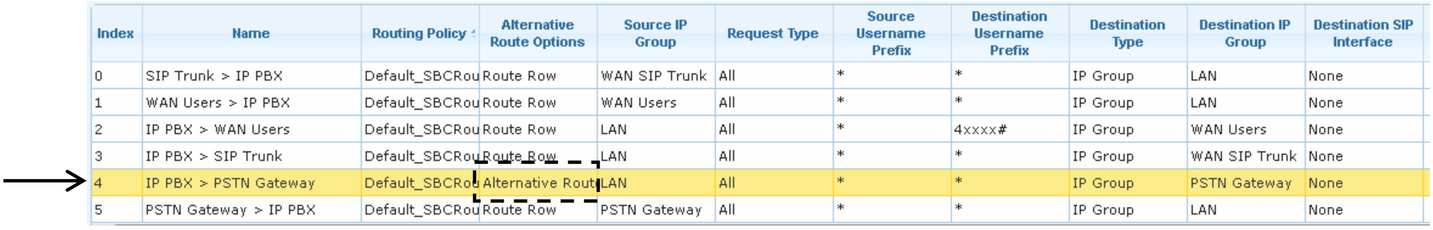


Index	5
Routing Policy	Default_SBCRoutingP
Name	PSTN Gateway > IP PBX
Alternative Route Options	Route Row
Source IP Group	PSTN Gateway
Request Type	All

Index	5
Routing Policy	Default_SBCRoutingP
Destination Type	IP Group
Destination IP Group	LAN
Destination SIP Interface	None
Destination Address	

The figure below shows the IP-to-IP Routing table with the configured alternative routing rule:

Figure 3-23: IP-to-IP Call Routing Rule for PSTN Fallback



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
0	SIP Trunk > IP PBX	Default_SBCRou	Route Row	WAN SIP Trunk	All	*	*	IP Group	LAN	None
1	WAN Users > IP PBX	Default_SBCRou	Route Row	WAN Users	All	*	*	IP Group	LAN	None
2	IP PBX > WAN Users	Default_SBCRou	Route Row	LAN	All	*	4xxxx#	IP Group	WAN Users	None
3	IP PBX > SIP Trunk	Default_SBCRou	Route Row	LAN	All	*	*	IP Group	WAN SIP Trunk	None
4	IP PBX > PSTN Gateway	Default_SBCRou	Alternative Rout	LAN	All	*	*	IP Group	PSTN Gateway	None
5	PSTN Gateway > IP PBX	Default_SBCRou	Route Row	PSTN Gateway	All	*	*	IP Group	LAN	None

3.2.2.6 Step 6: Assign a Trunk Group to the E1 Trunk

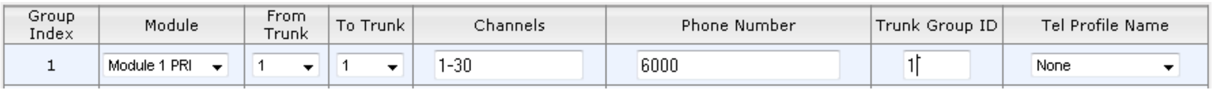
The example includes an E1 trunk that is connected between the SBC and PSTN. To route calls to the trunk, you first need to configure the trunk with a Trunk Group ID. A Trunk Group is a logical group of trunks (spans) as well as channels pertaining to these trunks.

The example assumes that you have already configured the E1 protocol settings for the trunk. The main trunk settings are done in the Trunk Settings page (**Configuration** tab > **VoIP** menu > **PSTN** > **Trunk Settings**). For more information, refer to the *User's Manual*.

➢ **To assign a Trunk Group to the E1 trunk:**

1. Open the Trunk Group table (**Configuration** tab > **VoIP** menu > **Gateway** > **Trunk Group** > **Trunk Group**).
2. Assign Trunk Group ID 1 to the trunk:

Figure 3-24: Assigning Trunk Group ID to E1 Trunk



Group Index	Module	From Trunk	To Trunk	Channels	Phone Number	Trunk Group ID	Tel Profile Name
1	Module 1 PRI	1	1	1-30	6000	1	None

Note: The 'Phone Number' parameter is only a logical value for enabling the Trunk Group and thus, can be any numerical value.

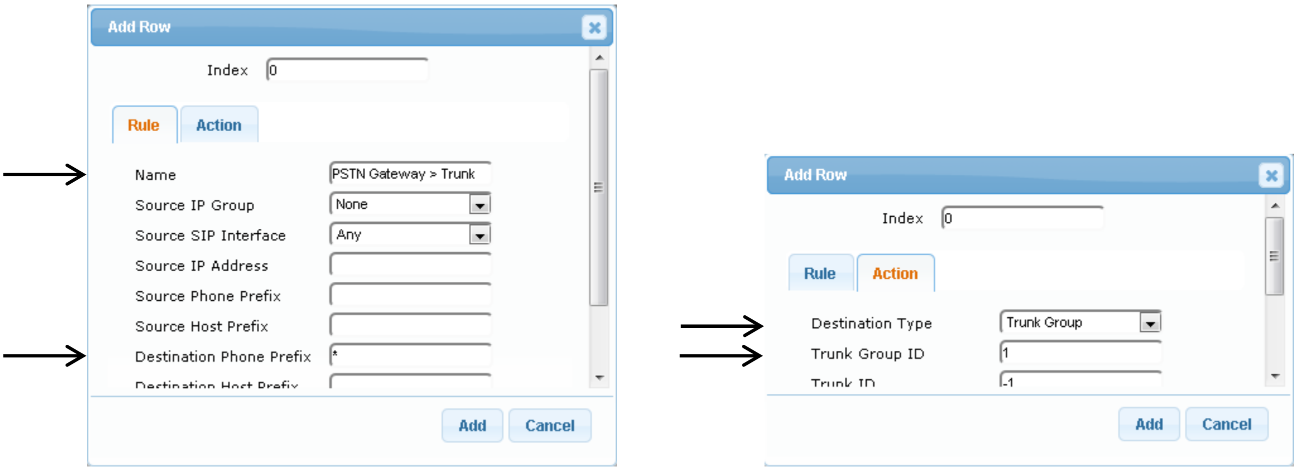
3.2.2.7 Step 7: Add an IP-to-Trunk Group Routing Rule

For call routing from the PSTN Gateway to the E1 trunk, you need to configure an IP-to-Trunk Group routing rule. In other words, you need to route calls from the IP Group that you configured for the PSTN Gateway (i.e., "PSTN Gateway") to the Trunk Group that you assigned the E1 trunk (i.e., ID 1).

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

1. Open the IP to Trunk Group Routing table (**Configuration** tab > **VoIP** menu > **Gateway** > **Routing** > **IP to Trunk Group Routing**).
2. Add a rule to route calls from the PSTN Gateway to the PSTN:

Figure 3-25: IP-to-Trunk Group Call Routing Rule



Index: 0

Name: PSTN Gateway > Trunk
Source IP Group: None
Source SIP Interface: Any
Source IP Address:
Source Phone Prefix:
Source Host Prefix:
Destination Phone Prefix: *
Destination Host Prefix:

Index: 0

Destination Type: Trunk Group
Trunk Group ID: 1
Trunk ID: -1

Note: The asterisk (*) value of the 'Destination Phone Prefix' parameter denotes all dialed calls and therefore, there is no need to specify the source IP Group.

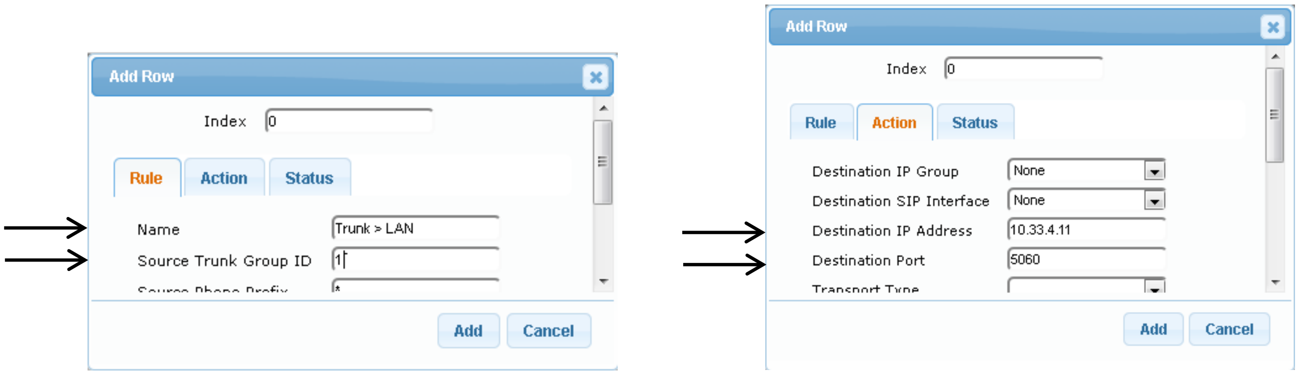
3.2.2.8 Step 8: Add a Tel-to-IP Routing Rule

To receive calls from the PSTN, you need to add a rule to route calls received on the E1 trunk (i.e., Trunk Group ID 1) to the SBC application. The SBC application address is the LAN network interface (i.e., 10.33.4.11:5060).

➢ **To add a Tel-to-IP routing rule:**

1. Open the Tel to IP Routing table (**Configuration** tab > **VoIP** menu > **Gateway** > **Routing** > **Tel to IP Routing**).
2. Add a rule to route calls from the Trunk Group to the SBC LAN:

Figure 3-26: Tel-to-IP Call Routing Rule



Index: 0
Name: Trunk > LAN
Source Trunk Group ID: 1
Source Phone Prefix: *

Index: 0
Destination IP Group: None
Destination SIP Interface: None
Destination IP Address: 10.33.4.11
Destination Port: 5060
Transport Type:

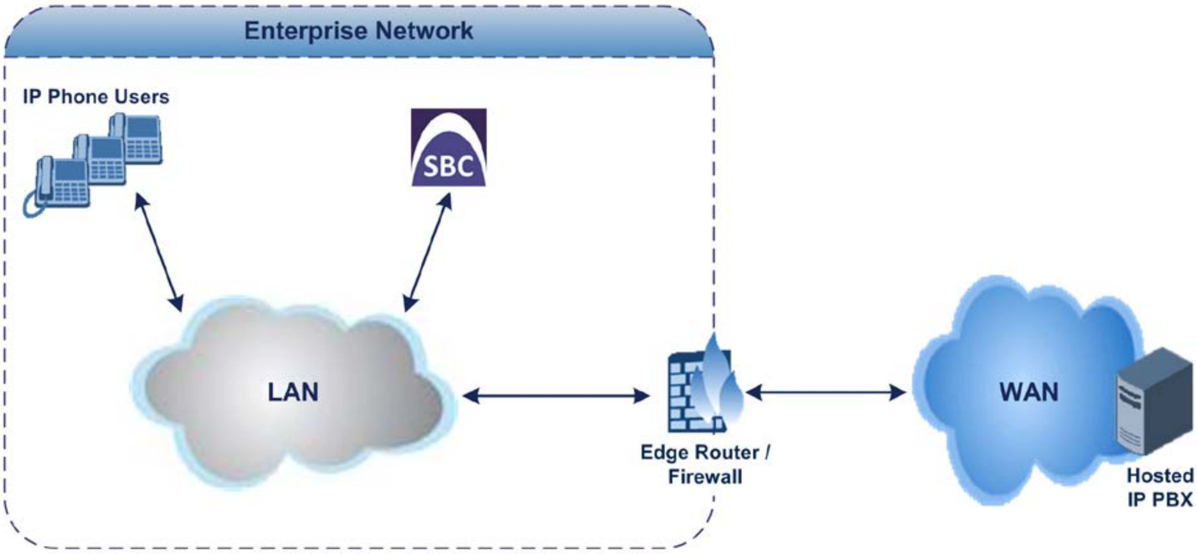
4 Hosted WAN IP PBX

The example describes how to configure the SBC when interworking between LAN IP phones and a hosted WAN IP PBX. The example scenario includes the following topology architecture:

- **Application:**
  - LAN IP phone users located behind NAT.
  - Hosted WAN IP PBX with IP address of 212.199.200.10.

  The figure below illustrates the application of the example scenario:

Figure 4-1: Hosted IP PBX Example - Application Topology



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

    The example employs one logical network interface using IP address 10.33.4.11. The interface is used for communicating with the LAN and WAN. Two sip Interfaces are required to resolve NAT traversal. As the SBC uses only one logical interface, it separates the traffic between the LAN and WAN using different logical ports defined per SIP Interface. The IP phones communicate with the SBC using port 5060; the edge router forwards messages from the hosted IP PBX to the SBC using port 5070.
  - **NAT Traversal:**

    When the SBC sends messages to the hosted IP PBX, it uses the public IP address of the edge router (212.199.200.90), instead of 10.33.4.11.

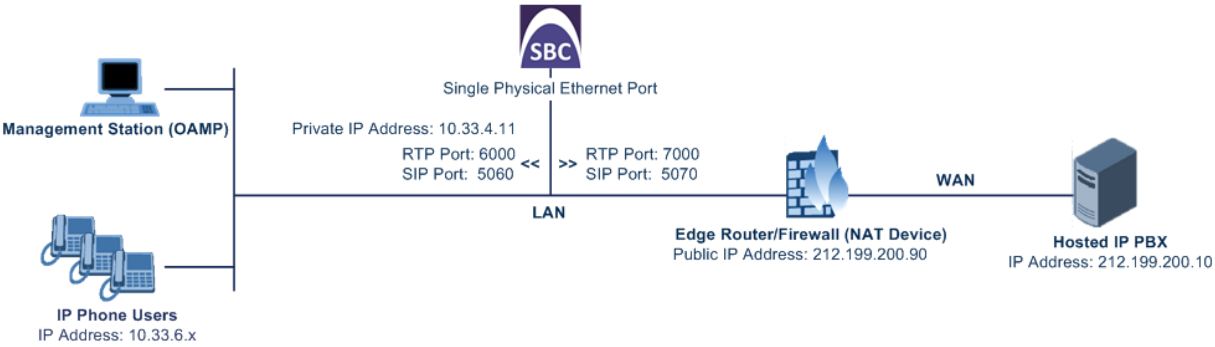
Note: You must configure port forwarding on the edge router to forward messages from the WAN to the SBC. Based on the example scenario, for SIP signaling you need to set the SIP Interface port to 5070.

  - **Physical LAN Port Connections:**

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

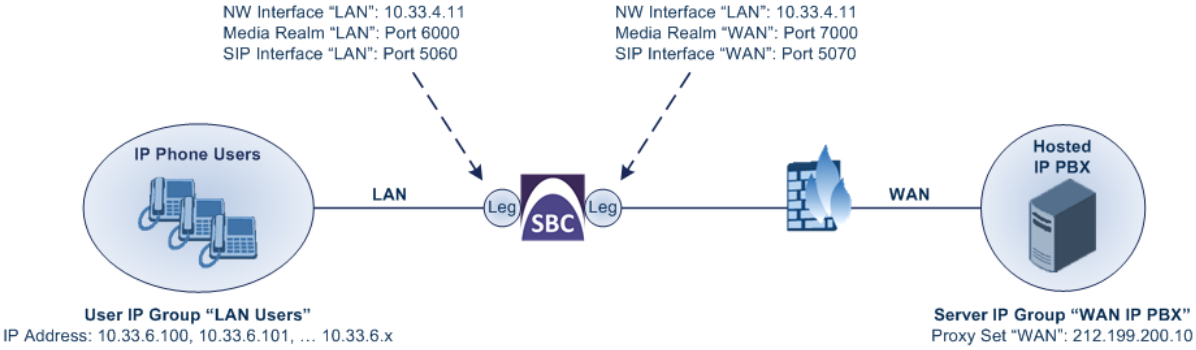
The SBC's logical network interfaces and LAN port connection is illustrated in the following figure:

Figure 4-2: SBC Logical Interfaces and Physical Port Connection Example


SBC
Single Physical Ethernet Port
Management Station (OAMP)
Private IP Address: 10.33.4.11
RTP Port: 6000
SIP Port: 5060
<<
>>
RTP Port: 7000
SIP Port: 5070
WAN
LAN
Edge Router/Firewall (NAT Device)
Public IP Address: 212.199.200.90
Hosted IP PBX
IP Address: 212.199.200.10
IP Phone Users
IP Address: 10.33.6.x

The main configuration entities required in the example are shown below:

Figure 4-3: Required Configuration Entities

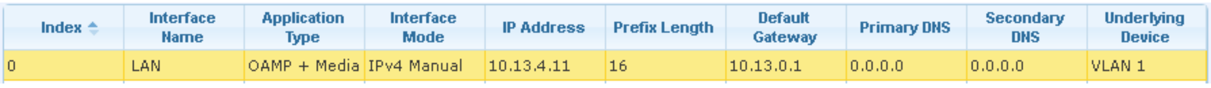

NW Interface "LAN": 10.33.4.11
Media Realm "LAN": Port 6000
SIP Interface "LAN": Port 5060
NW Interface "LAN": 10.33.4.11
Media Realm "WAN": Port 7000
SIP Interface "WAN": Port 5070
IP Phone Users
LAN
Leg
SBC
Leg
WAN
Hosted IP PBX
User IP Group "LAN Users"
IP Address: 10.33.6.100, 10.33.6.101, ... 10.33.6.x
Server IP Group "WAN IP PBX"
Proxy Set "WAN": 212.199.200.10

Note: For clarity, whenever configuring the various configuration entities in the example (e.g., SIP Interfaces and IP Groups), table rows with the name "LAN" are used for the SBC leg interfacing with the LAN IP phone users; table rows with the name "WAN" are used for the SBC leg interfacing with the WAN hosted IP PBX.

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

The example employs only one logical network interface (10.33.4.11), which is used for the LAN, WAN, and management (i.e., OAMP). The example assumes that the interface is already setup and thus, additional configuration is unnecessary.

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



Index	Interface Name	Application Type	Interface Mode	IP Address	Prefix Length	Default Gateway	Primary DNS	Secondary DNS	Underlying Device
0	LAN	OAMP + Media	IPv4 Manual	10.13.4.11	16	10.13.0.1	0.0.0.0	0.0.0.0	VLAN 1

Note: You can change the physical port assigned to the network interface ('Underlying Device'). For a description on how to do this, see the example in Section 2.

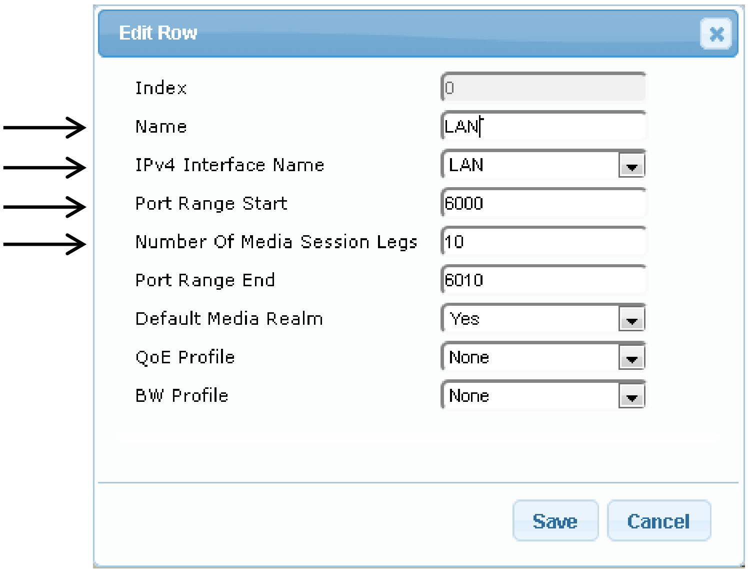
4.2 Step 2: Add Media Realms for LAN and WAN

In the example, you need to configure Media Realms for LAN traffic (IP phone users) and WAN traffic (hosted IP PBX). You will later apply the Media Realms to your VoIP network by assigning them to SIP Interfaces (see Section 2.5).

➢ **To add Media Realms:**

1. Open the Media Realm table (**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:

Figure 4-5: Media Realm for LAN Interface

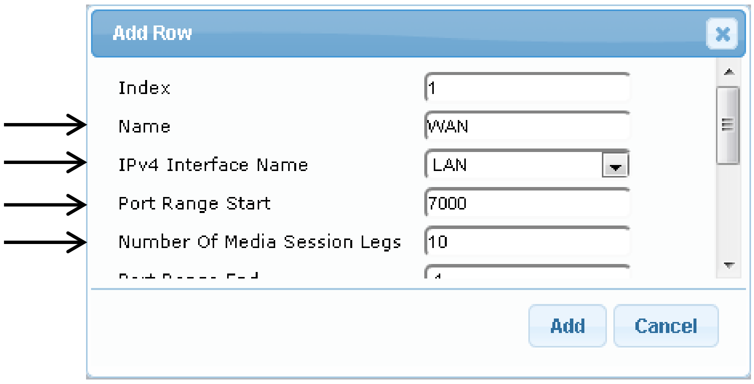


Edit Row

Index	0
Name	LAN
IPv4 Interface Name	LAN
Port Range Start	6000
Number Of Media Session Legs	10
Port Range End	6010
Default Media Realm	Yes
QoE Profile	None
BW Profile	None

3. Add a Media Realm for the WAN interface:

Figure 4-6: Media Realm for WAN Interface



Index	1
Name	WAN
IPv4 Interface Name	LAN
Port Range Start	7000
Number Of Media Session Legs	10
Port Range End	1

Note: The 'Port Range End' parameter's value is automatically calculated (based on start port range and number of sessions) when you click **Add** in the dialog box.

4.3 Step 3: Add SIP Interfaces for LAN and WAN

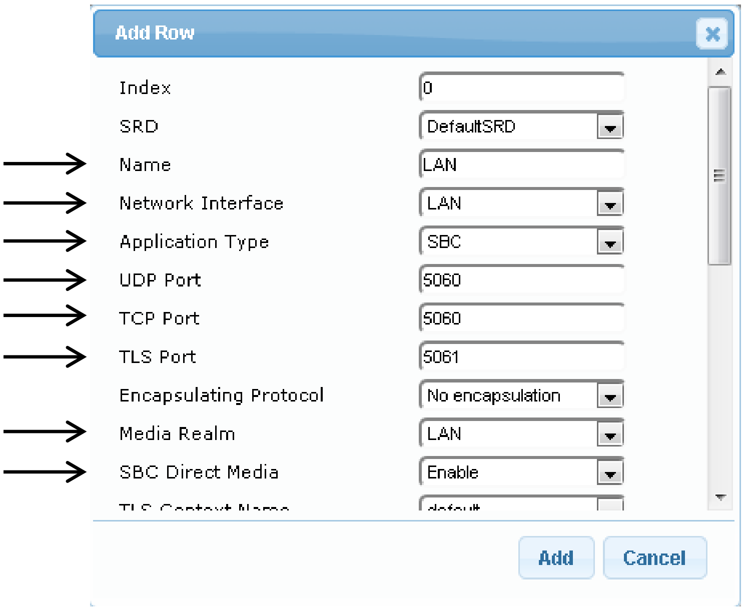
In the example, you need to add two SIP Interfaces - one for LAN and one for WAN. Two different SIP Interfaces, even though on the same logical LAN interface, are used to overcome NAT traversal. As the SBC uses only one logical interface, it separates the traffic between the LAN and WAN using different logical ports defined by each SIP Interface. The IP phones communicate with the SBC using port 5060, and the edge router forwards the SIP messages from the hosted IP PBX to the SBC using port 5070.

Notes: As the LAN users reside on the same LAN network, to reduce bandwidth usage and SBC resources, the media (RTP) path can be configured to flow directly between the LAN users without traversing the SBC. In this setup, only the SIP signaling traverses the SBC. This is referred to as *direct media* (or non-Media Anchoring). The 'SBC Direct Media' parameter in the SIP Interface table (see below) is used to enable the functionality.

➢ To add SIP Interfaces:

1. Open the SIP Interface table (**Configuration** tab > **VoIP** menu > **VoIP Network** > **SIP Interface Table**).
2. Add a SIP Interface for the LAN interface:

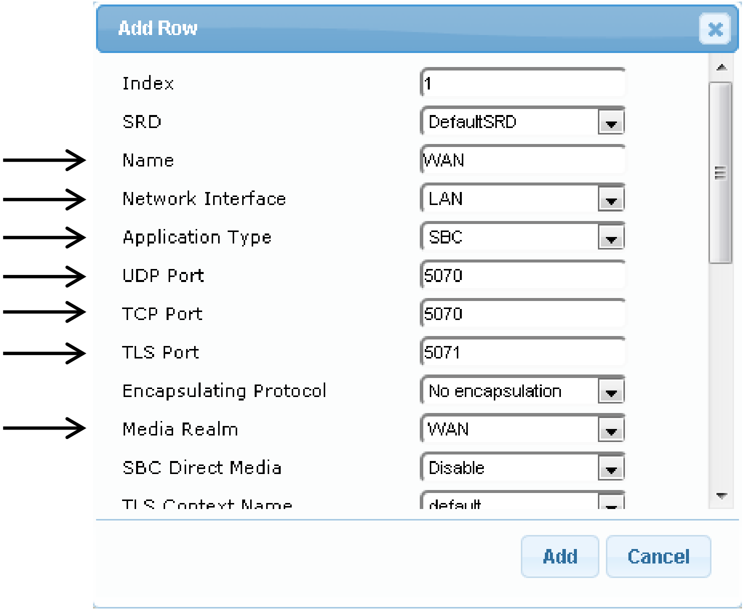
Figure 4-7: SIP Interface for LAN



Index	0
SRD	DefaultSRD
Name	LAN
Network Interface	LAN
Application Type	SBC
UDP Port	5060
TCP Port	5060
TLS Port	5061
Encapsulating Protocol	No encapsulation
Media Realm	LAN
SBC Direct Media	Enable
TLS Context Name	default

3. Add a SIP Interface for the WAN interface:

Figure 4-8: SIP Interface for WAN



Index	1
SRD	DefaultSRD
Name	WAN
Network Interface	LAN
Application Type	SBC
UDP Port	5070
TCP Port	5070
TLS Port	5071
Encapsulating Protocol	No encapsulation
Media Realm	WAN
SBC Direct Media	Disable
TLS Context Name	default

4.4 Step 4: Configure a NAT Translation Rule

As the SBC is located behind NAT, you need to configure it for NAT traversal. When the SBC sends SIP messages to the hosted IP PBX, it uses its' NAT traversal mechanism to replace the source IP address (i.e., IP address of the LAN users) with a public IP address.

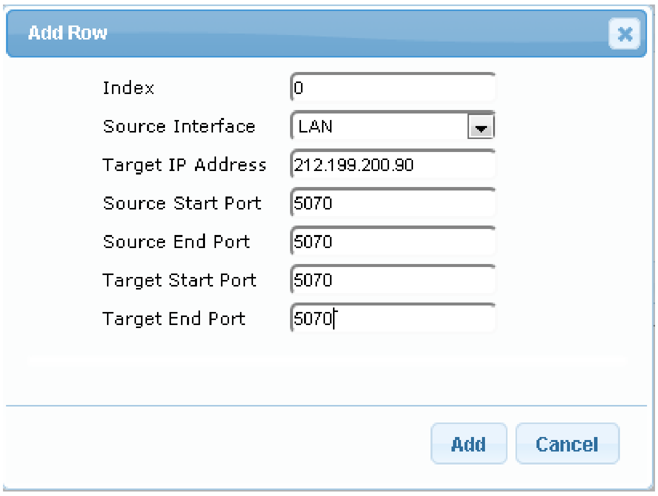
If the SBC were configured with two IP network interfaces (e.g., one LAN and one WAN), only one NAT rule would be required. The NAT rule would be configured for the network interface representing the WAN, with a public IP address but without specifying ports. However, our example uses only one network interface and therefore, you need to specify ports in order to differentiate between the LAN and WAN SIP Interfaces. In this case, the SBC will only replace the source IP address of messages sent on the WAN SIP Interface (i.e., "WAN") and not LAN SIP Interface (i.e., "LAN"). Thus, you need to add the following NAT rules:

- NAT rule for SIP messages with source port 5070, which you configured for the WAN SIP Interface in Section 4.3
- NAT rule for SIP messages with SDP source port 7000-7090, which you configured for the WAN Media Realm in Section 4.2

➢ To add NAT translation rules:

1. Open the NAT Translation table (**Configuration** tab > **VoIP** menu > **VoIP Network** > **NAT Translation Table**).
2. Add a NAT rule for SIP messages:

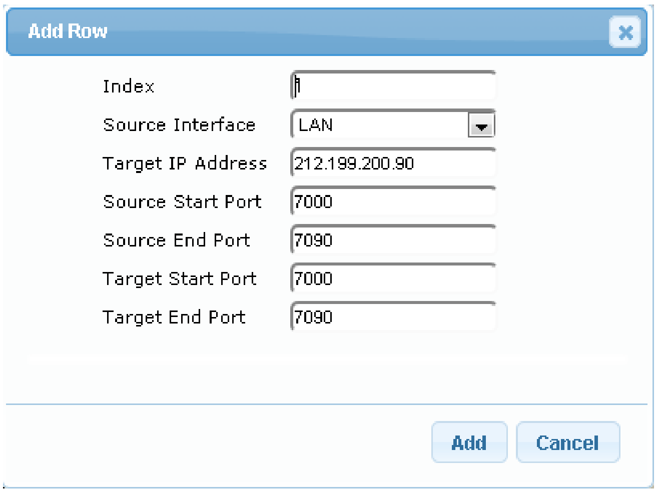
Figure 4-9: NAT Translation Rule for SIP Signaling


Add Row

Index	0
Source Interface	LAN
Target IP Address	212.199.200.90
Source Start Port	5070
Source End Port	5070
Target Start Port	5070
Target End Port	5070

3. Add a NAT rule for RTP packets:

Figure 4-10: NAT Translation Rule for RTP Packets


Add Row

Index	1
Source Interface	LAN
Target IP Address	212.199.200.90
Source Start Port	7000
Source End Port	7090
Target Start Port	7000
Target End Port	7090

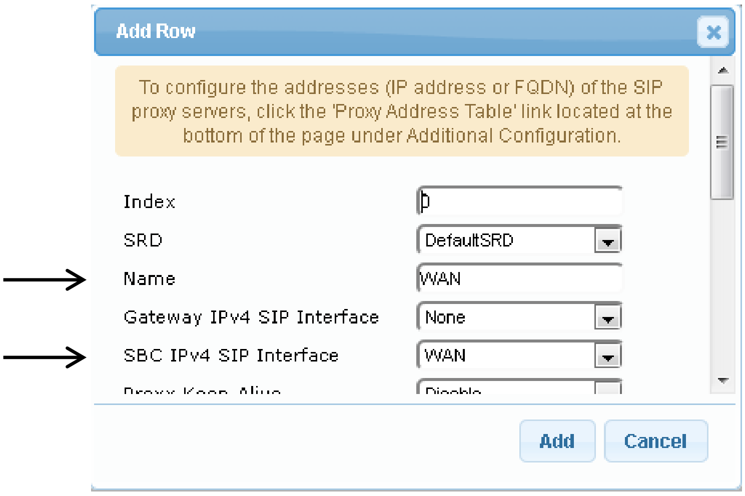
4.5 Step 5: Add a Proxy Set for Hosted IP PBX

In the example, you need to add a Proxy Set for the hosted IP PBX with address 212.199.200.10. You will later apply the Proxy Set to your VoIP network by assigning it to the IP Group of the hosted IP PBX (see Section 4.6).

➢ **To add a Proxy Set:**

1. Open the Proxy Sets table (**Configuration** tab > **VoIP** menu > **VoIP Network** > **Proxy Sets Table**).
2. Add a Proxy Set for the hosted WAN IP PBX:
   a. Add the Proxy Set:

Figure 4-11: Proxy Set for Hosted IP PBX

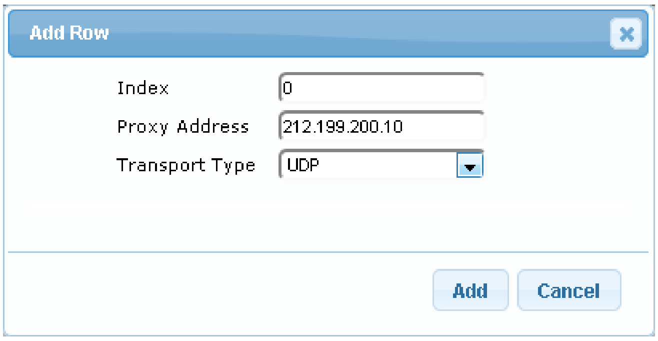


To configure the addresses (IP address or FQDN) of the SIP proxy servers, click the 'Proxy Address Table' link located at the bottom of the page under Additional Configuration.

Index	0
SRD	DefaultSRD
Name	WAN
Gateway IPv4 SIP Interface	None
SBC IPv4 SIP Interface	WAN
Proxy Keep Alive	Disable

   b. Select the table row of the Proxy Set that you added, and then click the **Proxy Address Table** link located below the table.
   c. Add the IP address of the hosted IP PBX :

Figure 4-12: Proxy Set Address for Hosted IP PBX



Index	0
Proxy Address	212.199.200.10
Transport Type	UDP

4.6 Step 6: Add IP Groups for LAN Users and Hosted IP PBX

In the example, you need to add an IP Group for the following entities:

- LAN users (user-type IP Group)
- Hosted WAN IP PBX (server-type IP Group)

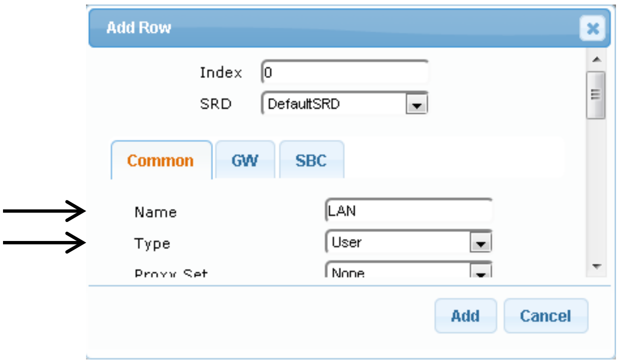
As the hosted IP PBX is a server-type IP Group, you need to assign it the Proxy Set that you configured previously, which defines its' address. In addition, you to enable the SBC to classify calls received from the IP PBX to its' IP Group, based on source IP address (i.e., Proxy Set).

For the LAN users, no Proxy Set is used and thus, classification by Proxy Set needs to be disabled.

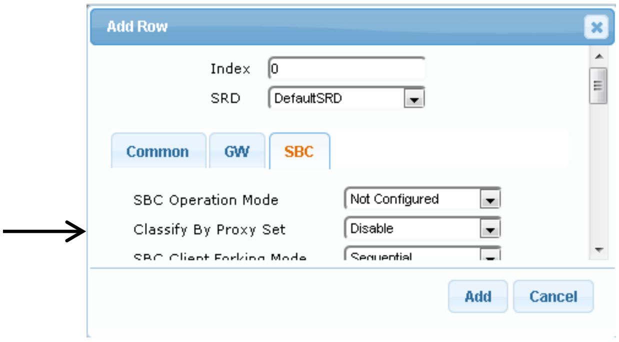
➢ To add IP Groups:

1. Open the IP Group table (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group Table**).
2. Add an IP Group for the LAN users:

Figure 4-13: IP Group for LAN Users



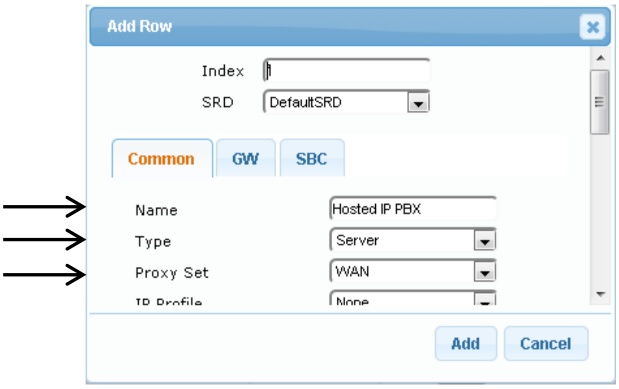
Index: 0
SRD: DefaultSRD
Name: LAN
Type: User
Proxy Set: None



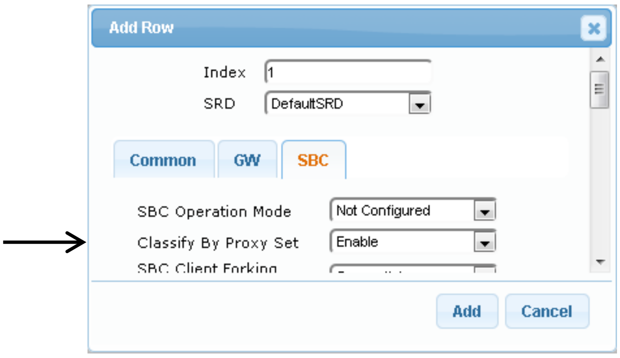
Index: 0
SRD: DefaultSRD
SBC Operation Mode: Not Configured
Classify By Proxy Set: Disable
SBC Client Forking Mode: Sequential

3. Add an IP Group for the Hosted IP PBX:

Figure 4-14: IP Group for Hosted IP PBX



Index: 1
SRD: DefaultSRD
Name: Hosted IP PBX
Type: Server
Proxy Set: WAN
IP Profile: None



Index: 1
SRD: DefaultSRD
SBC Operation Mode: Not Configured
Classify By Proxy Set: Enable
SBC Client Forking

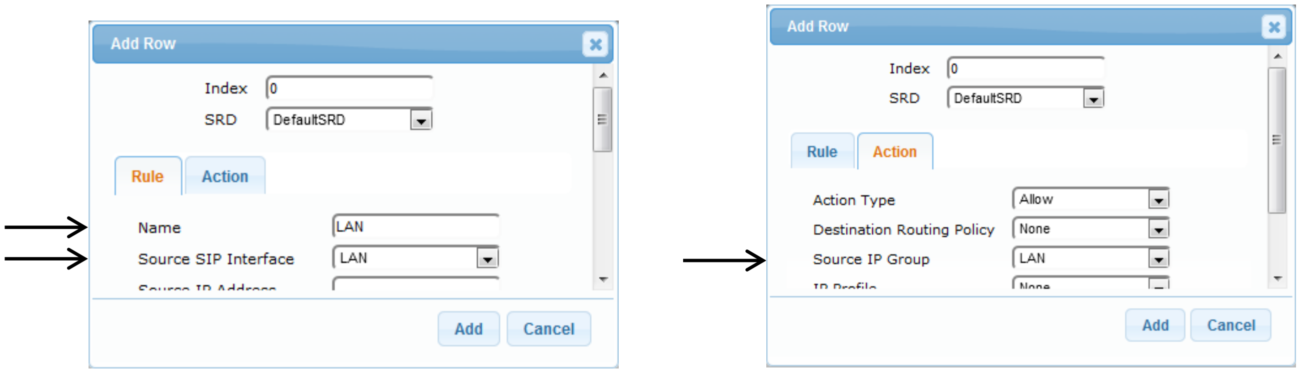
4.7 Step 7: Add a Classification Rule for LAN Users

For the SBC to identify calls from LAN users and classify them to their IP Group, you need to add a Classification rule. In the example, calls received on SIP Interface "LAN" will be identified as LAN users and assigned to IP Group "LAN".

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

1. Open the Classification table (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **Classification Table**).
2. Add a Classification rule:

Figure 4-15: Classification Rule for LAN Users



Index	0
SRD	DefaultSRD
Name	LAN
Source SIP Interface	LAN
Source IP Address	

Index	0
SRD	DefaultSRD
Action Type	Allow
Destination Routing Policy	None
Source IP Group	LAN
IP Profile	None

4.8 Step 8: Add IP-to-IP Call Routing Rules

For call routing between LAN users and the hosted IP PBX, you need to add IP-to-IP routing rules for the following call directions:

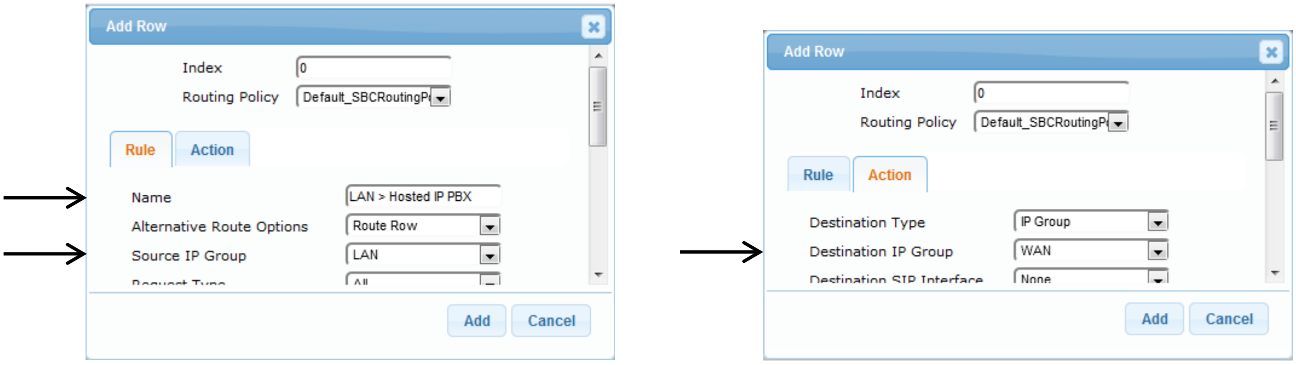
- Calls from LAN users to hosted IP PBX
- Calls from hosted IP PBX to LAN users

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

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

1. Open the IP-to-IP Routing table (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **IP-to-IP Routing Table**).
2. Add a rule to route calls from the LAN users to the hosted IP PBX:

Figure 4-16: Call Routing Rule from LAN Users to Hosted IP PBX



Add Row

Index: 0
Routing Policy: Default_SBCRoutingP(

Rule | Action

Name: LAN > Hosted IP PBX
Alternative Route Options: Route Row
Source IP Group: LAN
Request Type: All

Add | Cancel

Add Row

Index: 0
Routing Policy: Default_SBCRoutingP(

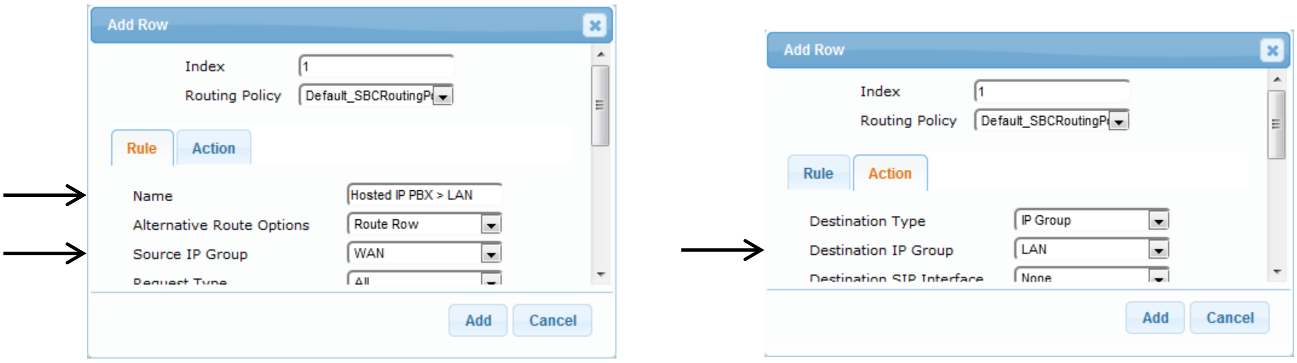
Rule | Action

Destination Type: IP Group
Destination IP Group: WAN
Destination SIP Interface: None

Add | Cancel

3. Add a rule to route calls from hosted IP PBX to the LAN users:

Figure 4-17: Call Routing Rule from Hosted IP PBX to LAN Users



Add Row

Index: 1
Routing Policy: Default_SBCRoutingP(

Rule | Action

Name: Hosted IP PBX > LAN
Alternative Route Options: Route Row
Source IP Group: WAN
Request Type: All

Add | Cancel

Add Row

Index: 1
Routing Policy: Default_SBCRoutingP(

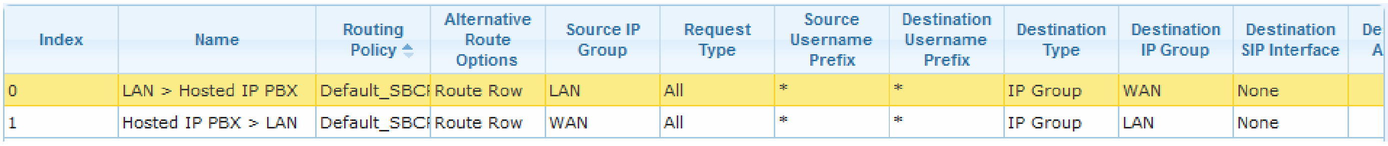
Rule | Action

Destination Type: IP Group
Destination IP Group: LAN
Destination SIP Interface: None

Add | Cancel

Once you have configured the IP-to-IP routing rules, the IP-to-IP Routing table should appear populated as shown below:

Figure 4-18: Configured IP-to-IP Routing Rules in the IP-to-IP Routing Table



Index	Name	Routing Policy	Alternative Route Options	Source IP Group	Request Type	Source Username Prefix	Destination Username Prefix	Destination Type	Destination IP Group	Destination SIP Interface	De A
0	LAN > Hosted IP PBX	Default_SBCI	Route Row	LAN	All	*	*	IP Group	WAN	None	
1	Hosted IP PBX > LAN	Default_SBCI	Route Row	WAN	All	*	*	IP Group	LAN	None	

Notes:

- The single configured SRD (default) is automatically associated with the rules through its' associated, default Routing Policy.
- A destination SIP Interface is not specified for the routing rules. For server-type IP Groups, the SIP Interface that is assigned to the associated Proxy Set is used; for user-type IP Groups (no Proxy Set is configured), the SIP Interface is determined during user registration with the device.

5 Call Survivability for LAN Users upon Hosted IP PBX Failure

The example is based on the same topology setup as described in the previous example (see Section 4).

The example describes how to configure call survivability, whereby upon connectivity failure with the hosted IP PBX (e.g., WAN failure), call routing between the LAN users themselves are maintained.

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

> **Note:** You can also set up PSTN Fallback upon hosted IP PBX failure, as described in the example in Section 3.2.

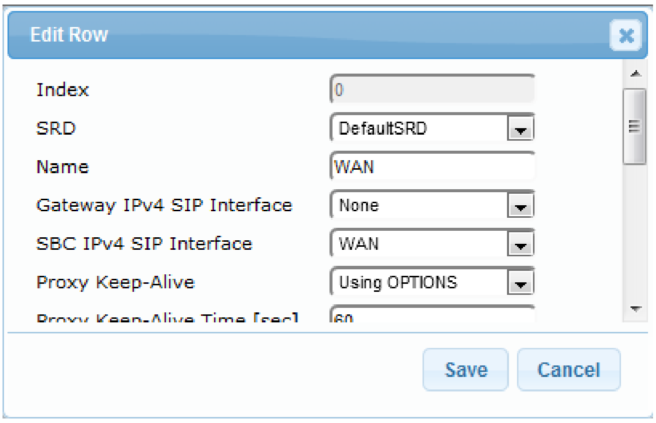
5.1 Step 1: Enable Keep-Alive for Hosted IP PBX

The SBC performs call survivability upon connectivity failure with the hosted IP PBX. For the device to detect connectivity failure with the IP PBX, you need to enable the keep-alive mechanism with the IP PBX. The keep-alive mechanism periodically checks connectivity by sending SIP OPTIONS messages.

➢ **To enable keep-alive mechanism with the hosted IP PBX:**

1. Open the Proxy Sets table (**Configuration** tab > **VoIP** menu > **V Network** > **Proxy Sets Table**).
2. Edit Proxy Set "WAN", which you configured for the hosted IP PBX (in Section 4.5), to enable proxy keep-alive using SIP OPTIONS messages:

Figure 5-1: Enabling Keep-Alive with Hosted IP PBX



Index	0
SRD	DefaultSRD
Name	WAN
Gateway IPv4 SIP Interface	None
SBC IPv4 SIP Interface	WAN
Proxy Keep-Alive	Using OPTIONS
Proxy Keep-Alive Time [sec]	60

5.2 Step 2: Add an Alternative IP-to-IP Call Routing Rule

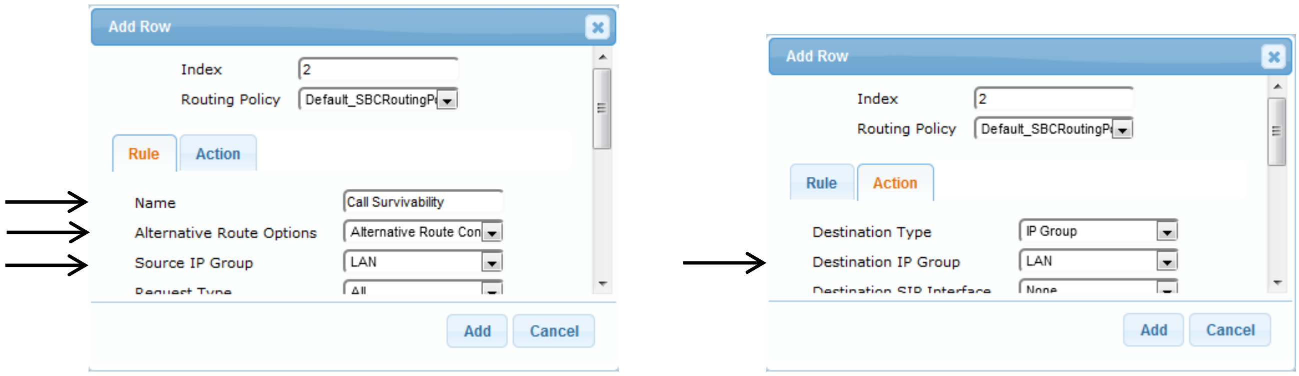
You need to add an alternative IP-to-IP call routing rule that is used when connectivity with the hosted IP PBX fails. The alternative routing rule will route calls from LAN users to LAN users, instead of to the hosted IP PBX.

> **Notes:**
>
> - You must add the alternative routing rule to the table index row that is immediately below the row of the LAN users to hosted IP PBX routing rule, and set the 'Alternative Route Options' parameter to **Alternative Route Consider Inputs**.
> - When the SBC detects the return of connectivity with the hosted IP PBX, it uses the normal routing rule that routes calls from LAN users to hosted IP PBX, instead of the alternative rule.

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

1. Open the IP-to-IP Routing table (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **IP-to-IP Routing Table**).
2. Add a rule for routing calls between the LAN users:

Figure 5-2: Alternative Routing Rule for Routing between LAN Users

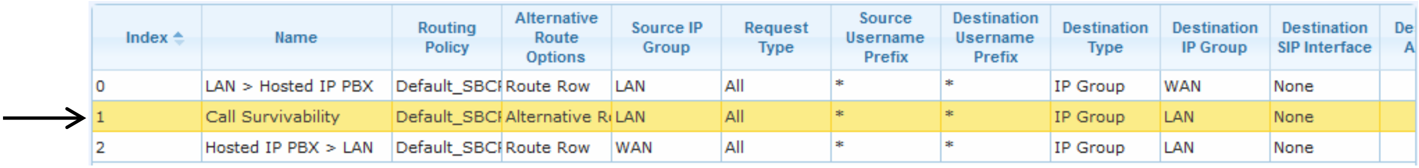


Index: 2
Routing Policy: Default_SBCRoutingP(
Name: Call Survivability
Alternative Route Options: Alternative Route Con
Source IP Group: LAN
Request Type: All

Index: 2
Routing Policy: Default_SBCRoutingP(
Destination Type: IP Group
Destination IP Group: LAN
Destination SIP Interface: None

3. In the table, move the new row to the row located immediately below the row of the LAN users to hosted IP PBX routing rule. To do this:
   a. Make sure that the table is sorted according to the 'Index' column. If it's not, simply click the 'Index' column heading.
   b. Select the row that you added above, and then click the **Up** button to move the row one index up in the table (i.e., to Index 1); the alternative routing rule is moved to the row immediately below the LAN users to hosted IP PBX rule:

Figure 5-3: IP-to-IP Call Routing Rule for LAN User Survivability



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	De A
0	LAN > Hosted IP PBX	Default_SBCI	Route Row	LAN	All	*	*	IP Group	WAN	None	
1	Call Survivability	Default_SBCI	Alternative R	LAN	All	*	*	IP Group	LAN	None	
2	Hosted IP PBX > LAN	Default_SBCI	Route Row	WAN	All	*	*	IP Group	LAN	None	

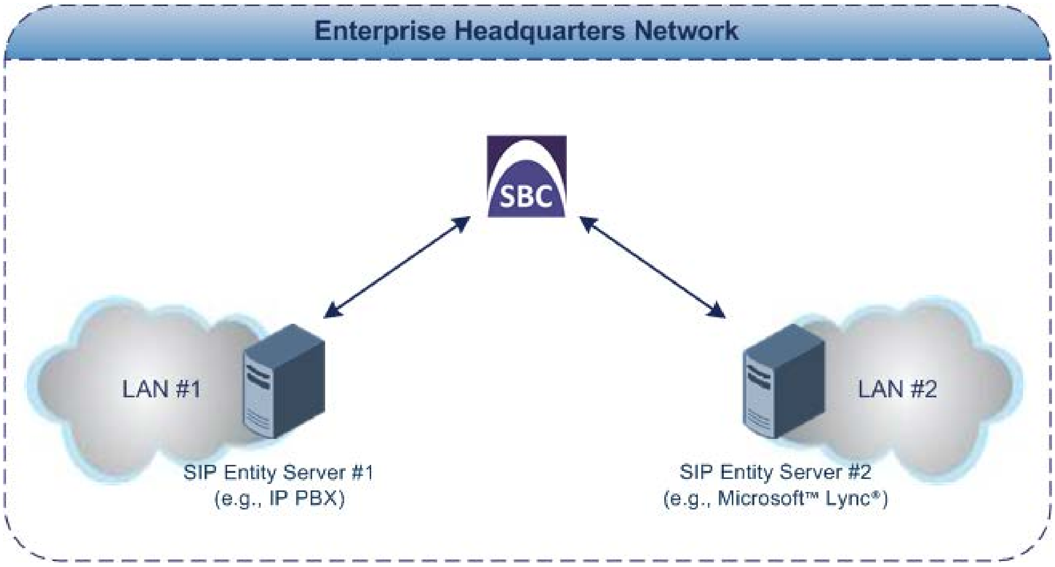
6 SIP Normalization between SIP Entity Servers

The example describes how to configure SIP normalization when the SBC interworks between different SIP entities. The 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
- **Required SIP Normalization:**
  - Voice transcoding between G.711 and G.729.
  - SIP transport protocol translation between UDP and TCP.
  - Phone number normalization. SIP Entity Server #1 employs E.164 number format while SIP Entity Server #2 does not.
  - Manipulation of 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:

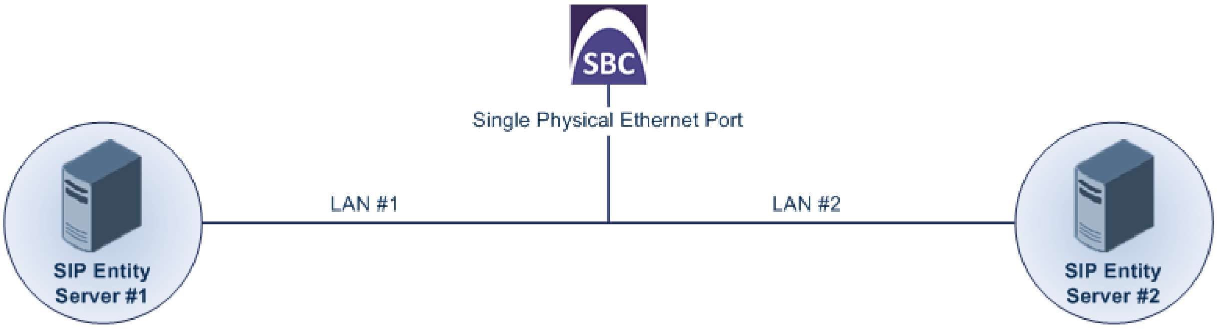
Figure 6-1: SIP Normalization Example - Application Topology



- **Topology:**
  - **SBC Logical Network Interface Connection:**
    The SBC communicates with the SIP entity servers using a single IP network interface.
  - **SBC Physical LAN Port Connection:**
    The SBC uses a single LAN port to connect to the LAN.

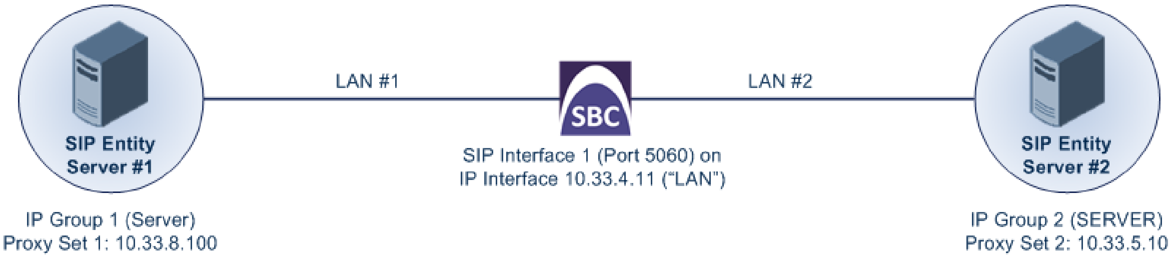
The figure below shows the SBC's logical network interface and LAN port connection of the example scenario:

Figure 6-2: SBC Physical Port Connection and Logical Interface



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

Figure 6-3: Required Configuration Entities

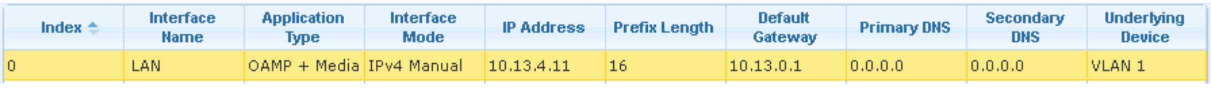


Note: For clarity, whenever configuring the various entities in the example (e.g., Media Realms, Proxy Sets, and IP Groups), table row index 0 is used for the SBC network interfacing with SIP Entity Server #1; row index 1 is used for the SBC network interfacing with SIP Entity Server #2.

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

The example employs only one logical network interface (10.33.4.11), which is used for the LAN as well as management (i.e., OAMP). The example assumes that this interface is already setup and thus, additional configuration is unnecessary.

Figure 6-4: Logical IP Network Interface for LAN



Index	Interface Name	Application Type	Interface Mode	IP Address	Prefix Length	Default Gateway	Primary DNS	Secondary DNS	Underlying Device
0	LAN	OAMP + Media	IPv4 Manual	10.13.4.11	16	10.13.0.1	0.0.0.0	0.0.0.0	VLAN 1

Note: You can change the physical port assigned to the network interface ('Underlying Device'). For a description on how to do this, see the example in Section 2.

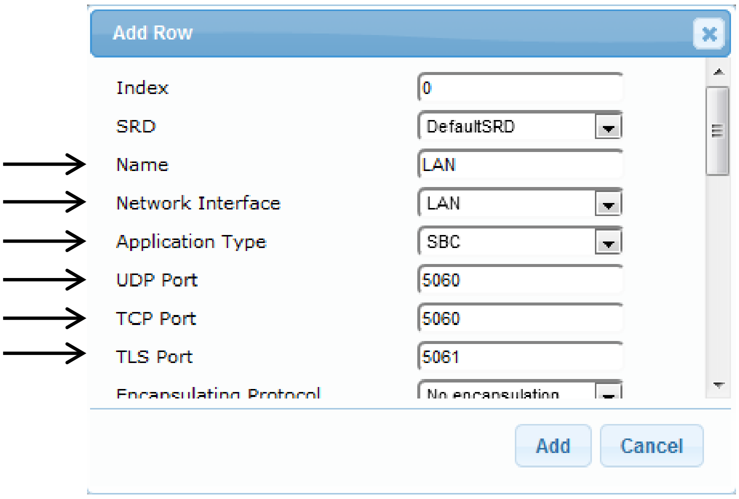
6.2 Step 2: Add a SIP Interface for LAN

You need to add a SIP Interface for the LAN which interfaces with both SIP servers. The SIP Interface is associated with the logical IP network interface, 10.33.4.11 ("LAN").

➢ **To add a SIP Interface:**

1. Open the SIP Interface table (**Configuration** tab > **VoIP** menu > **VoIP Network** > **SIP Interface Table**).
2. Add a SIP Interface for the LAN interface:

Figure 6-5: SIP Interface for LAN Interface



Index	0
SRD	DefaultSRD
Name	LAN
Network Interface	LAN
Application Type	SBC
UDP Port	5060
TCP Port	5060
TLS Port	5061
Encapsulating Protocol	No encapsulation

6.3 Step 3: Add Proxy Sets for SIP Servers

The Proxy Set defines the actual address of SIP server entities in your network. Therefore, you need to add a Proxy Set for the following entities:

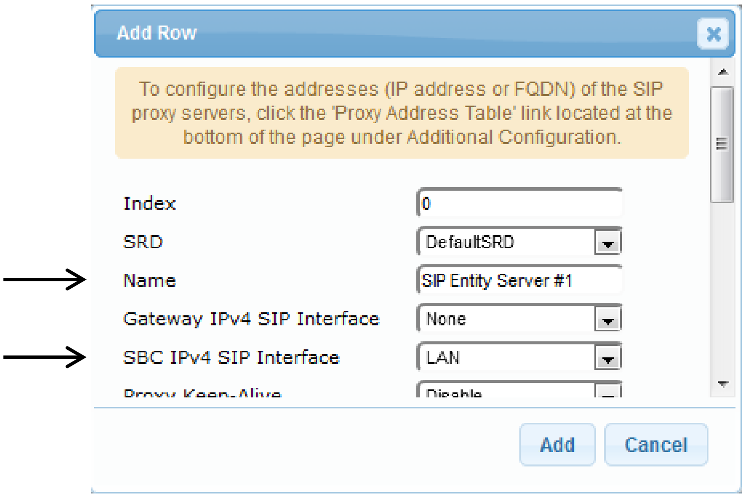
- SIP Entity Server #1 - address 10.33.8.100 and using UDP transport
- SIP Entity Server #2 - address 10.33.5.10 and using TCP transport

You will later apply the Proxy Sets to your VoIP network by assigning them to IP Groups, which represent these entities.

➢ **To add Proxy Sets:**

1. Open the Proxy Sets table (**Configuration** tab > **VoIP** menu > **VoIP Network > Proxy Sets Table**).
2. Add a Proxy Set for SIP Entity Server #1:
   a. Add the Proxy Set:

Figure 6-6: Proxy Set for SIP Entity Server #1



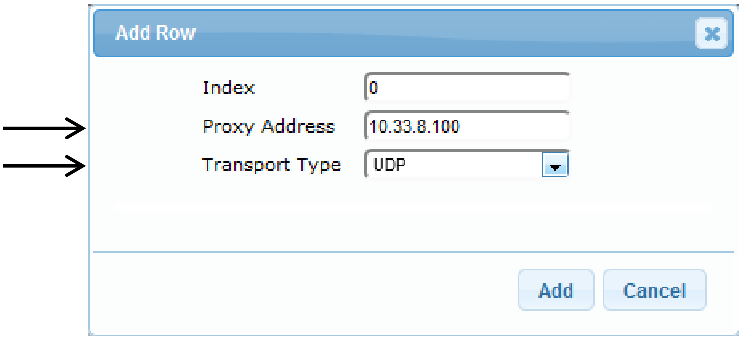
Add Row

To configure the addresses (IP address or FQDN) of the SIP proxy servers, click the 'Proxy Address Table' link located at the bottom of the page under Additional Configuration.

Index	0
SRD	DefaultSRD
Name	SIP Entity Server #1
Gateway IPv4 SIP Interface	None
SBC IPv4 SIP Interface	LAN
Proxy Keep-Alive	Disable

   b. Select the table row of the Proxy Set that you added, and then click the **Proxy Address Table** link located below the table.
   c. Add the IP address of the SIP Entity Server #1:

Figure 6-7: Proxy Set Address for SIP Entity Server #1



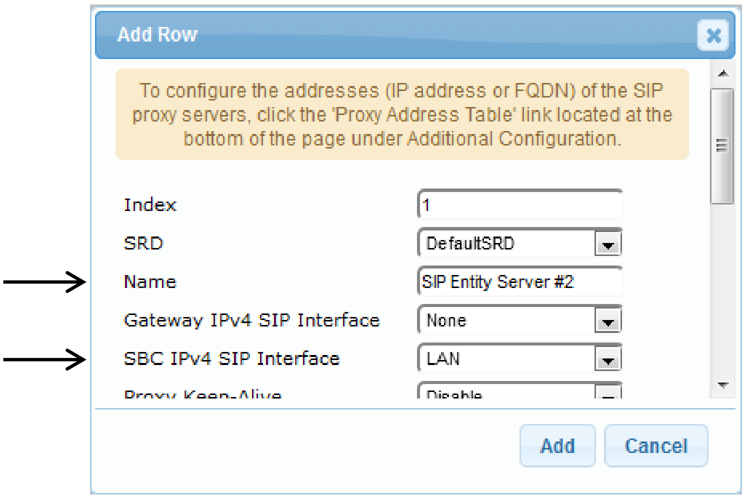
Add Row

Index	0
Proxy Address	10.33.8.100
Transport Type	UDP

3. Add a Proxy Set for SIP Entity Server #2:

   a. Add the Proxy Set:

Figure 6-8: Proxy Set for SIP Entity Server #2



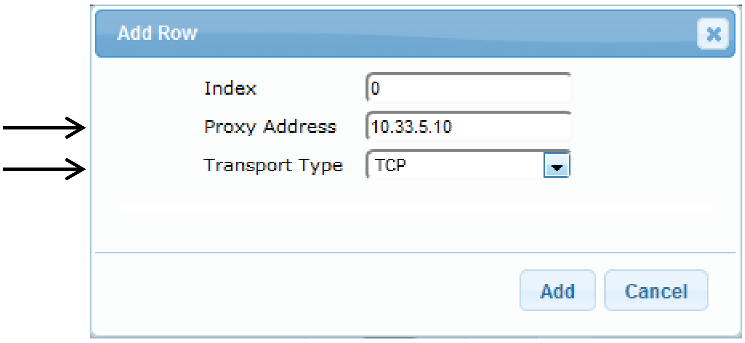
To configure the addresses (IP address or FQDN) of the SIP proxy servers, click the 'Proxy Address Table' link located at the bottom of the page under Additional Configuration.

Index	1
SRD	DefaultSRD
Name	SIP Entity Server #2
Gateway IPv4 SIP Interface	None
SBC IPv4 SIP Interface	LAN
Proxy Keep-Alive	Disable

   b. Select the table row of the Proxy Set that you added, and then click the **Proxy Address Table** link located below the table.

   c. Add the IP address of SIP Entity Server #2:

Figure 6-9: Proxy Set Address for SIP Entity Server #2



Index	0
Proxy Address	10.33.5.10
Transport Type	TCP

6.4 Step 4: Add IP Groups for SIP Servers

The IP Group represents the SIP entity. In the example, you need to add an IP Group for the following entities:

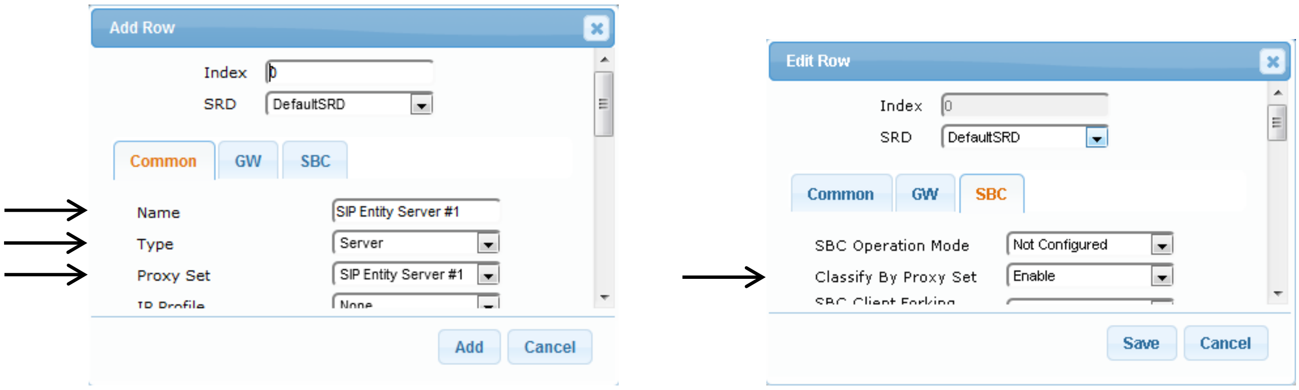
- SIP Entity Server #1 (server-type IP Group)
- SIP Entity Server #2 (server-type IP Group)

For the server-type IP Groups, you need to assign their respective Proxy Sets, which define their IP addresses and which you configured in the previous step. In addition, you need to enable the SBC to classify incoming calls to the IP Groups, based on their source IP address (i.e., Proxy Set).

➢ To add IP Groups:

1. Open the IP Group table (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group Table**).
2. Add an IP Group for SIP Entity Server #1:

Figure 6-10: IP Group for SIP Entity Server #1

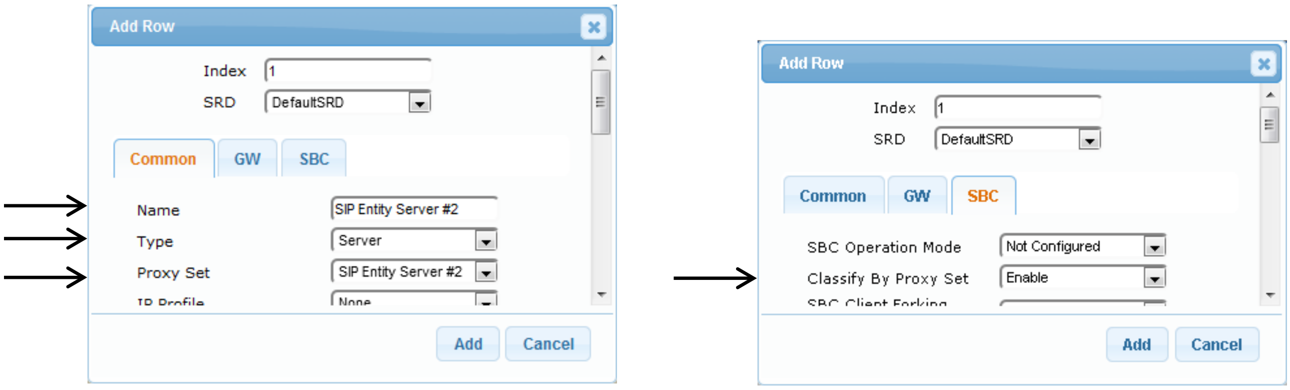


Index 0
SRD DefaultSRD
Name SIP Entity Server #1
Type Server
Proxy Set SIP Entity Server #1
IP Profile None

Index 0
SRD DefaultSRD
SBC Operation Mode Not Configured
Classify By Proxy Set Enable
SBC Client Forking

3. Add an IP Group for SIP Entity Server #2:

Figure 6-11: IP Group for SIP Entity Server #2



Index 1
SRD DefaultSRD
Name SIP Entity Server #2
Type Server
Proxy Set SIP Entity Server #2
IP Profile None

Index 1
SRD DefaultSRD
SBC Operation Mode Not Configured
Classify By Proxy Set Enable
SBC Client Forking

6.5 Step 5: Add IP-to-IP Call Routing Rules

For call routing between the SIP entities, you need to add IP-to-IP routing rules for the following call directions:

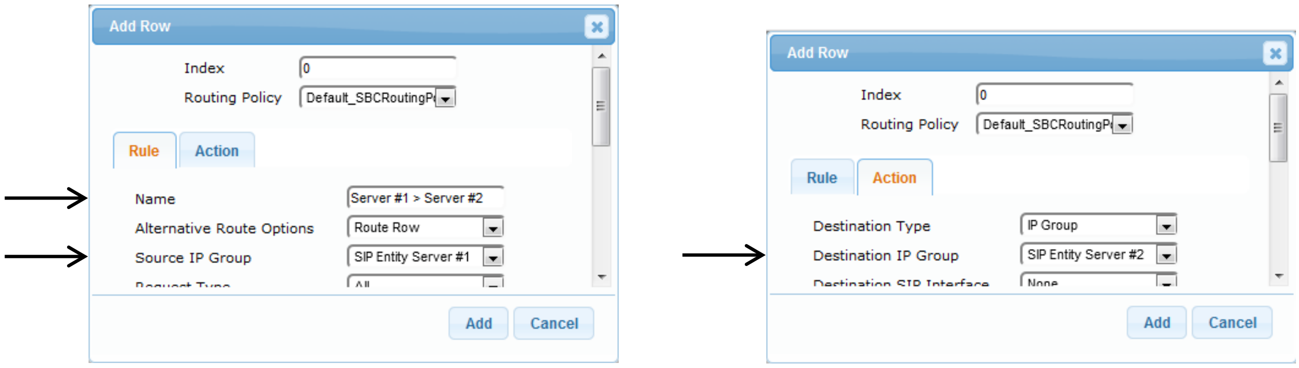
- Calls from SIP Entity Server #1 to SIP Entity Server #2
- Calls from SIP Entity Server #2 to SIP Entity Server #1

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 IP-to-IP Routing table (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **IP-to-IP Routing Table**).
2. Add a rule to route calls from the SIP Entity Server #1 to the SIP Entity Server #2:

Figure 6-12: Call Routing Rule from SIP Entity Server #1 to the SIP Entity Server #2

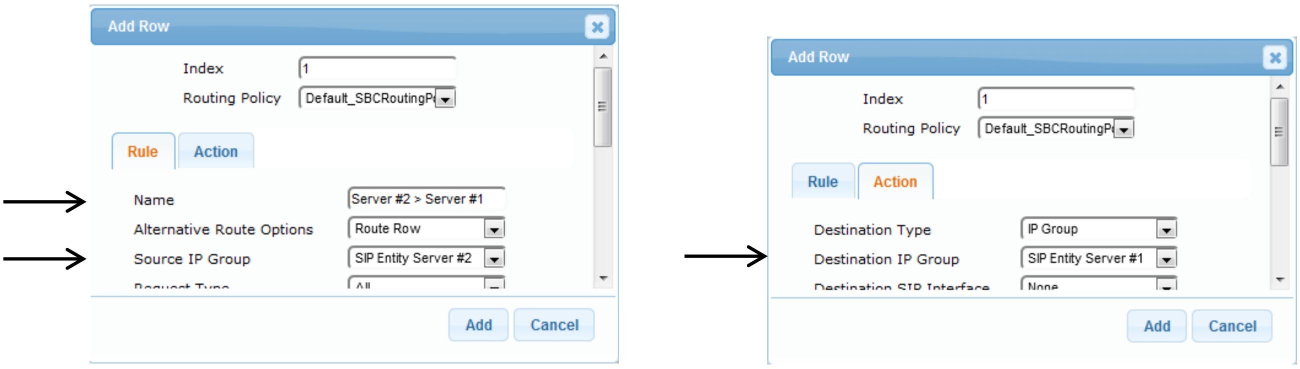


Index: 0
Routing Policy: Default_SBCRoutingP
Name: Server #1 > Server #2
Alternative Route Options: Route Row
Source IP Group: SIP Entity Server #1
Request Type: All

Index: 0
Routing Policy: Default_SBCRoutingP
Destination Type: IP Group
Destination IP Group: SIP Entity Server #2
Destination SIP Interface: None

3. Add a rule to route calls from SIP Entity Server #2 to SIP Entity Server #1:

Figure 6-13: Call Routing Rule from SIP Entity Server #2 to SIP Entity Server #1

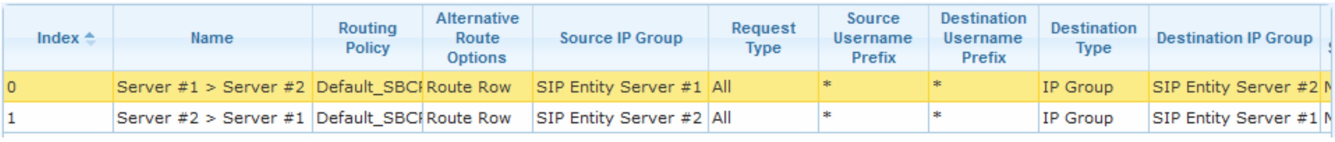


Index: 1
Routing Policy: Default_SBCRoutingP
Name: Server #2 > Server #1
Alternative Route Options: Route Row
Source IP Group: SIP Entity Server #2
Request Type: All

Index: 1
Routing Policy: Default_SBCRoutingP
Destination Type: IP Group
Destination IP Group: SIP Entity Server #1
Destination SIP Interface: None

When you have completed configuring the above IP-to-IP routing rules, the IP-to-IP Routing table lists all the rules, as shown below:

Figure 6-14: IP-to-IP Call Routing Rules



Index	Name	Routing Policy	Alternative Route Options	Source IP Group	Request Type	Source Username Prefix	Destination Username Prefix	Destination Type	Destination IP Group
0	Server #1 > Server #2	Default_SBCI	Route Row	SIP Entity Server #1	All	*	*	IP Group	SIP Entity Server #2
1	Server #2 > Server #1	Default_SBCI	Route Row	SIP Entity Server #2	All	*	*	IP Group	SIP Entity Server #1

6.6 Voice Transcoding

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

- SIP Entity Server #1 uses G.711 A-law or G.711 µ-law, and does not allow any other coder in the SDP offer-exchange coder list
- SIP Entity Server #2 uses G.729

The configuration for the example uses the following terms related to coders:

- *Extension Coders*: Voice codecs supported by the SIP entity. The SBC adds these coders to the SDP offer sent to the SIP entity. Extension coders are required for transcoding when the two communicating SIP entities support different coders (i.e., supported coders do not appear in the SDP offer).
- *Allowed Coders*: Coders that are permitted to be listed in the SDP offer that the device sends to the SIP entity. This is required for SIP entities that accept only SDPs that include specific coders (for whatever reason). The Allowed coders would include the Extension coder as well as other coders.

6.6.1 Step 1: Add Extension Coder Groups for SIP Entities

A Coder Group (or Extension Coder Group) defines the codecs supported by the SIP entity. Even if the original SDP offer does not include the coder supported by the SIP entity, the SBC adds it to the SDP before sending it to the SIP entity.

In the example, you need to configure a Coder Group per SIP entity server with the supported coder:

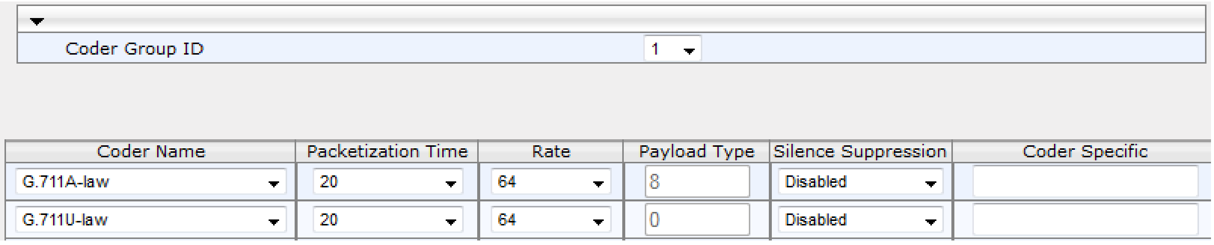
- SIP Entity Server #1 - G.711 A-law and G.711 µ-law
- SIP Entity Server #2 - G.729

In Section 6.6.3, you will assign the Coder Groups to the IP Profiles of the SIP entities.

➢ To add Coder Groups for the SIP entity servers:

1. Open the Coder Group Settings table (**Configuration** tab > **VoIP** menu > **Coders and Profiles** > **Coders Group Settings**).
2. Add a Coder Group for SIP Entity Server #1:

Figure 6-15: Coder Group for SIP Entity Server #1

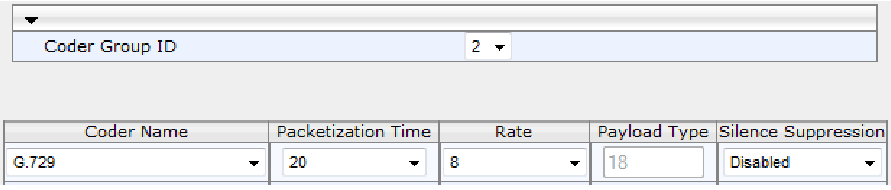


Coder Group ID: 1

Coder Name	Packetization Time	Rate	Payload Type	Silence Suppression	Coder Specific
G.711A-law	20	64	8	Disabled	
G.711U-law	20	64	0	Disabled	

3. Add a Coder Group for SIP Entity Server #2:

Figure 6-16: 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

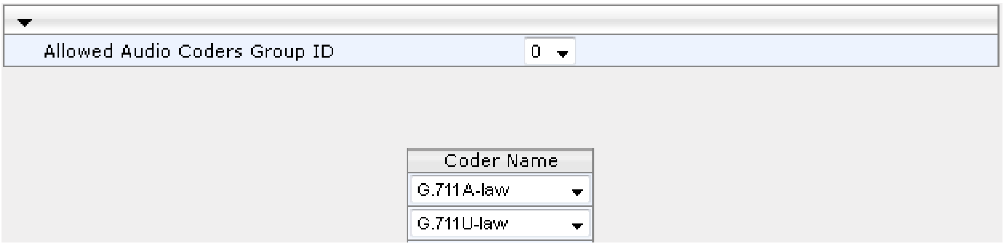
6.6.2 Step 2: Add Allowed Coders Group for SIP Entity Server #1

In the example, SIP Entity Server #1 allows only the G.711 A-law and G.711 µ-law coders to be listed in the SDP offer sent to it by the SBC. If other coders are listed in the SDP, the SBC removes them before sending them to the SIP entity. Therefore, you need to configure an Allowed Audio Coders Group with these coders. In Section 6.6.3, you will assign the Allowed Audio Coders Group to the IP Profile of the SIP entity.

➢ **To add Allowed Audio Coders Group for SIP entity server #1:**

1. Open the Allowed Audio Coders Group table (**Configuration** tab > **VoIP** menu > **SBC** > **Allowed Audio Coders Group**).
2. Add an Allowed Audio Coders Group for SIP Entity Server #1:

Figure 6-17: Allowed Audio Coders Group for SIP Entity Server #1



Allowed Audio Coders Group ID: 0

Coder Name
G.711A-law
G.711U-law

6.6.3 Step 3: Add IP Profiles for SIP Entities and Assign their Coder Groups

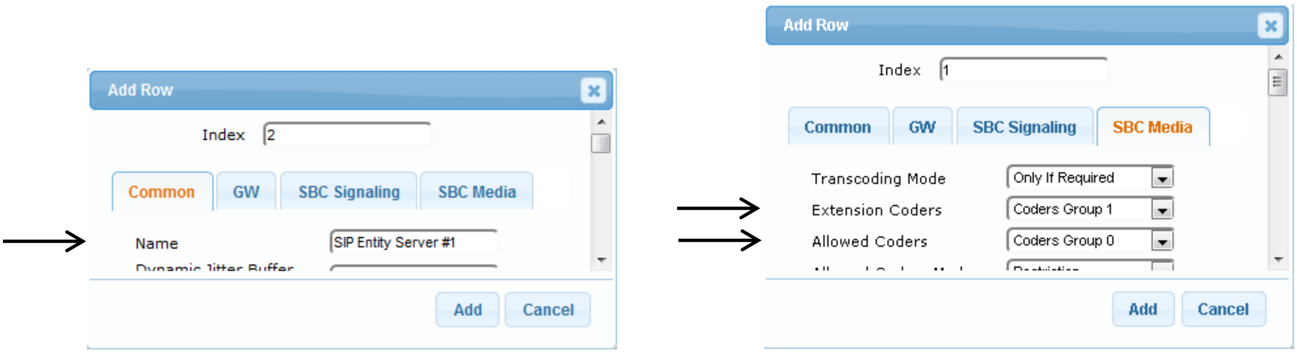
An IP Profile defines a set of configuration settings that can be assigned to specific calls. In the example, you need to configure an IP Profile for each SIP entity server and assign it the supported codec (i.e., Coder Group) that you configured in the previous steps:

- SIP Entity Server #1: Supports only G.711 (A-law and µ-law) and does not allow other additional coders to be listed in the SDP. Therefore, the IP Profile must be assigned the following:
  - Extension Coders Group (Index 1): G.711 (A-law and µ-law)
  - Allowed Audio Coders Group (Index 0): G.711 (A-law and µ-law)
- SIP Entity Server #2: Supports only G.729, but accepts SDPs listing other additional coders. Therefore, the following configuration is required:
  - Extension Coders Group (Index 2): G.729

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

1. Open the IP Profile Settings table (**Configuration** tab > **VoIP** menu > **Coders and Profiles** > **IP Profile Settings**).
2. Add an IP Profile for SIP Entity Server #1:

Figure 6-18: IP Profile for SIP Entity Server #1



Index: 2

Name: SIP Entity Server #1

Index: 1

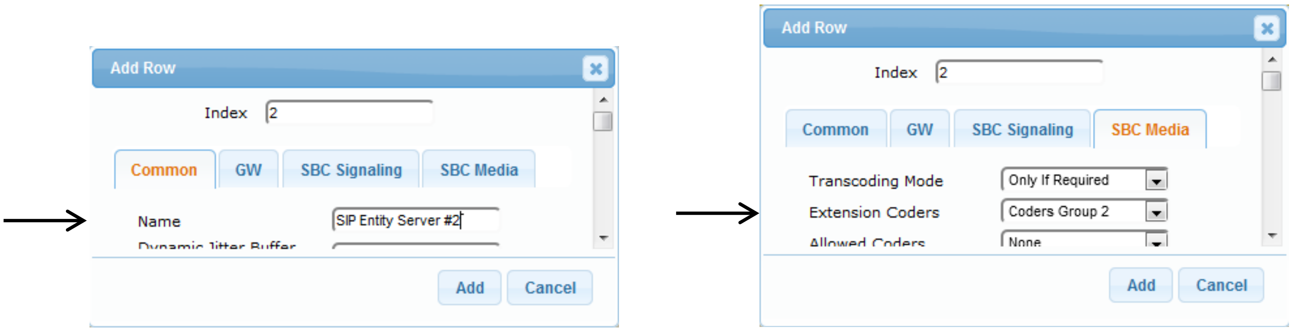
Transcoding Mode: Only If Required

Extension Coders: Coders Group 1

Allowed Coders: Coders Group 0

3. Add an IP Profile for SIP Entity Server #2:

Figure 6-19: IP Profile for SIP Entity Server #2



Index: 2

Name: SIP Entity Server #2

Index: 2

Transcoding Mode: Only If Required

Extension Coders: Coders Group 2

Allowed Coders: None

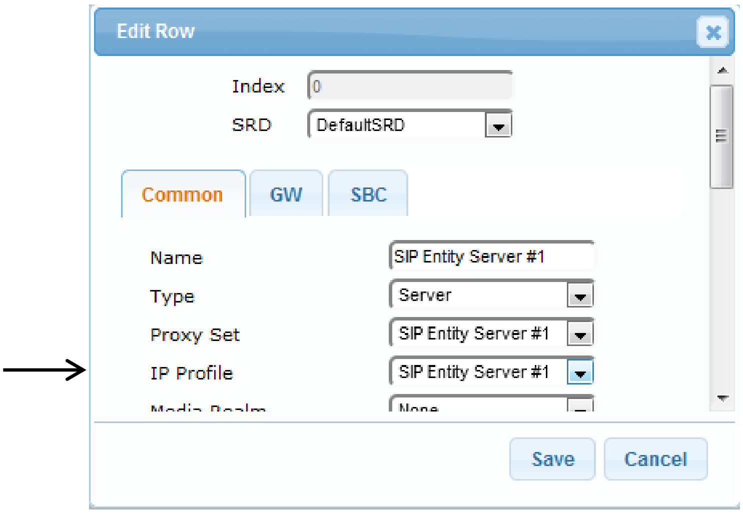
6.6.4 Step 4: Assign IP Profiles to SIP Entity IP Groups

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

➢ To assign the IP Profiles to the IP Groups:

1. Open the IP Group table (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group Table**).
2. Edit IP Group "SIP Entity Server #1":

Figure 6-20: Assigning IP Profile to IP Group of SIP Entity Server #1



Index: 0

SRD: DefaultSRD

Name: SIP Entity Server #1

Type: Server

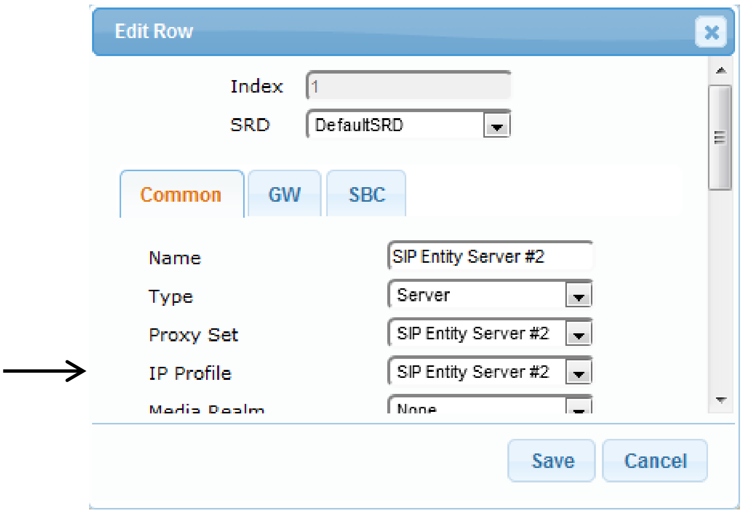
Proxy Set: SIP Entity Server #1

IP Profile: SIP Entity Server #1

Media Realm: None

3. Edit IP Group "SIP Entity Server #2":

Figure 6-21: Assigning IP Profile to IP Group of SIP Entity Server #2



Index 1

SRD DefaultSRD

Name SIP Entity Server #2

Type Server

Proxy Set SIP Entity Server #2

IP Profile SIP Entity Server #2

Media Realm None

6.7 Phone Number Manipulation

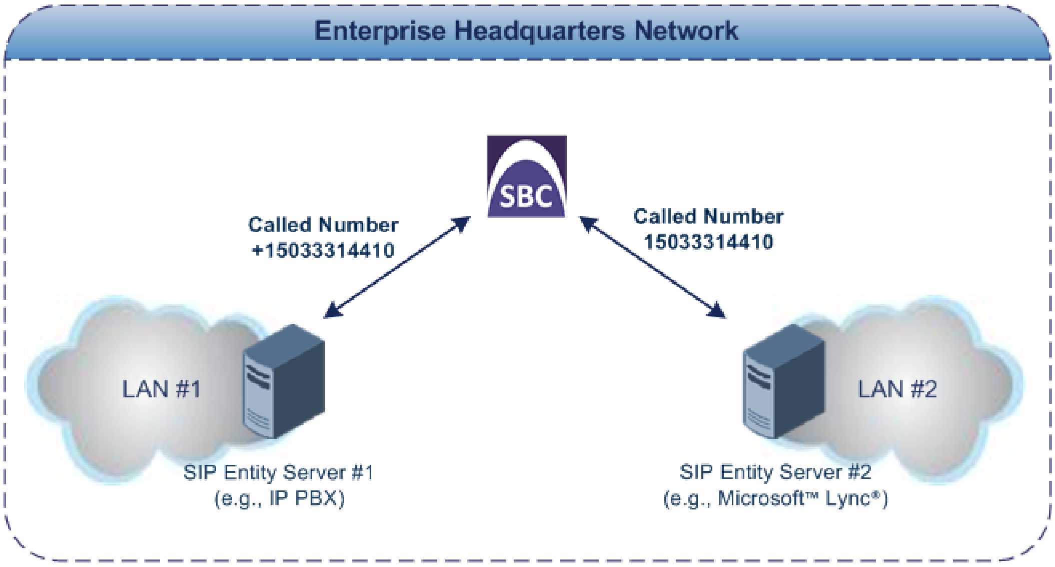
In the example, SIP Entity Server #1 employs the E.164 number format while SIP Entity Server #2 does not. Therefore, the SBC needs to perform phone number normalization when routing calls between these entities.

The following number manipulation rules need to be configured:

- Calls received from SIP Entity Server #1 with destination (called) number prefix "+": remove the 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.

The figure below shows an example of number manipulation (+15033314410 to 15033314410 and vice versa) between the two SIP entities:

Figure 6-22: Phone Number Manipulation Example



6.7.1 Step 1: Add Number Manipulation Rules

You need to add the following number manipulation rules:

- Calls received from SIP Entity Server #1:
  - Remove "+" from the destination Request-URI
  - Remove "+" from the source Request-URI
- Calls received from SIP Entity Server #2:
  - Add "+" to the destination Request-URI
  - Add "+" to from the source Request-URI

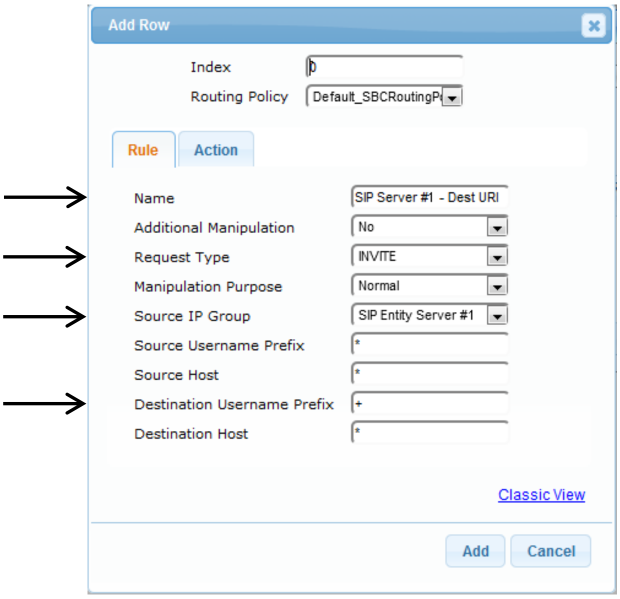
➢ To add number manipulation rules:

1. Open the IP-to-IP Inbound Manipulation table (**Configuration** tab > **VoIP** menu > **SBC** submenu > **Manipulations SBC** > **IP-to-IP Inbound**).

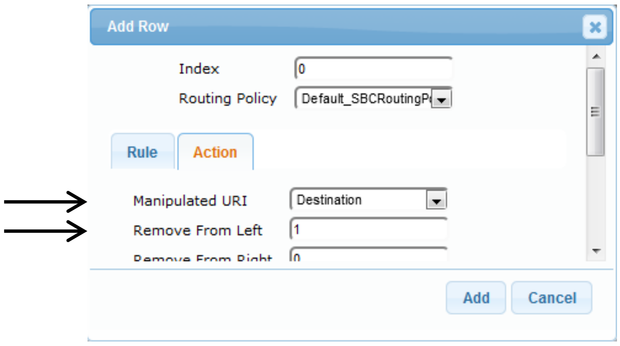
2. Add the following manipulation rules for calls received from SIP Entity Server #1:

   a. Remove "+" from destination Request-URI:

Figure 6-23: Inbound Number Manipulation (Dest. URI) for SIP Entity Server #1



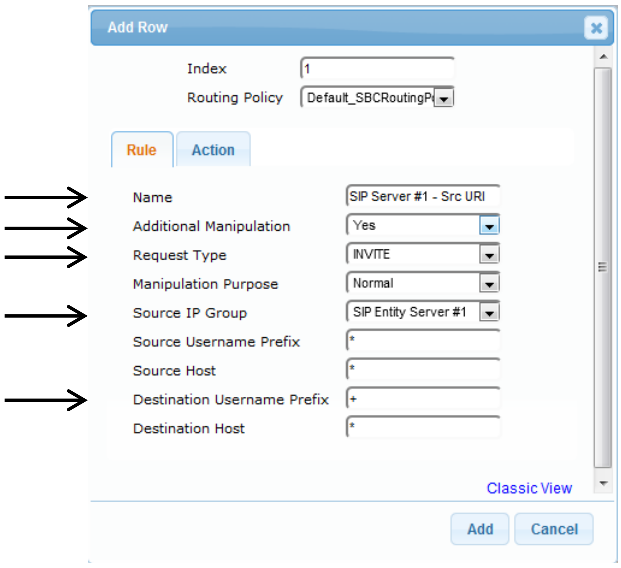
Index: 0
Routing Policy: Default_SBCRoutingP
Name: SIP Server #1 - Dest URI
Additional Manipulation: No
Request Type: INVITE
Manipulation Purpose: Normal
Source IP Group: SIP Entity Server #1
Source Username Prefix: *
Source Host: *
Destination Username Prefix: +
Destination Host: *



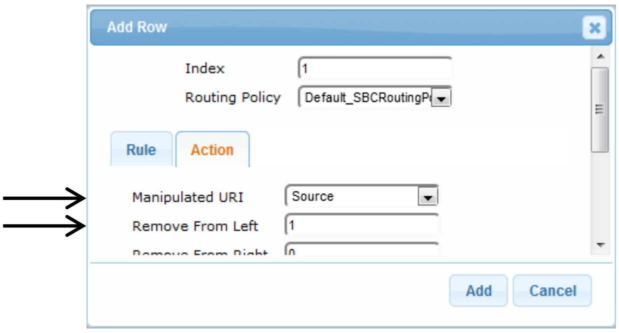
Index: 0
Routing Policy: Default_SBCRoutingP
Manipulated URI: Destination
Remove From Left: 1
Remove From Right: 0

   b. Remove "+" from source Request-URI:

Figure 6-24: Inbound Number Manipulation (Source URI) for SIP Entity Server #1



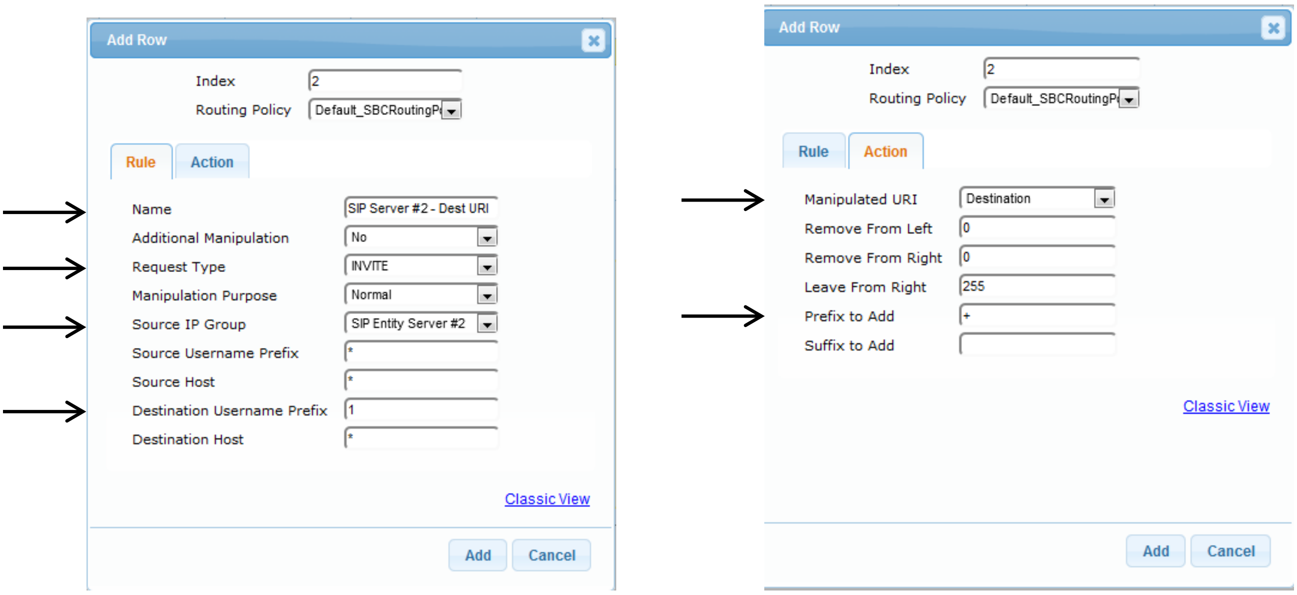
Index: 1
Routing Policy: Default_SBCRoutingP
Name: SIP Server #1 - Src URI
Additional Manipulation: Yes
Request Type: INVITE
Manipulation Purpose: Normal
Source IP Group: SIP Entity Server #1
Source Username Prefix: *
Source Host: *
Destination Username Prefix: +
Destination Host: *



Index: 1
Routing Policy: Default_SBCRoutingP
Manipulated URI: Source
Remove From Left: 1
Remove From Right: 0

3. Add the following manipulation rules for calls received from SIP Entity Server #2:
   a. Add "+" to destination Request-URI:

Figure 6-25: Inbound Number Manipulation (Dest. URI) for SIP Entity Server #2

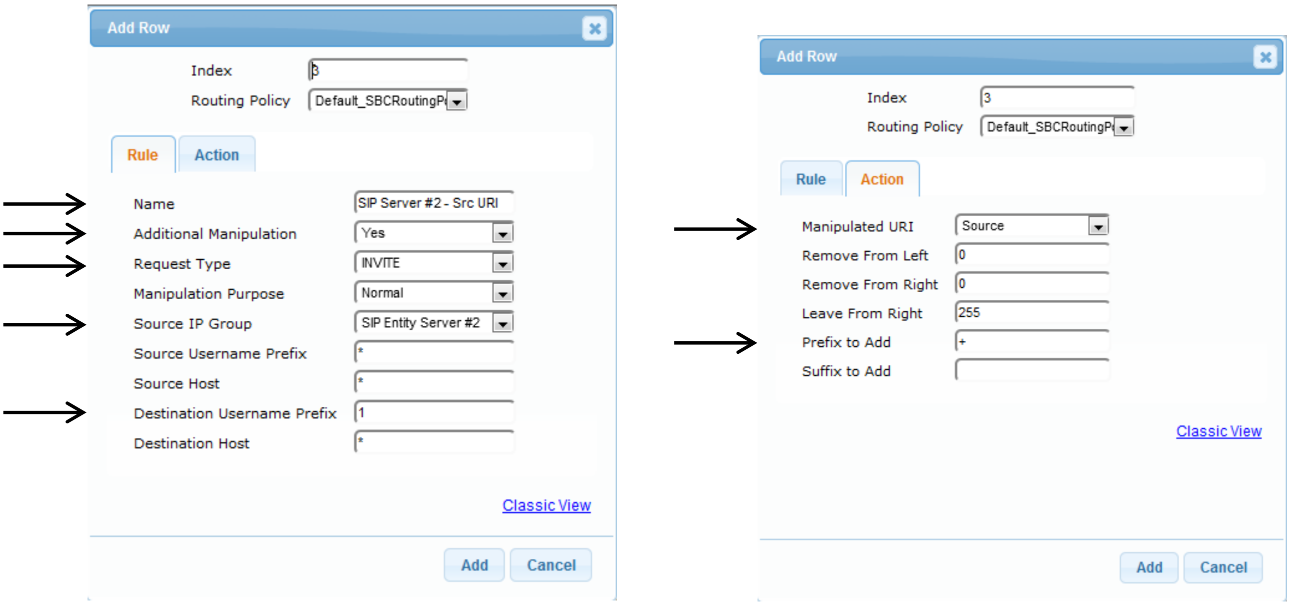


Index	2
Routing Policy	Default_SBCRoutingP
Name	SIP Server #2 - Dest URI
Additional Manipulation	No
Request Type	INVITE
Manipulation Purpose	Normal
Source IP Group	SIP Entity Server #2
Source Username Prefix	*
Source Host	*
Destination Username Prefix	1
Destination Host	*

Index	2
Routing Policy	Default_SBCRoutingP
Manipulated URI	Destination
Remove From Left	0
Remove From Right	0
Leave From Right	255
Prefix to Add	+
Suffix to Add	

   b. Add "+" to source Request-URI:

Figure 6-26: Inbound Number Manipulation (Source URI) for SIP Entity Server #2

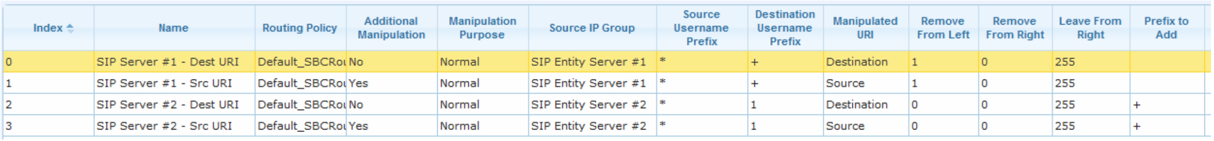


Index	3
Routing Policy	Default_SBCRoutingP
Name	SIP Server #2 - Src URI
Additional Manipulation	Yes
Request Type	INVITE
Manipulation Purpose	Normal
Source IP Group	SIP Entity Server #2
Source Username Prefix	*
Source Host	*
Destination Username Prefix	1
Destination Host	*

Index	3
Routing Policy	Default_SBCRoutingP
Manipulated URI	Source
Remove From Left	0
Remove From Right	0
Leave From Right	255
Prefix to Add	+
Suffix to Add	

Once you have configured the IP-to-IP inbound manipulation rules, the IP-to-IP Inbound Manipulation table should appear populated as shown below:

Figure 6-27: Configured IP-to-IP Inbound Manipulation Rules in the IP-to-IP Inbound Manipulation Table



Index	Name	Routing Policy	Additional Manipulation	Manipulation Purpose	Source IP Group	Source Username Prefix	Destination Username Prefix	Manipulated URI	Remove From Left	Remove From Right	Leave From Right	Prefix to Add
0	SIP Server #1 - Dest URI	Default_SBCRou	No	Normal	SIP Entity Server #1	*	+	Destination	1	0	255	
1	SIP Server #1 - Src URI	Default_SBCRou	Yes	Normal	SIP Entity Server #1	*	+	Source	1	0	255	
2	SIP Server #2 - Dest URI	Default_SBCRou	No	Normal	SIP Entity Server #2	*	1	Destination	0	0	255	+
3	SIP Server #2 - Src URI	Default_SBCRou	Yes	Normal	SIP Entity Server #2	*	1	Source	0	0	255	+

6.8 SIP Message Manipulation

The example requires that the SBC 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 host name "itsp" (e.g., 4410@itsp.com).

6.8.1 Step 1: Add a SIP Message Manipulation Rule

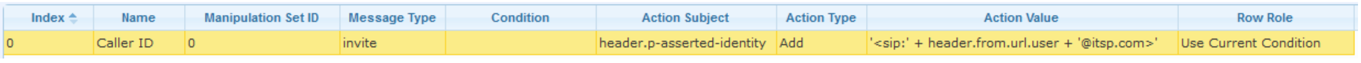
The caller ID is represented in SIP messages by the P-Asserted-Identity header. Therefore, you need to configure a manipulation rule that adds the header to INVITE messages. In addition, the value of the header must contain the user part, obtained from the From header, and the host name, "itsp". An example of such a P-Asserted-Identity header is shown below:

```
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,SUB
SCRIBE,UPDATE
User-Agent: Audiocodes-Sip-Gateway-Mediant/v.7.00A.004
P-Asserted-Identity: sip:1000@itsp.com
```

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

1. Open the Message Manipulations table (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Manipulations**).
2. Add the following manipulation rule:
   - **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 6-28: SIP Message Manipulation Rule



Index	Name	Manipulation Set ID	Message Type	Condition	Action Subject	Action Type	Action Value	Row Role
0	Caller ID	0	invite		header.p-asserted-identity	Add	'<sip:' + header.from.url.user + '@itsp.com>'	Use Current Condition

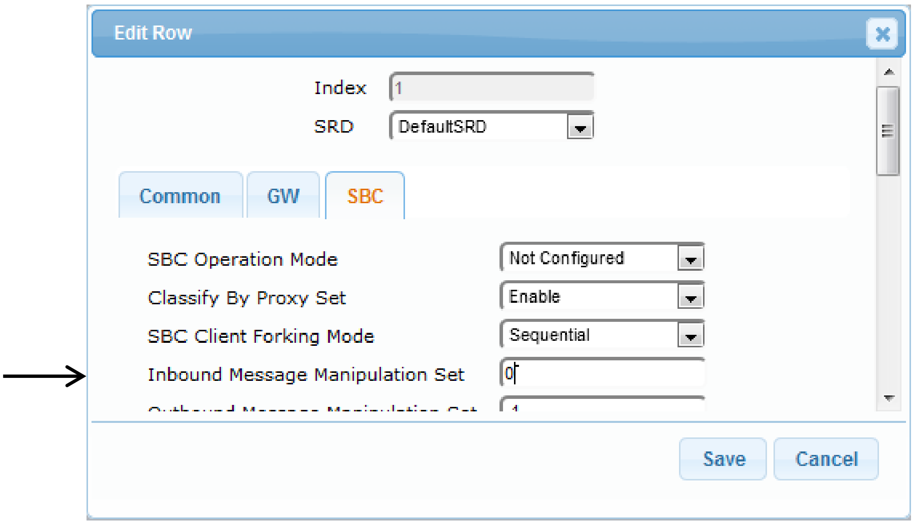
6.8.2 Step 2: Assign Manipulation Rule to IP Group of SIP Entity Server #2

As the SIP message manipulation rule must be performed on INVITE messages received from SIP Entity Server #2, you need to assign the rule (Index 0) 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 (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group Table**).
2. Edit the IP Group of SIP Entity Server #2:

Figure 6-29: Assigning Manipulation Rule to IP Group of SIP Entity Server #2



Index 1

SRD DefaultSRD

SBC Operation Mode Not Configured

Classify By Proxy Set Enable

SBC Client Forking Mode Sequential

Inbound Message Manipulation Set 0

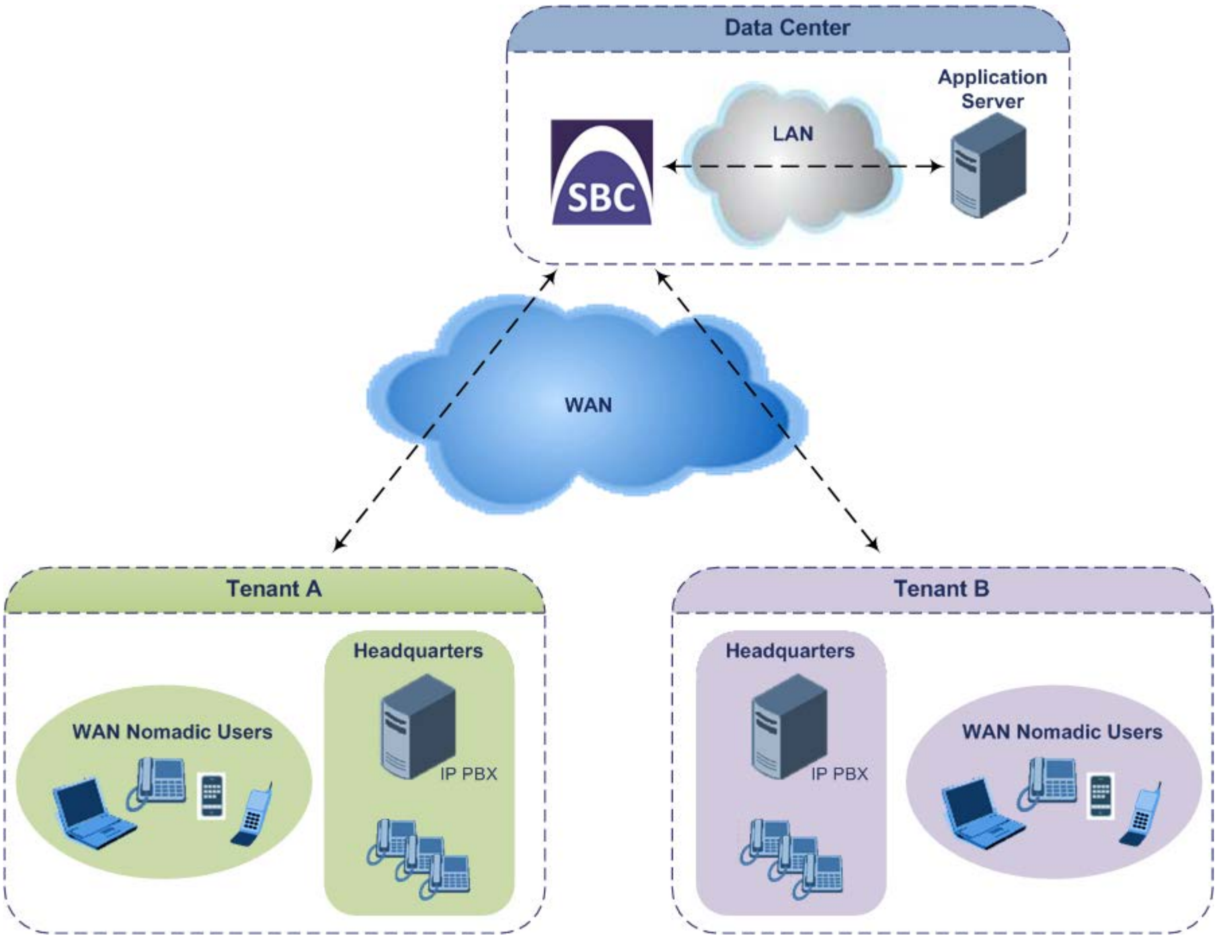
7 Multi-Tenant Deployment

Multi-tenant configuration can include the following topology: 1) all tenants share a common routing table, 2) semi-"bleeding" configuration topology, whereby each tenant has its' own routing table, but all share the resources of a common SIP entity (e.g., Application server or SIP trunk) and 3) fully, non-"bleeding" configuration topology (recommended), whereby each tenant has its own routing table without sharing any common resources (e.g., all use a dedicated Application server or SIP trunk).

This chapter provides a multi-tenant configuration example of a semi-"bleeding" topology:

- **Application:**
  - SBC at the Data Center with an Application Server, servicing all tenants (i.e., common resource)
  - Tenant A:
    - Local IP PBX
    - WAN Nomadic users
  - Tenant B:
    - Local IP PBX
    - WAN Nomadic users

Figure 7-1: Multi-Tenant Example Scenario



- **Topology:**
  - **SBC Logical IP Network Interface Connections:**
    - One logical network interface at IP address 10.33.4.11 for interfacing with the SIP Trunk provider over the LAN. The interface is also used for management (OAMP).
    - One logical network interface at IP address 212.199.200.90 for interfacing with the tenants through the DMZ and over WAN.
  - **SBC Physical LAN Port Connections:**
    - One Ethernet port connected to the LAN.
    - One Ethernet port connected to the DMZ (WAN).

A summary of the configuration topology is shown below:

Figure 7-2: Summary of Configuration Topology

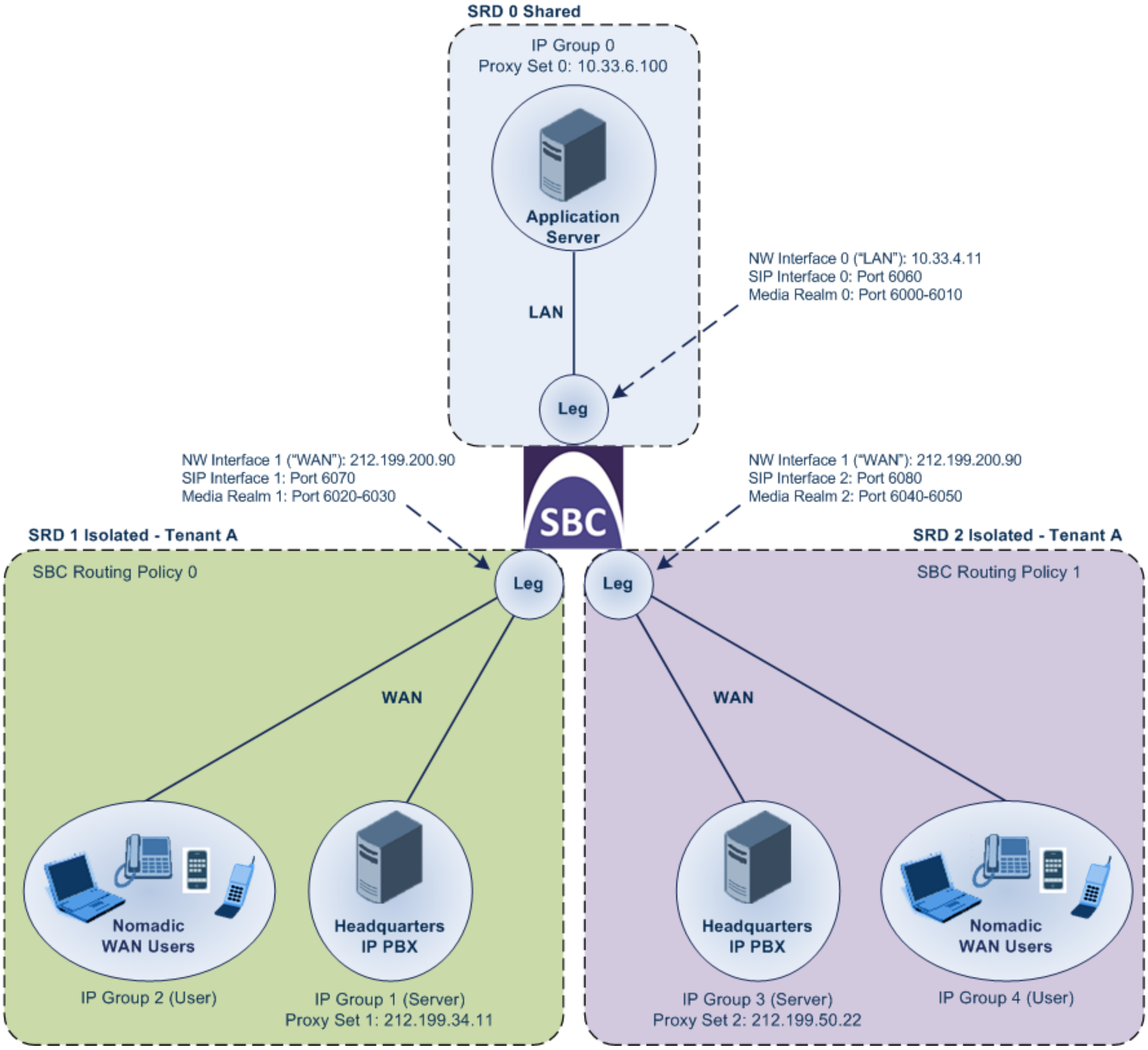

SRD 0 Shared
IP Group 0
Proxy Set 0: 10.33.6.100
Application Server
LAN
Leg
NW Interface 0 ("LAN"): 10.33.4.11
SIP Interface 0: Port 6060
Media Realm 0: Port 6000-6010
NW Interface 1 ("WAN"): 212.199.200.90
SIP Interface 1: Port 6070
Media Realm 1: Port 6020-6030
SBC
NW Interface 1 ("WAN"): 212.199.200.90
SIP Interface 2: Port 6080
Media Realm 2: Port 6040-6050
SRD 1 Isolated - Tenant A
SBC Routing Policy 0
Leg
WAN
Nomadic WAN Users
IP Group 2 (User)
Headquarters IP PBX
IP Group 1 (Server)
Proxy Set 1: 212.199.34.11
SRD 2 Isolated - Tenant A
SBC Routing Policy 1
Leg
WAN
Headquarters IP PBX
IP Group 3 (Server)
Proxy Set 2: 212.199.50.22
Nomadic WAN Users
IP Group 4 (User)

Table 7-1: Detailed Configuration Topology

Configuration Entity	Requirements	SRD
Logical NW Interfaces	Two: ▪ LAN (10.33.4.11) – interfaces with Application Server (and used for device OAMP management) in LAN ▪ WAN (212.199.200.90) – interfaces with tenants in the WAN	n/a
SRD	Three: ▪ SRD 0 – Application Server (Shared) ▪ SRD 1 - Tenant A (Isolated and Routing Policy 0) ▪ SRD 2 - Tenant B (Isolated and Routing Policy 1) Note: All configuration entities associated with SRD 0 can be used (shared) by all tenants.	n/a
Media Realm	Three: ▪ Media Realm 0 – Application Server (6000-6010; 2 sessions) ▪ Media Realm 1 – Tenant A (6020-6030; 2 sessions) ▪ Media Realm 2 – Tenant B (6040-6050; 2 sessions)	n/a
SIP Interface	Three:	
	▪ SIP Interface 0 – Application Server (6060) on LAN interface	▪ 0
	▪ SIP Interface 1 – Tenant A (6070) on WAN interface	▪ 1
	▪ SIP Interface 2 – Tenant B (6080) on WAN interface	▪ 2
Proxy Set	Three:	
	▪ Proxy Set 0 – Application Server (10.33.6.100 using UDP transport)	▪ 0
	▪ Proxy Set 1 – Tenant A (212.199.34.11 using UDP transport)	▪ 1
	▪ Proxy Set 2 – Tenant B (212.199.50.22 using UDP transport)	▪ 2
IP Group	Five:	
	▪ IP Group 0 – Application Server (Server-type)	▪ 0
	▪ IP Group 1 – Tenant A HQ IP-PBX (Server-type)	▪ 1
	▪ IP Group 2 – Tenant A Users	▪ 1
	▪ IP Group 3 – Tenant B HQ (Server-type)	▪ 2
	▪ IP Group 4 – Tenant B Users	▪ 2
Routing Policy	Two:	
	▪ Routing Policy 0 – Tenant A	n/a
	▪ Routing Policy 1 – Tenant B	n/a
Classification	Four: Incoming SIP dialogs from tenants are classified as received from the tenants’ IP Groups, by Proxy Set (i.e., IP address from where the dialog was received). IP Group 0 of the Application Server uses below Classification rules, which also associate the incoming dialogs to a Routing Policy of one of the tenant’s.	
	▪ Classification 0 – Classify all incoming dialogs received on SIP Interface 0 and source IP Group 0 (of Application Server) with destination prefix host name “tenant-a.com", classify them as belonging to Routing Policy 0 (Tenant A).	▪ 0

<table>
<tr><th>Configuration Entity</th><th colspan="3">Requirements</th><th>SRD</th></tr>
<tr><td rowspan="3"></td><td colspan="3">▪ Classification 1 – Classify all incoming dialogs received on SIP Interface 0 and source IP Group 0 (of Application Server) with destination prefix host name “tenant-b.com", classify them as belonging to Routing Policy 1 (Tenant B).</td><td>▪ 0</td></tr>
<tr><td colspan="3">▪ Classification 2 – Classify incoming calls from Tenant A's WAN nomadic users. The rule classifies calls received on Tenant A's SRD (SIP Interface) and whose destination prefix is "tenant-a.com", as belonging to the IP Group of Tenant A's WAN nomadic users ("Tenant-A Users").</td><td>▪ 1</td></tr>
<tr><td colspan="3">▪ Classification 3 - Classify incoming calls from Tenant B's WAN nomadic users. The rule classifies calls that are received on Tenant B's SRD (SIP Interface) and whose destination prefix is "tenant-b.com", as belonging to the IP Group of Tenant B's WAN nomadic users ("Tenant-B Users").</td><td>▪ 2</td></tr>
<tr><td rowspan="8">IP-to-IP Routing Rules</td><td colspan="4">Ten (five per tenant):</td></tr>
<tr><th colspan="2">Routing Policy 0 (Tenant A)</th><th colspan="2">Routing Policy 1 (Tenant B)</th></tr>
<tr><th>Source</th><th>Destination</th><th>Source</th><th>Destination</th></tr>
<tr><td>IP Group 0</td><td>IP Group 1</td><td>IP Group 0</td><td>IP Group 3</td></tr>
<tr><td>IP Group 1</td><td>IP Group 2 (users)</td><td>IP Group 3</td><td>IP Group 4 (users)</td></tr>
<tr><td>IP Group 1</td><td>IP Group 0
(alt. route if no users)</td><td>IP Group 3</td><td>IP Group 0
(alt. route if no users)</td></tr>
<tr><td>IP Group 2</td><td>IP Group 1</td><td>IP Group 4</td><td>IP Group 3</td></tr>
<tr><td>IP Group 2</td><td>IP Group 2
(call survivability)</td><td>IP Group 4</td><td>IP Group 4
(call survivability)</td></tr>
</table>

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

For the example, you need to add two logical IP network interfaces:

- **LAN:** IP address 10.33.4.11
- **WAN:** IP address 212.199.200.90

The example assumes that the OAMP network interface is also used for the LAN interface, which is already set up.

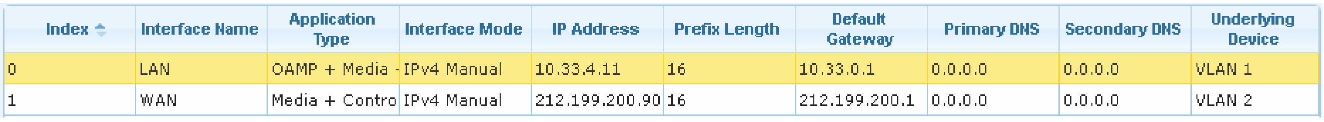
In addition, to apply your physical, Ethernet port separation between LAN and WAN traffic (configured previously), you need to assign the VLANs (*Underlying Device*) that you configured in Step 2, to the network interfaces, where:

- VLAN 1 (Ethernet Group 1) is assigned to the LAN interface
- VLAN 2 (Ethernet Group 2) is assigned to the WAN interface

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

1. Open the Interface table (**Configuration** tab > **VoIP** menu > **Network** > **IP Interfaces Table**).
2. Configure LAN and WAN interfaces:

Figure 7-3: Configured Logical IP Network Interfaces for LAN and WAN in Interface Table



Index	Interface Name	Application Type	Interface Mode	IP Address	Prefix Length	Default Gateway	Primary DNS	Secondary DNS	Underlying Device
0	LAN	OAMP + Media -	IPv4 Manual	10.33.4.11	16	10.33.0.1	0.0.0.0	0.0.0.0	VLAN 1
1	WAN	Media + Contro	IPv4 Manual	212.199.200.90	16	212.199.200.1	0.0.0.0	0.0.0.0	VLAN 2

7.2 Step 2: Add SBC Routing Policies

The SBC Routing Policy determines the IP-to-IP Routing "table" used for a specific tenant. Once configured, to apply the SBC Routing Policy you need to:

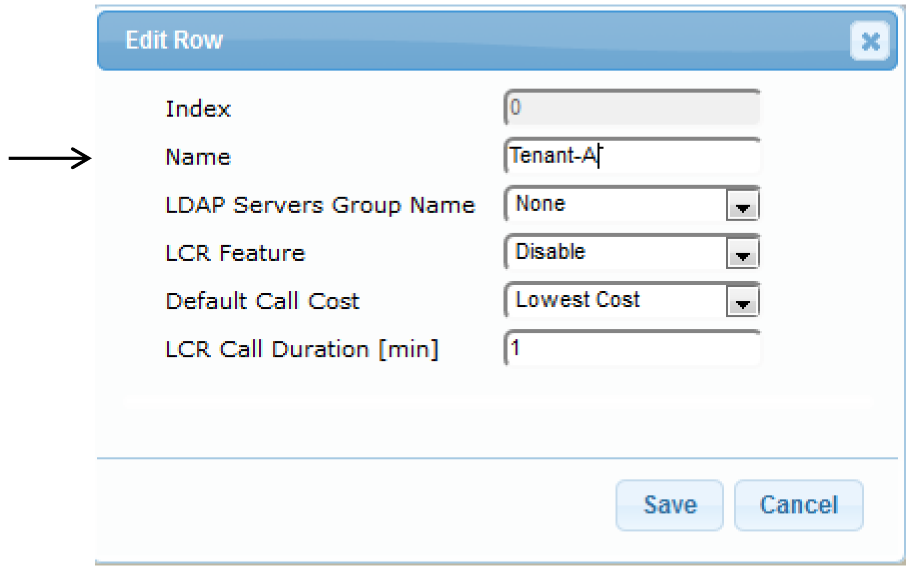
1. Associate it with a specific tenant by assigning it to the tenant’s SRD (in the SRD table).
2. Assign it to IP-to-IP Routing rules in the IP-to-IP Routing table.

In the example, two Routing Policies must be configured – one for Tenant A (Routing Policy at Index 0) and one for Tenant B (Routing Policy at Index 1).

➢ **To add Routing Policies:**

1. Open the SBC Routing Policy table (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > S**BC Routing Policy**).
2. Add a Routing Policy for Tenant A. You can use the default Routing Policy (Index 0), but modify it as shown below:

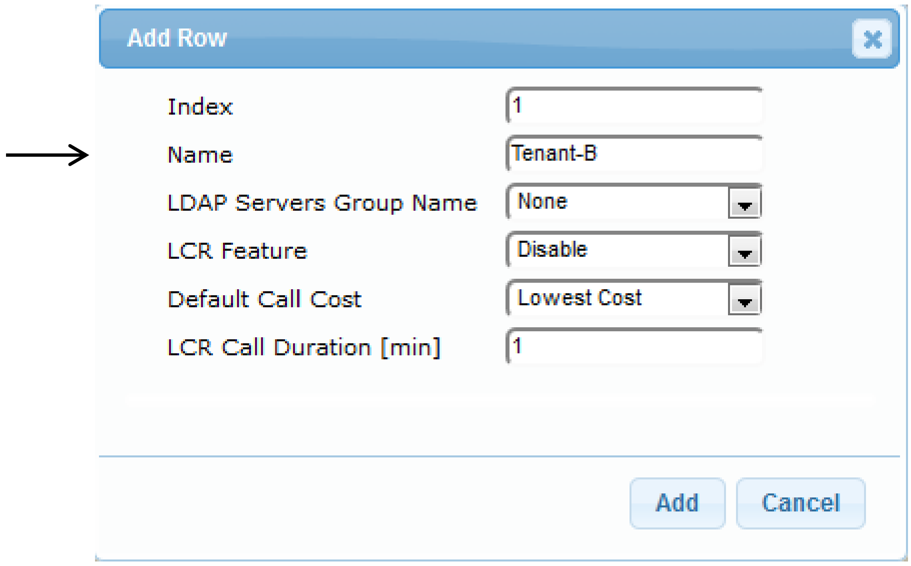
Figure 7-4: Routing Policy for Tenant A



Index	0
Name	Tenant-A
LDAP Servers Group Name	None
LCR Feature	Disable
Default Call Cost	Lowest Cost
LCR Call Duration [min]	1

3. Add a Routing Policy for Tenant B:

Figure 7-5: Routing Policy for Tenant B



Index	1
Name	Tenant-B
LDAP Servers Group Name	None
LCR Feature	Disable
Default Call Cost	Lowest Cost
LCR Call Duration [min]	1

7.3 Step 3: Add SRDs

The SRD represents a VoIP network and therefore, in the example, you need to configure SRDs for the following:

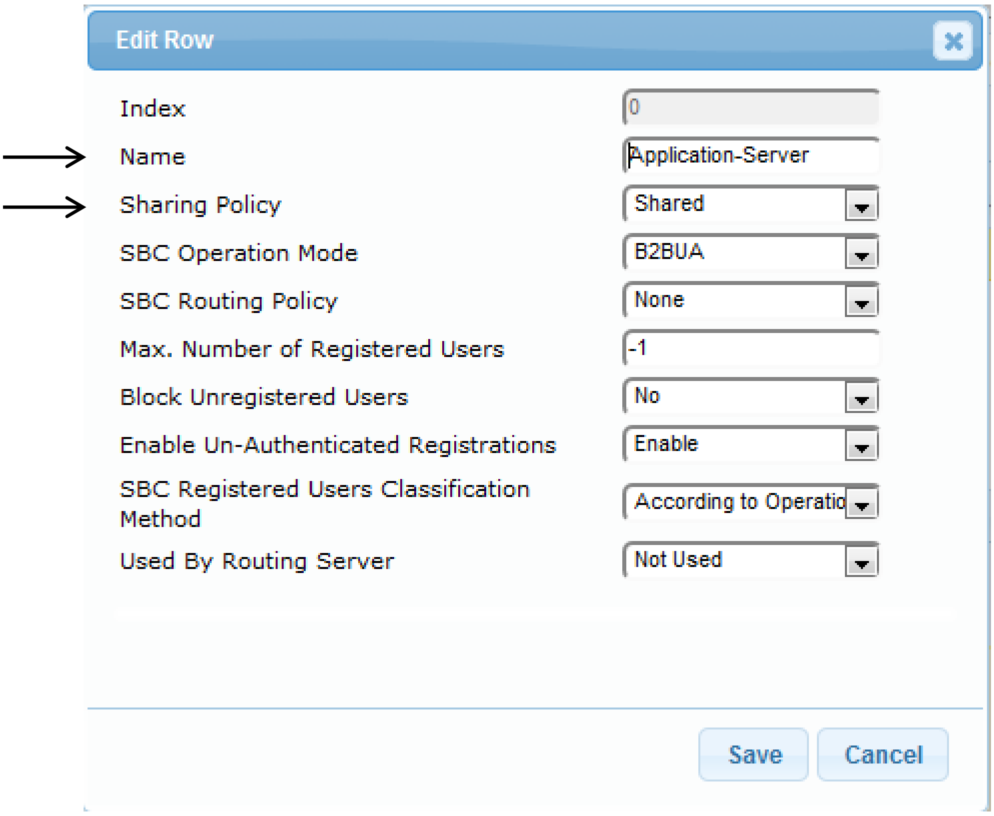
- Application Server at the datacenter: SRD 0
- Tenant A: SRD 1
- Tenant B: SRD 2

In addition, to create separate logical networks, you need to configure the tenant SRDs as Isolated. As both tenants use the same Application server, the SRD of the Application server must be configured as Shared (default).

➢ To add SRDs:

1. Open the SRD table (**Configuration** tab > **VoIP** menu > **VoIP Network** > **SRD Table**).
2. Add an SRD for the Application server. You can use the default SRD (Index 0), but modify it as shown below, where the 'Sharing Policy' is set to **Shared** (default):

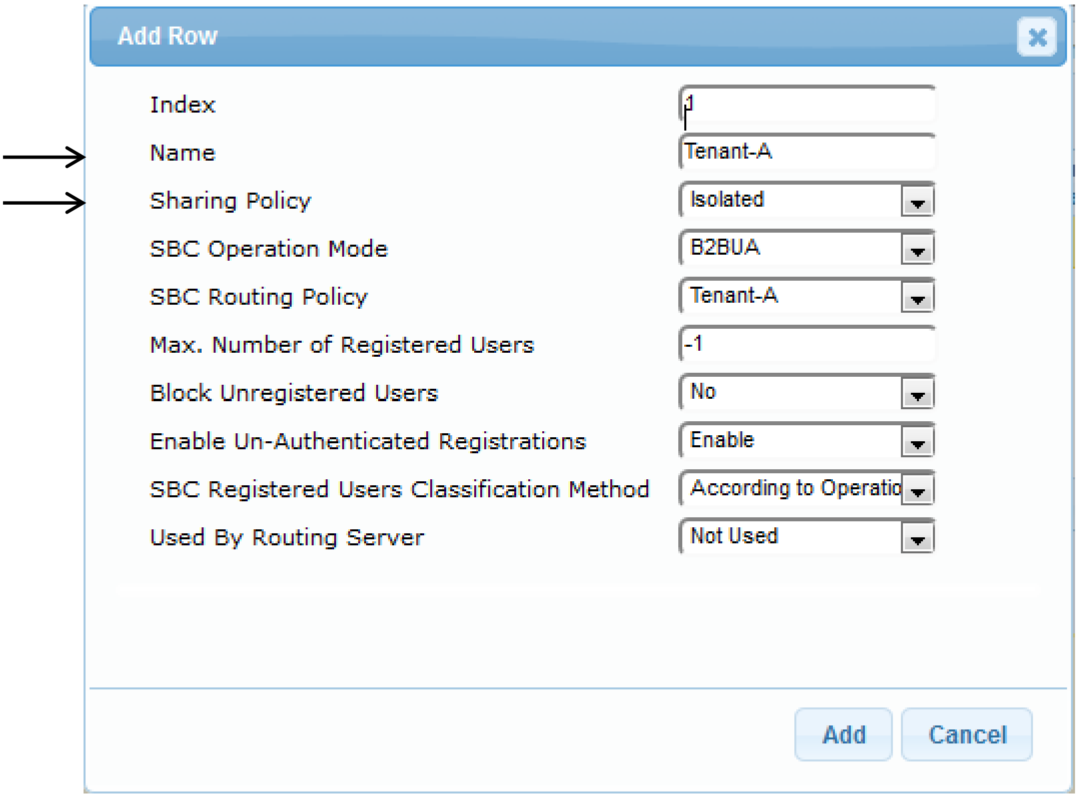
Figure 7-6: SRD for Application Server



Index	0
Name	Application-Server
Sharing Policy	Shared
SBC Operation Mode	B2BUA
SBC Routing Policy	None
Max. Number of Registered Users	-1
Block Unregistered Users	No
Enable Un-Authenticated Registrations	Enable
SBC Registered Users Classification Method	According to Operatio
Used By Routing Server	Not Used

3. Add an SRD for Tenant A and set the 'Sharing Policy' to **Isolated**:

Figure 7-7: SRD for Tenant A

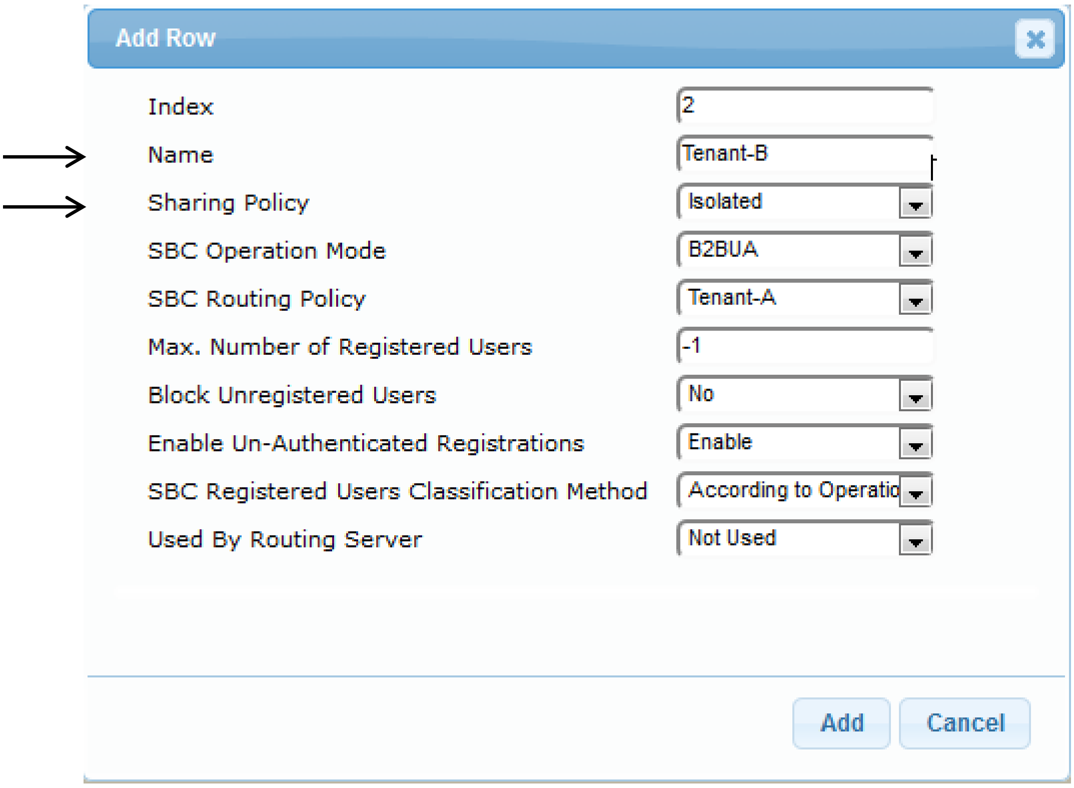


Add Row

Index	1
Name	Tenant-A
Sharing Policy	Isolated
SBC Operation Mode	B2BUA
SBC Routing Policy	Tenant-A
Max. Number of Registered Users	-1
Block Unregistered Users	No
Enable Un-Authenticated Registrations	Enable
SBC Registered Users Classification Method	According to Operatio
Used By Routing Server	Not Used

4. Add an SRD for Tenant B and set the ‘Sharing Policy’ to **Isolated**:

Figure 7-8: SRD for Tenant B



Add Row

Index	2
Name	Tenant-B
Sharing Policy	Isolated
SBC Operation Mode	B2BUA
SBC Routing Policy	Tenant-A
Max. Number of Registered Users	-1
Block Unregistered Users	No
Enable Un-Authenticated Registrations	Enable
SBC Registered Users Classification Method	According to Operatio
Used By Routing Server	Not Used

7.4 Step 4: Add Media Realms

Media Realms define a local port range for media (RTP) traffic on a specified local network interface. In the example, you need to configure Media Realms for the following:

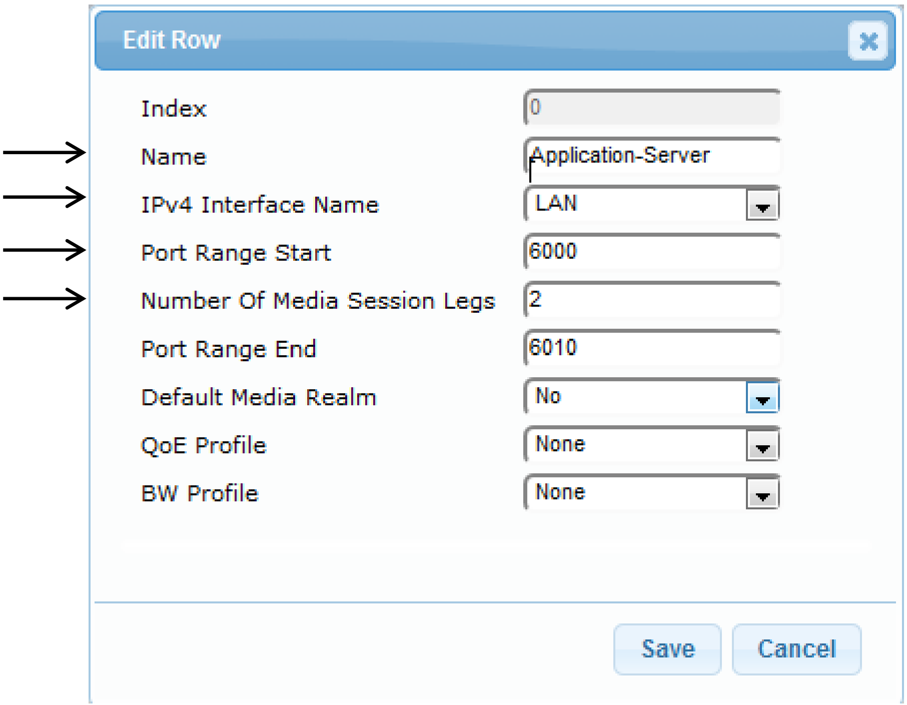
- Application server: Media Realm 0 on the LAN interface
- Tenant A: Media Realm 1 on the WAN interface
- Tenant B: Media Realm 2 on the WAN interface

You will later apply the Media Realms to your VoIP networks, by assigning them to the SIP Interfaces associated with the networks.

➢ To add Media Realms:

1. Open the Media Realm table (**Configuration** tab > **VoIP** menu > **VoIP Network** > **Media Realm Table**).
2. Add a Media Realm for the Application server on the LAN interface. You can use the default Media Realm (Index 0), but modify it as shown below:

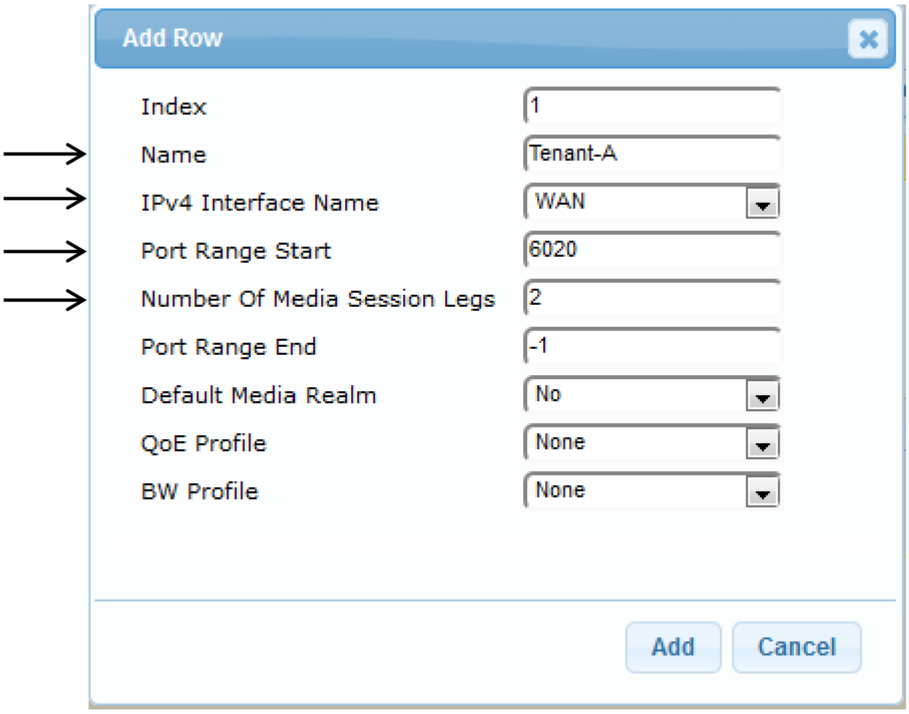
Figure 7-9: Media Realm for Application Server on LAN Interface



Index	0
Name	Application-Server
IPv4 Interface Name	LAN
Port Range Start	6000
Number Of Media Session Legs	2
Port Range End	6010
Default Media Realm	No
QoE Profile	None
BW Profile	None

3. Add a Media Realm for Tenant A on the WAN interface:

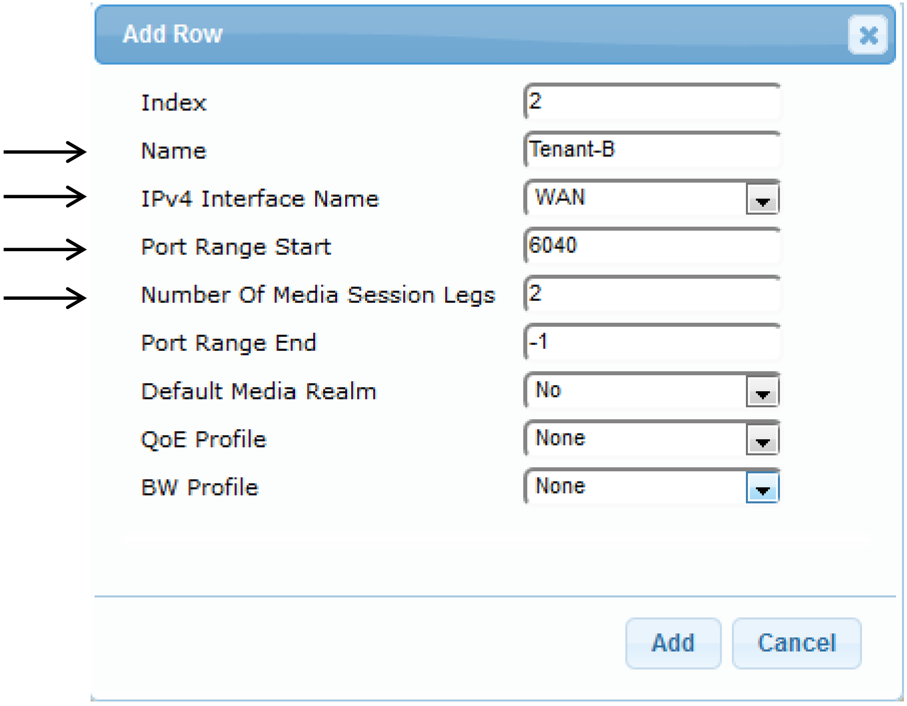
Figure 7-10: Media Realm for Tenant A on WAN Interface



Index	1
Name	Tenant-A
IPv4 Interface Name	WAN
Port Range Start	6020
Number Of Media Session Legs	2
Port Range End	-1
Default Media Realm	No
QoE Profile	None
BW Profile	None

4. Add a Media Realm for Tenant B on the WAN interface:

Figure 7-11: Media Realm for Tenant B on WAN Interface



Index	2
Name	Tenant-B
IPv4 Interface Name	WAN
Port Range Start	6040
Number Of Media Session Legs	2
Port Range End	-1
Default Media Realm	No
QoE Profile	None
BW Profile	None

Note: The 'Port Range End' parameter's value is automatically calculated (based on start port range and number of sessions) after you click **Add**.

7.5 Step 5: Add SIP Interfaces

The SIP Interface represents a Layer-3 network, defining the listening port for SIP signaling traffic on a specific network interface. In the example, you need to configure SIP Interfaces for the following:

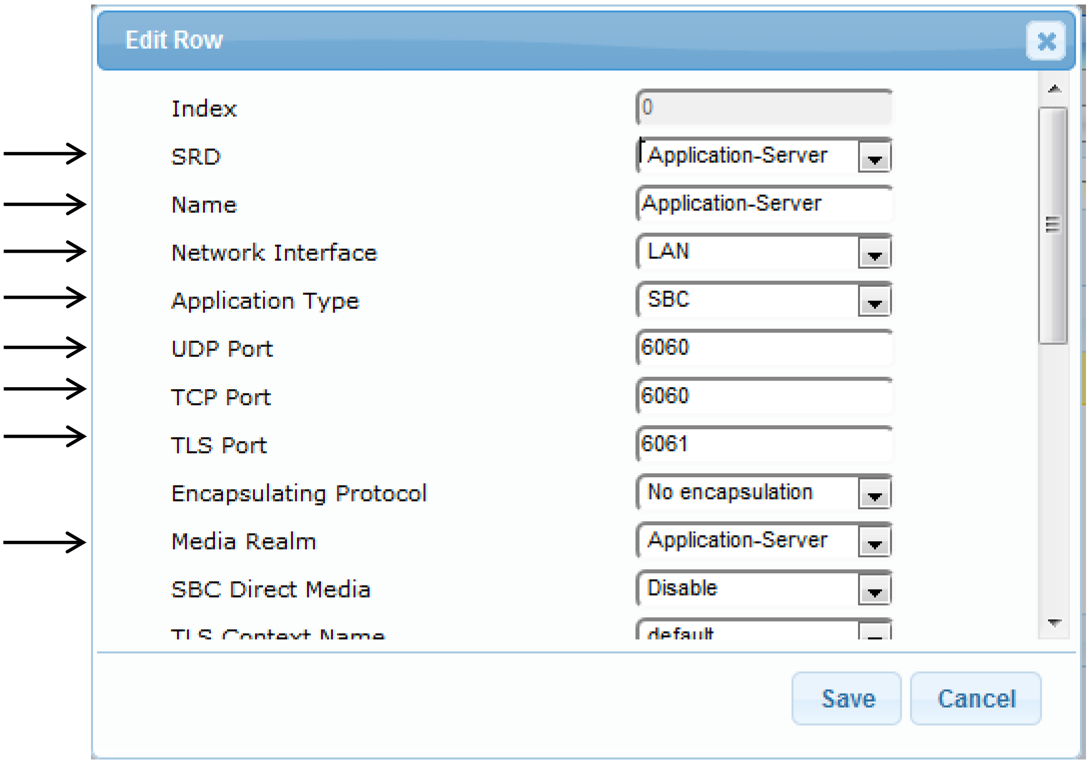
- Application server: SIP Interface 0 on the LAN interface
- Tenant A: SIP Interface 1 on the WAN interface
- Tenant B: SIP Interface 2 on the WAN interface

The SIP Interface is also associated with a Media Realm (which you configured in the previous step).

➢ **To add SIP Interfaces:**

1. Open the SIP Interface table (**Configuration** tab > **VoIP** menu > **VoIP Network** > **SIP Interface Table**).
2. Add a SIP Interface for the Application server on the LAN interface. You can use the default SIP Interface (Index 0), but modify it as shown below:

Figure 7-12: SIP Interface for Application Server on LAN Interface

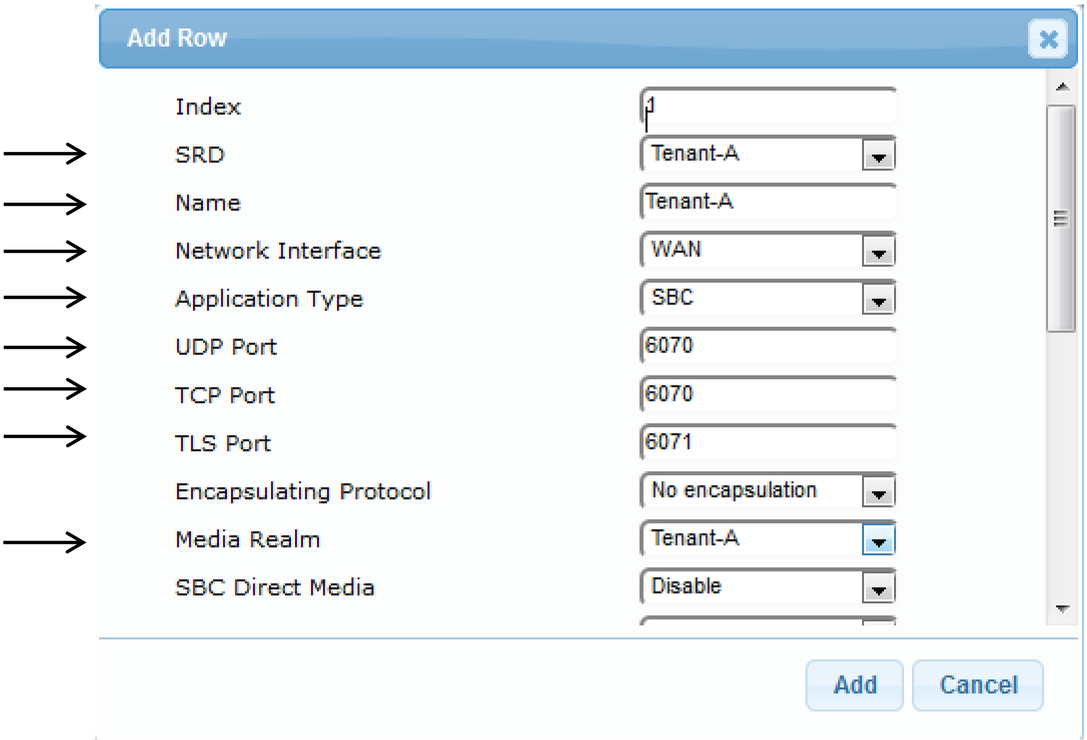


Edit Row

Index	0
SRD	Application-Server
Name	Application-Server
Network Interface	LAN
Application Type	SBC
UDP Port	6060
TCP Port	6060
TLS Port	6061
Encapsulating Protocol	No encapsulation
Media Realm	Application-Server
SBC Direct Media	Disable
TLS Context Name	default

3. Add a SIP Interface for Tenant A on the WAN interface:

Figure 7-13: SIP Interface for Tenant A on WAN Interface

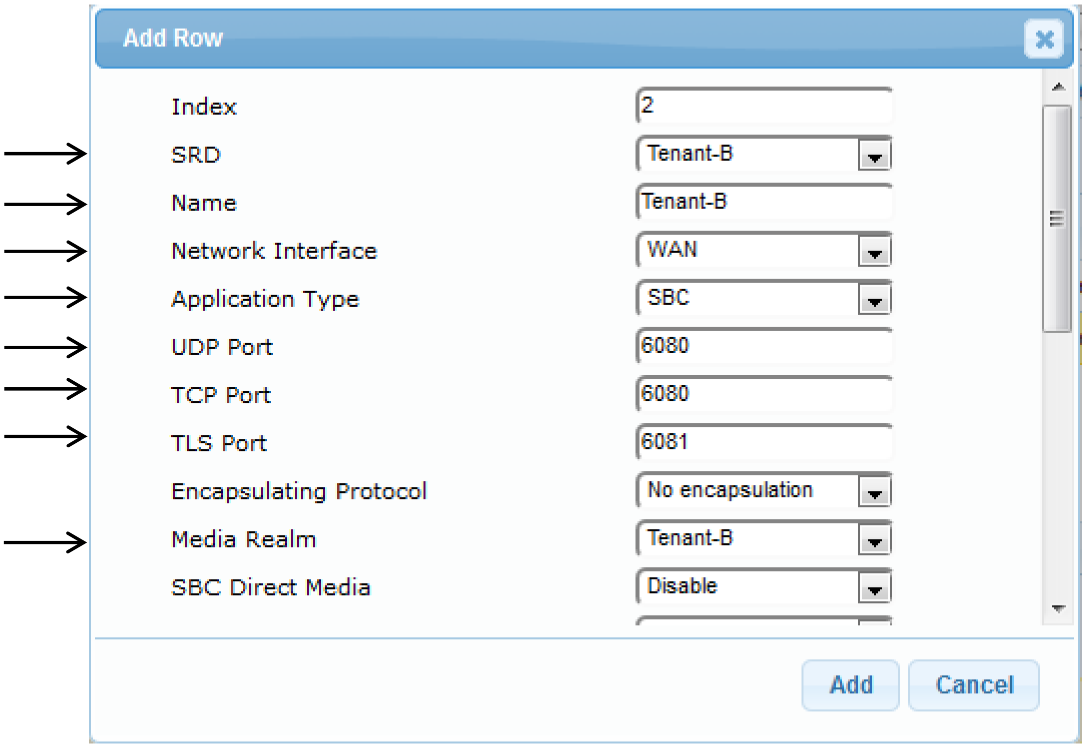


Add Row

Index	1
SRD	Tenant-A
Name	Tenant-A
Network Interface	WAN
Application Type	SBC
UDP Port	6070
TCP Port	6070
TLS Port	6071
Encapsulating Protocol	No encapsulation
Media Realm	Tenant-A
SBC Direct Media	Disable

4. Add a SIP Interface for Tenant B on WAN Interface:

Figure 7-14: SIP Interface for Tenant B on WAN Interface

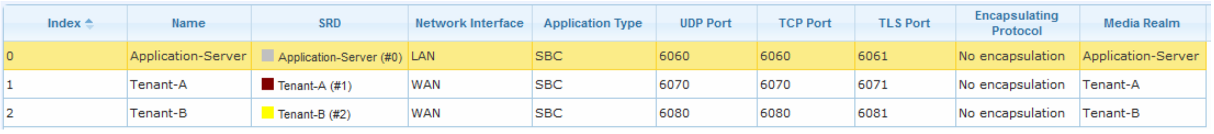


Add Row

Index	2
SRD	Tenant-B
Name	Tenant-B
Network Interface	WAN
Application Type	SBC
UDP Port	6080
TCP Port	6080
TLS Port	6081
Encapsulating Protocol	No encapsulation
Media Realm	Tenant-B
SBC Direct Media	Disable

Once you have configured the SIP Interfaces, the SIP Interface table should appear populated as shown below:

Figure 7-15: Configured SIP Interfaces in the SIP Interface Table



Index	Name	SRD	Network Interface	Application Type	UDP Port	TCP Port	TLS Port	Encapsulating Protocol	Media Realm
0	Application-Server	Application-Server (#0)	LAN	SBC	6060	6060	6061	No encapsulation	Application-Server
1	Tenant-A	Tenant-A (#1)	WAN	SBC	6070	6070	6071	No encapsulation	Tenant-A
2	Tenant-B	Tenant-B (#2)	WAN	SBC	6080	6080	6081	No encapsulation	Tenant-B

7.6 Step 6: Add Proxy Sets

The Proxy Set defines the actual address of SIP server entities in your network. In the example, you need to configure Proxy Sets for the following:

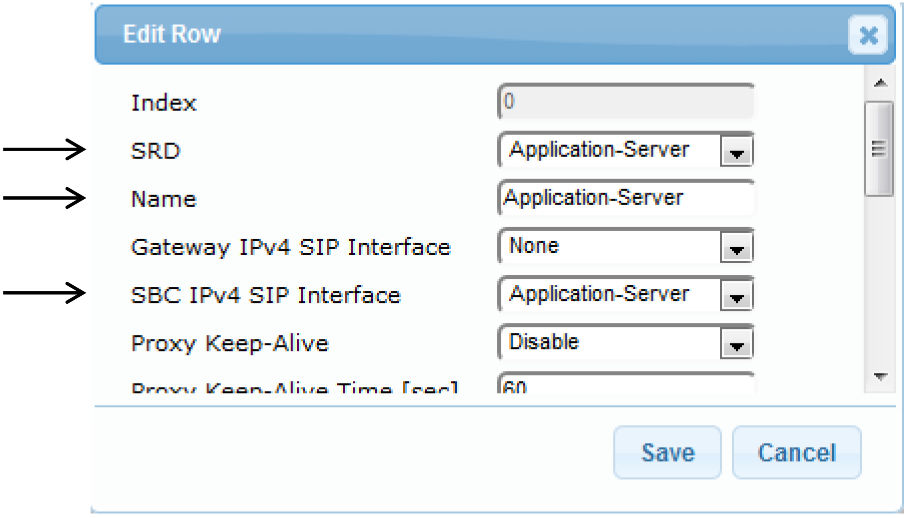
- Application Server: Proxy Set 0 with IP address 10.33.6.100
- Tenant A: Proxy Set 0 with IP address 212.199.34.11
- Tenant B: Proxy Set 0 with IP address 212.199.50.22

You will later apply the Proxy Sets to your VoIP networks, by assigning them to their corresponding IP Groups.

➢ **To add Proxy Sets:**

1. Open the Proxy Sets table (**Configuration** tab > **VoIP** menu > **VoIP Network** > **Proxy Sets Table**).
2. Add a Proxy Set for the Application Server. You can use the default Proxy Set (Index 0), but modify it as shown below:
   a. Add the Proxy Set:

Figure 7-16: Proxy Set for Application Server



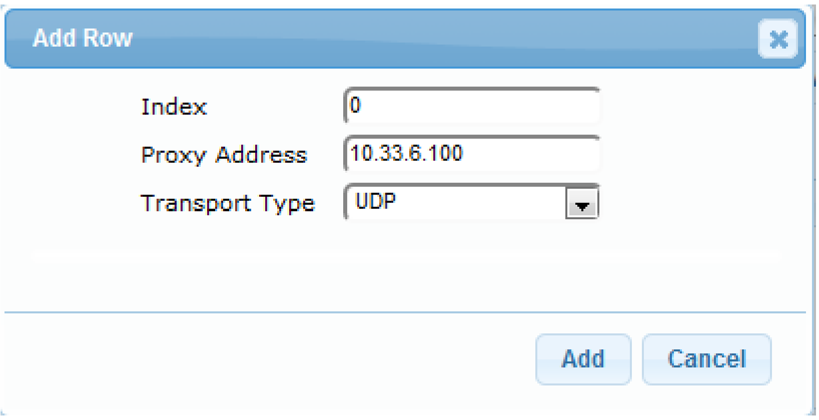
Edit Row

Index	0
SRD	Application-Server
Name	Application-Server
Gateway IPv4 SIP Interface	None
SBC IPv4 SIP Interface	Application-Server
Proxy Keep-Alive	Disable
Proxy Keep-Alive Time [sec]	60

   b. Select the table row of the Proxy Set that you added, and then click the **Proxy Address Table** link located below the table.

c. Add the IP address of the Application server:

Figure 7-17: Proxy Set Address for IP PBX

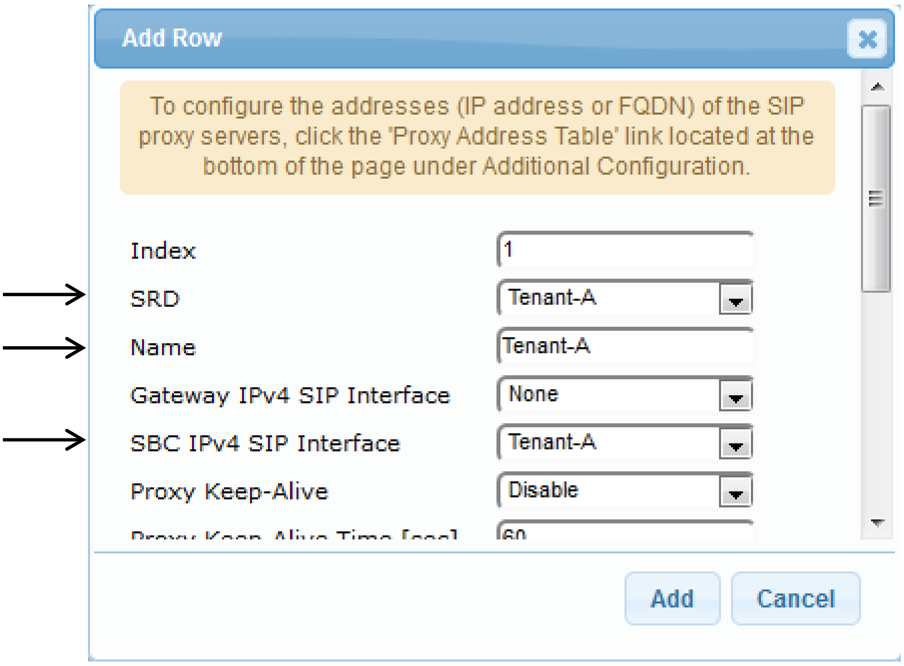


Index	0
Proxy Address	10.33.6.100
Transport Type	UDP

3. Add a Proxy Set for Tenant A:

a. Add the Proxy Set:

Figure 7-18: Proxy Set for Tenant A



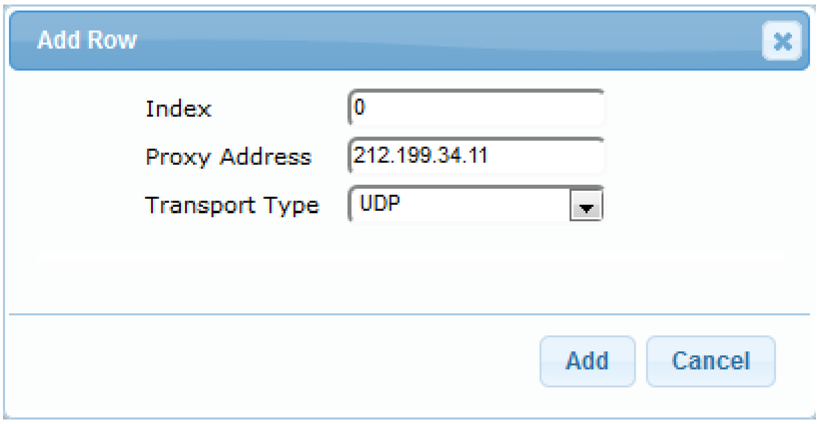
To configure the addresses (IP address or FQDN) of the SIP proxy servers, click the 'Proxy Address Table' link located at the bottom of the page under Additional Configuration.

Index	1
SRD	Tenant-A
Name	Tenant-A
Gateway IPv4 SIP Interface	None
SBC IPv4 SIP Interface	Tenant-A
Proxy Keep-Alive	Disable
Proxy Keep-Alive Time [sec]	60

b. Select the table row of the Proxy Set that you added, and then click the **Proxy Address Table** link located below the table.

c. Add the IP address of Tenant A:

Figure 7-19: Proxy Set Address for Tenant A

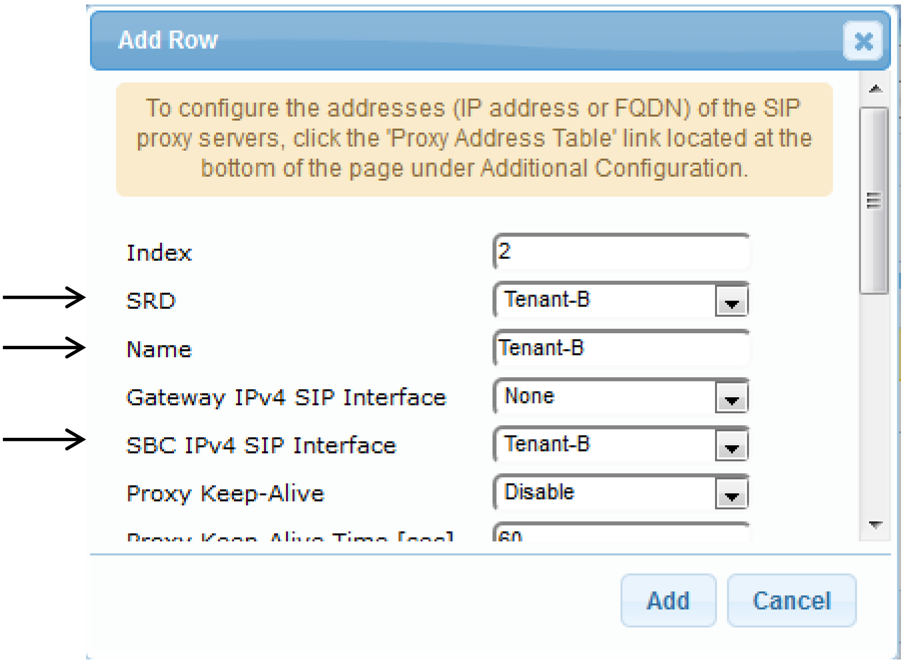


Index	0
Proxy Address	212.199.34.11
Transport Type	UDP

4. Add a Proxy Set for Tenant B:

a. Add the Proxy Set:

Figure 7-20: Proxy Set for Tenant B



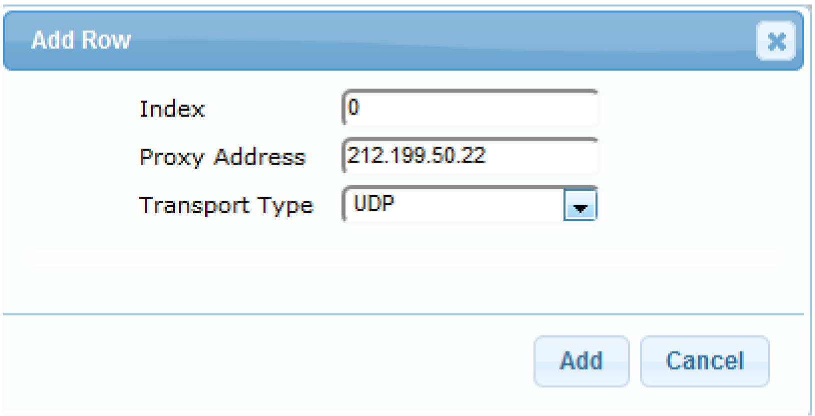
To configure the addresses (IP address or FQDN) of the SIP proxy servers, click the 'Proxy Address Table' link located at the bottom of the page under Additional Configuration.

Index	2
SRD	Tenant-B
Name	Tenant-B
Gateway IPv4 SIP Interface	None
SBC IPv4 SIP Interface	Tenant-B
Proxy Keep-Alive	Disable
Proxy Keep-Alive Time [sec]	60

b. Select the table row of the Proxy Set that you added, and then click the **Proxy Address Table** link located below the table.

c. Add the IP address of Tenant B:

Figure 7-21: Proxy Set Address for Tenant B



Index: 0

Proxy Address: 212.199.50.22

Transport Type: UDP

7.7 Step 7: Add IP Groups

The IP Group represents the SIP entity with which the device sends and receives calls. In the example, you need to add IP Groups for the following:

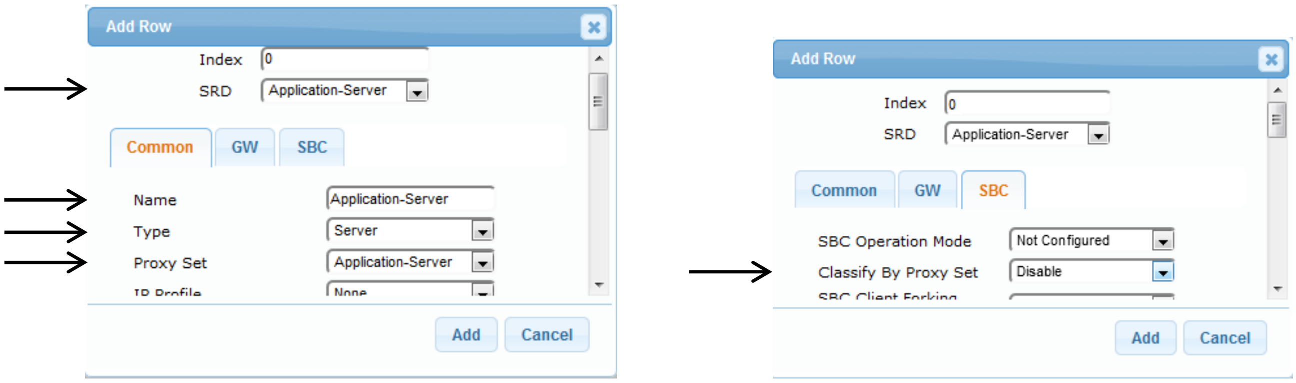
- Application Server: Server-type IP Group 0
- Tenant A:
  - IP-PBX at HQ: Server-type IP Group 1
  - Nomadic users: User-type IP Group 2
- Tenant B:
  - IP-PBX at HQ: Server-type IP Group 3
  - Nomadic users: User-type IP Group 4

For the Server-type IP Groups (except the Application server), you need to enable classification of incoming SIP dialogs to the IP Groups, based on Proxy Set (i.e., based on the source IP address). As the Application server is used by both tenants, classification by Proxy Set can't be used; instead, classification rules, configured later in the Classification table, must be configured (see Section 7.8). For the User-type IP Groups, classification is also based on Classification rules.

➢ To add IP Groups:

1. Open the IP Group table (**Configuration** tab > **VoIP** menu > **VoIP Network** > **IP Group Table**).
2. Add an IP Group for the Application server (disable Classification by Proxy Set):

Figure 7-22: IP Group for Application Server

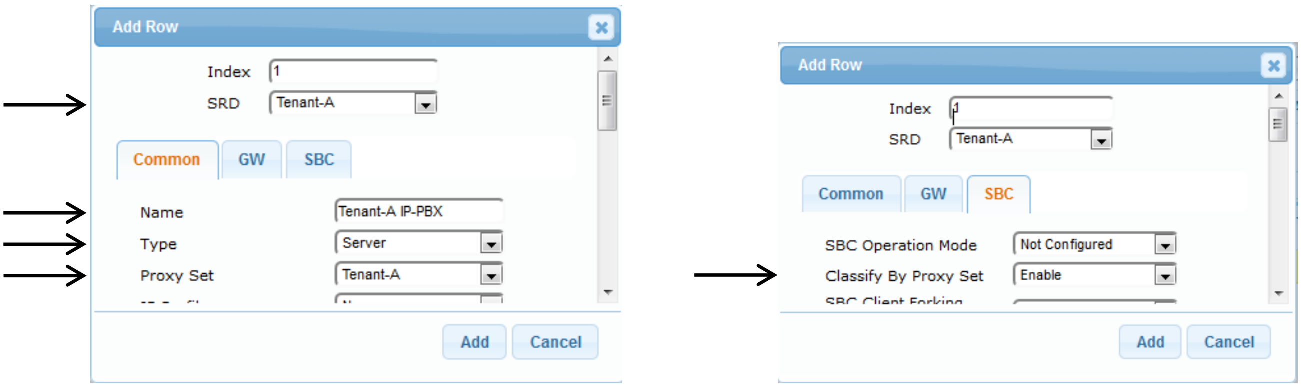


Index 0
SRD Application-Server
Name Application-Server
Type Server
Proxy Set Application-Server
IP Profile None

Index 0
SRD Application-Server
SBC Operation Mode Not Configured
Classify By Proxy Set Disable
SBC Client Forking

3. Add IP Groups for Tenant A:
   a. Add an IP Group for the IP-PBX of Tenant A:

Figure 7-23: IP Group for Tenant A IP-PBX

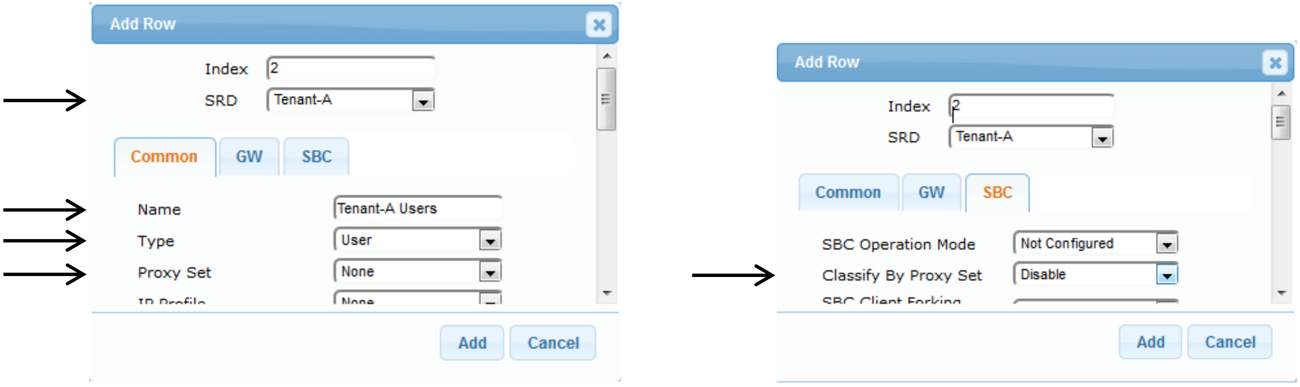


Index 1
SRD Tenant-A
Name Tenant-A IP-PBX
Type Server
Proxy Set Tenant-A

Index 1
SRD Tenant-A
SBC Operation Mode Not Configured
Classify By Proxy Set Enable
SBC Client Forking

   b. Add an IP Group for the nomadic WAN users of Tenant A:

Figure 7-24: IP Group for Tenant-A WAN Nomadic Users



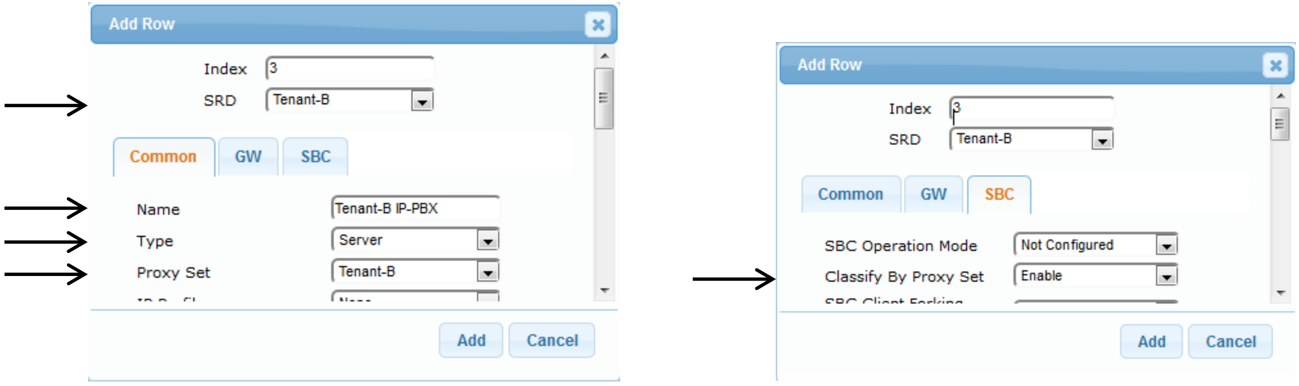
Index 2
SRD Tenant-A
Name Tenant-A Users
Type User
Proxy Set None
IP Profile None

Index 2
SRD Tenant-A
SBC Operation Mode Not Configured
Classify By Proxy Set Disable
SBC Client Forking

4. Add IP Groups for Tenant B:

   a. Add an IP Group for the IP-PBX of Tenant B:

Figure 7-25: IP Group for Tenant B IP-PBX



Add Row

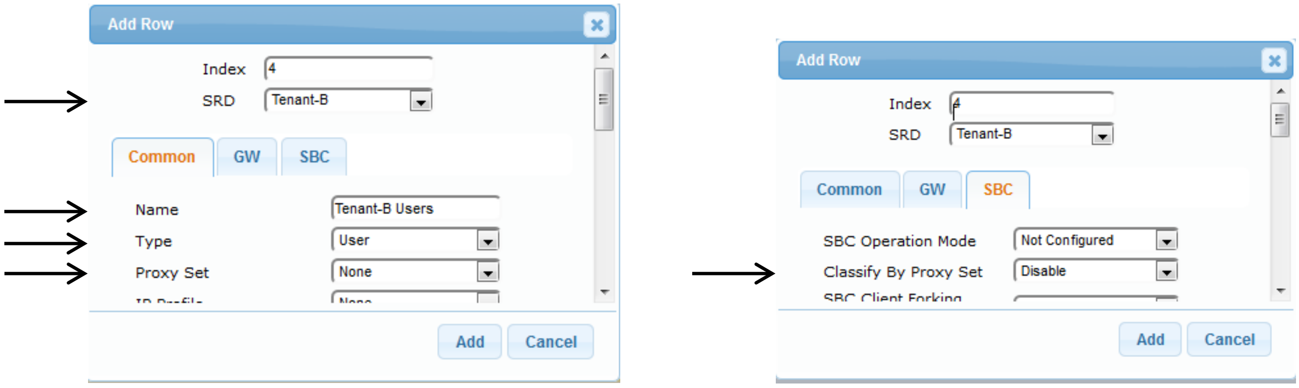
Index: 3
SRD: Tenant-B

Common tab:
Name: Tenant-B IP-PBX
Type: Server
Proxy Set: Tenant-B

SBC tab:
SBC Operation Mode: Not Configured
Classify By Proxy Set: Enable

   b. Add an IP Group for the nomadic WAN users of Tenant B:

Figure 7-26: IP Group for Tenant-B WAN Nomadic Users



Add Row

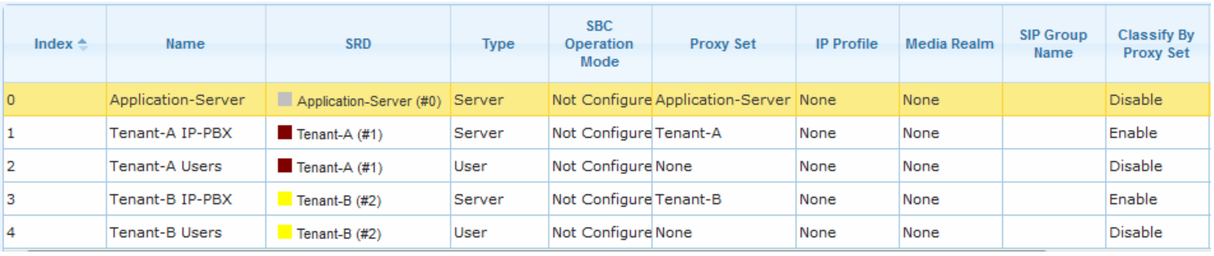
Index: 4
SRD: Tenant-B

Common tab:
Name: Tenant-B Users
Type: User
Proxy Set: None

SBC tab:
SBC Operation Mode: Not Configured
Classify By Proxy Set: Disable

Once you have configured the IP Groups, the IP Group table should appear populated as shown below:

Figure 7-27: Configured IP Groups in the IP Group Table



Index	Name	SRD	Type	SBC Operation Mode	Proxy Set	IP Profile	Media Realm	SIP Group Name	Classify By Proxy Set
0	Application-Server	⬜ Application-Server (#0)	Server	Not Configure	Application-Server	None	None		Disable
1	Tenant-A IP-PBX	🟥 Tenant-A (#1)	Server	Not Configure	Tenant-A	None	None		Enable
2	Tenant-A Users	🟥 Tenant-A (#1)	User	Not Configure	None	None	None		Disable
3	Tenant-B IP-PBX	🟨 Tenant-B (#2)	Server	Not Configure	Tenant-B	None	None		Enable
4	Tenant-B Users	🟨 Tenant-B (#2)	User	Not Configure	None	None	None		Disable

7.8 Step 8: Add Classification Rules

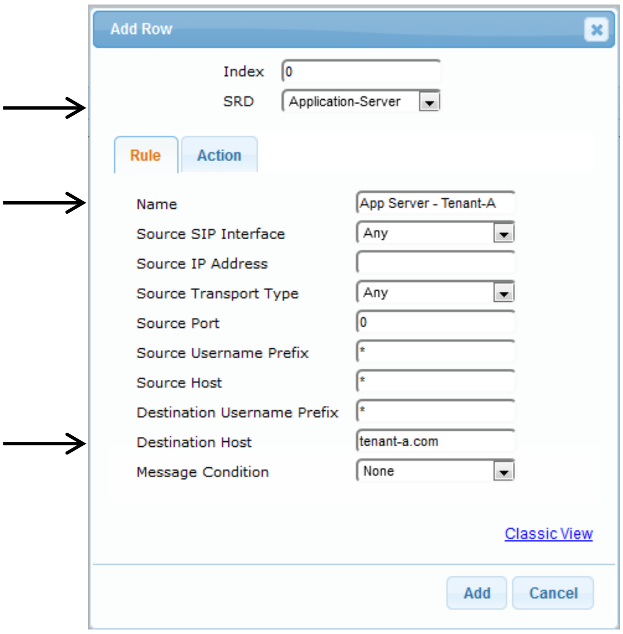
In the example, you need to add the following Classification rules:

- **Classify calls from the Application server:** You need to classify incoming calls from the Application server as belonging to its' IP Group (as classification by Proxy Set was disabled for this IP Group – see Section 7.7). In addition, classification must also determine which tenant's routing table (i.e., Routing Policy) to use in order to route the call to the destination. Thus, you need to add two Classification rules (one for each tenant):
    - Classify incoming calls that are received on the Application Server's SRD (SIP Interface) and with destination hostname “tenant-a.com", as belonging to IP Group "Application-Server" and assign the calls to the Routing Policy of Tenant A.
    - Classify incoming calls that are received on the Application Server's SRD (SIP Interface) and with destination hostname “tenant-b.com", as belonging to IP Group "Application-Server" and assign the calls to the Routing Policy of Tenant B.
- **Classify calls from WAN nomadic users:** For the SBC to identify calls from WAN nomadic users and classify them to their respective User-type IP Groups (which you configured in Section 7.7), you need to add the following Classification rules.
    - Tenant A: Classify incoming calls that are received on Tenant A's SRD (SIP Interface) and whose destination prefix is “tenant-a.com”, as belonging to the IP Group of Tenant A's WAN nomadic users ("Tenant-A Users").
    - Tenant B: Classify incoming calls that are received on Tenant B's SRD (SIP Interface) and whose destination prefix is “tenant-b.com”, as belonging to the IP Group of Tenant B's WAN nomadic users ("Tenant-B Users").

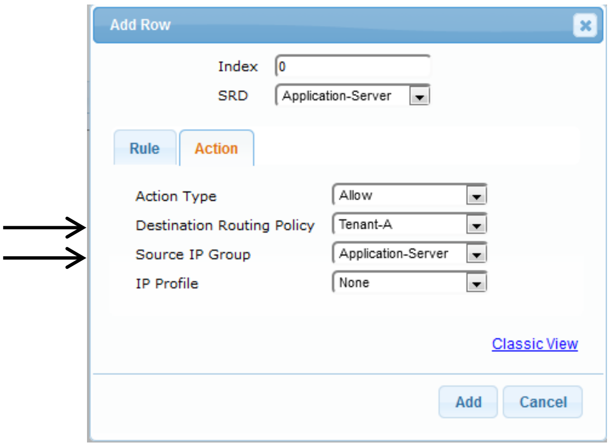
➢ To add classification rule the nomadic users:

1. Open the Classification table (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **Classification Table**).
2. Add Classification rules for classifying incoming calls to the Application server's IP Group:
   a. Incoming calls for Tenant A (i.e., assigns to Routing Policy "Tenant-A"):

Figure 7-28: Classification Rule for Calls from Application Server to Tenant A



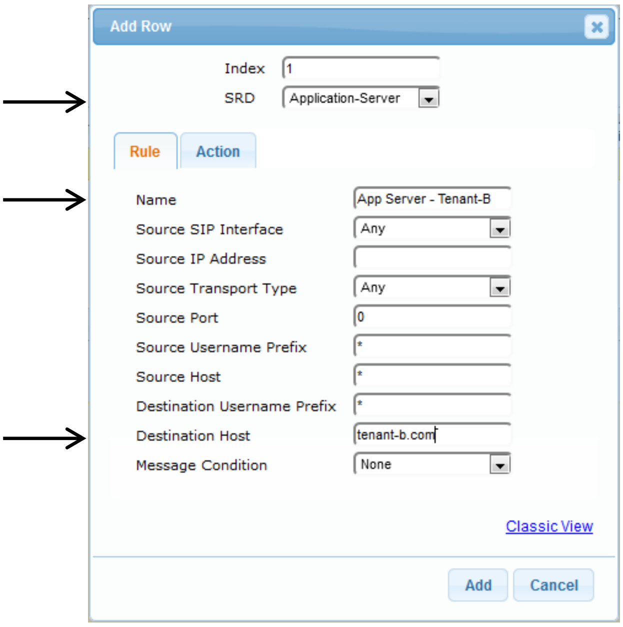
Index: 0
SRD: Application-Server
Name: App Server - Tenant-A
Source SIP Interface: Any
Source IP Address:
Source Transport Type: Any
Source Port: 0
Source Username Prefix: *
Source Host: *
Destination Username Prefix: *
Destination Host: tenant-a.com
Message Condition: None



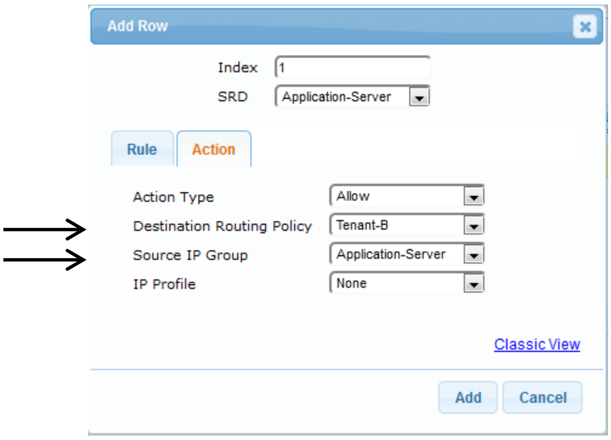
Index: 0
SRD: Application-Server
Action Type: Allow
Destination Routing Policy: Tenant-A
Source IP Group: Application-Server
IP Profile: None

   b. Incoming calls for Tenant B (i.e., assigns to Routing Policy "Tenant-B"):

Figure 7-29: Classification Rule for Calls from Application Server to Tenant B



Index: 1
SRD: Application-Server
Name: App Server - Tenant-B
Source SIP Interface: Any
Source IP Address:
Source Transport Type: Any
Source Port: 0
Source Username Prefix: *
Source Host: *
Destination Username Prefix: *
Destination Host: tenant-b.com
Message Condition: None

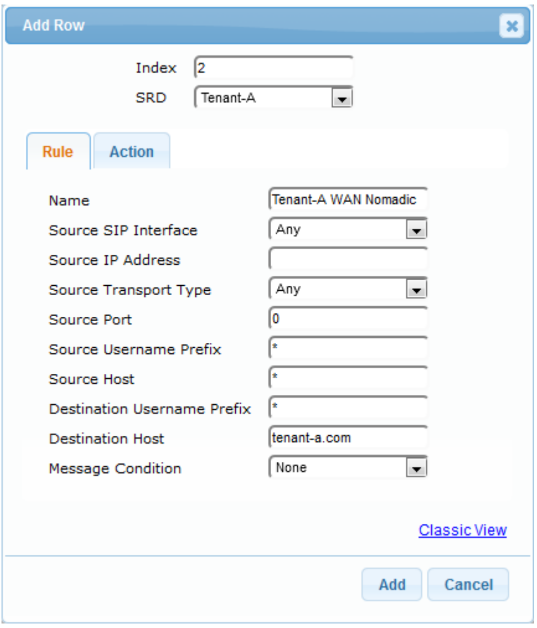


Index: 1
SRD: Application-Server
Action Type: Allow
Destination Routing Policy: Tenant-B
Source IP Group: Application-Server
IP Profile: None

3. Add Classification rules for classifying incoming calls to the WAN Nomadic users' IP Group:

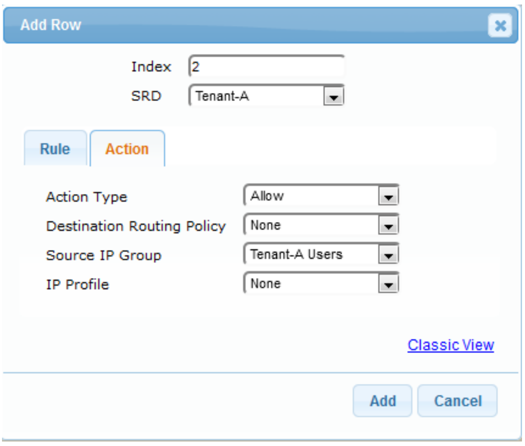
   a. Tenant A:

Figure 7-30: Classification Rule for Calls from WAN Nomadic Users of Tenant A



Index: 2
SRD: Tenant-A

Name: Tenant-A WAN Nomadic
Source SIP Interface: Any
Source IP Address:
Source Transport Type: Any
Source Port: 0
Source Username Prefix: *
Source Host: *
Destination Username Prefix: *
Destination Host: tenant-a.com
Message Condition: None

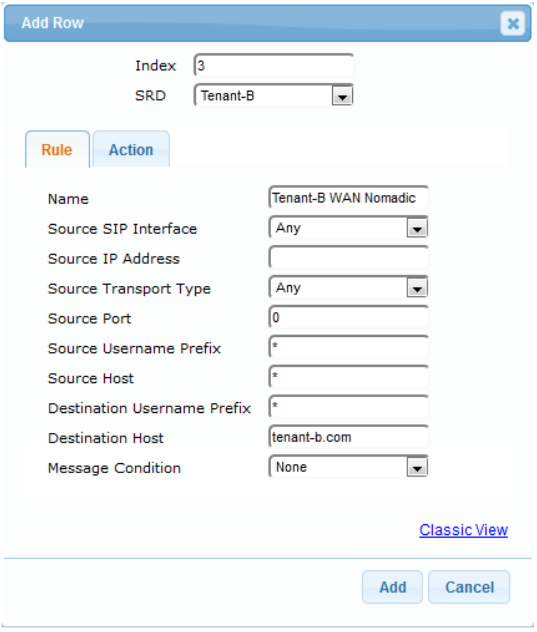


Index: 2
SRD: Tenant-A

Action Type: Allow
Destination Routing Policy: None
Source IP Group: Tenant-A Users
IP Profile: None

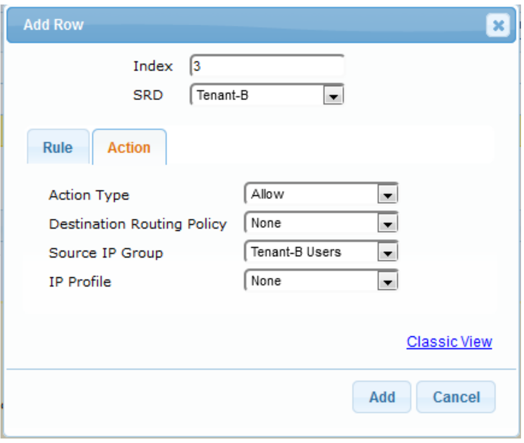
   b. Tenant B:

Figure 7-31: Classification Rule for Calls from WAN Nomadic Users of Tenant B



Index: 3
SRD: Tenant-B

Name: Tenant-B WAN Nomadic
Source SIP Interface: Any
Source IP Address:
Source Transport Type: Any
Source Port: 0
Source Username Prefix: *
Source Host: *
Destination Username Prefix: *
Destination Host: tenant-b.com
Message Condition: None

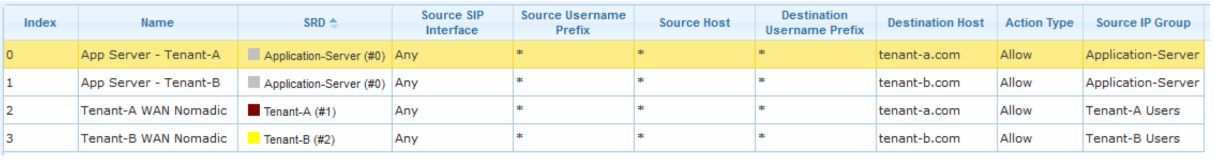


Index: 3
SRD: Tenant-B

Action Type: Allow
Destination Routing Policy: None
Source IP Group: Tenant-B Users
IP Profile: None

Once you have configured the Classification rules, the Classification table should appear populated as shown below:

Figure 7-32: Configured Classification Rules in the Classification Table



Index	Name	SRD ▲	Source SIP Interface	Source Username Prefix	Source Host	Destination Username Prefix	Destination Host	Action Type	Source IP Group
0	App Server - Tenant-A	⬜ Application-Server (#0)	Any	*	*	*	tenant-a.com	Allow	Application-Server
1	App Server - Tenant-B	⬜ Application-Server (#0)	Any	*	*	*	tenant-b.com	Allow	Application-Server
2	Tenant-A WAN Nomadic	🟥 Tenant-A (#1)	Any	*	*	*	tenant-a.com	Allow	Tenant-A Users
3	Tenant-B WAN Nomadic	🟨 Tenant-B (#2)	Any	*	*	*	tenant-b.com	Allow	Tenant-B Users

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

Each tenant is configured with its own set of routing rules in the IP-to-IP Routing table, logically grouped by its' SBC Routing Policy. Thus, the Routing Policy creates a dedicated routing "table" for each tenant. In the example, each tenant has its own Routing Policy, which you configured in Section 7.2 on page 71 and assigned to the tenant SRDs in Section 7.3 on page 72.

The call routing rules use the IP Groups of these entities to denote the source and destination of the call. In the example, you need to add the following call routing rules per tenant (Routing Policy):

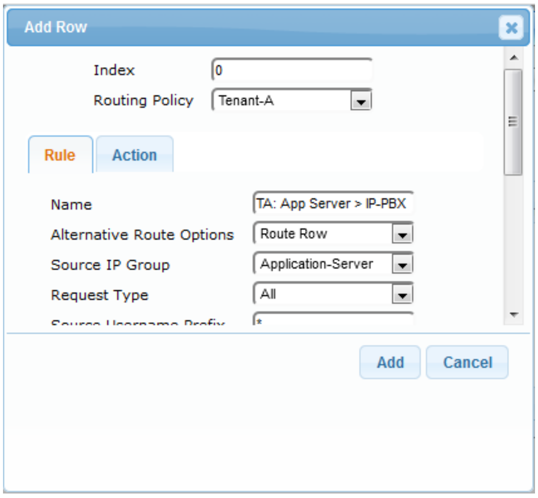
Tenant A (Routing Policy 0)			Tenant B (Routing Policy 1)		
Source	**Destination**	**Description**	**Source**	**Destination**	**Description**
IP Group 0	**IP Group 1**	Call routing from Application server to HQ IP-PBX	**IP Group 0**	**IP Group 3**	Call routing from Application server to HQ IP-PBX
IP Group 1	**IP Group 2**	Call routing from HQ IP-PBX to WAN nomadic users	**IP Group 3**	**IP Group 4**	Call routing from HQ IP-PBX to WAN nomadic users
IP Group 1	**IP Group 0**	Call routing from HQ IP-PBX to Application server, if unable to route to WAN nomadic users (alternative route for previous rule)	**IP Group 3**	**IP Group 0**	Call routing from HQ IP-PBX to Application server, if unable to route to WAN nomadic users (alternative route for previous rule)
IP Group 2	**IP Group 1**	Call routing from WAN nomadic users to HQ IP-PBX	**IP Group 4**	**IP Group 3**	Call routing from WAN nomadic users to HQ IP-PBX
IP Group 2	**IP Group 2**	Call routing between WAN nomadic users, if unable to route to HQ IP-PBX (alternative route for previous rule – call survivability)	**IP Group 4**	**IP Group 4**	Call routing between WAN nomadic users, if unable to route to HQ IP-PBX (alternative route for previous rule – call survivability)

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

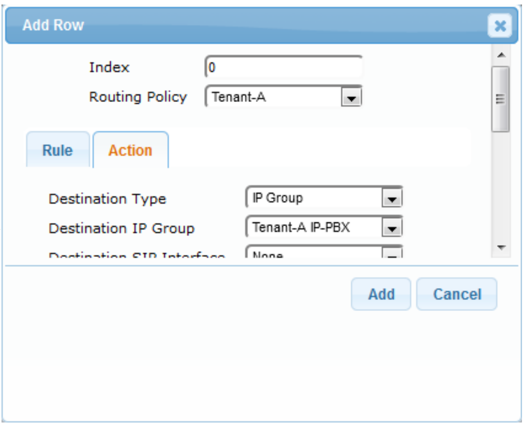
1. Open the IP-to-IP Routing table (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **IP-to-IP Routing Table**).
2. **Add routing rules for Tenant A:**

    a. Add a rule for routing calls from Application Server to the HQ IP PBX:

Figure 7-33: Call Routing Rule - Application Server to HQ IP PBX for Tenant A



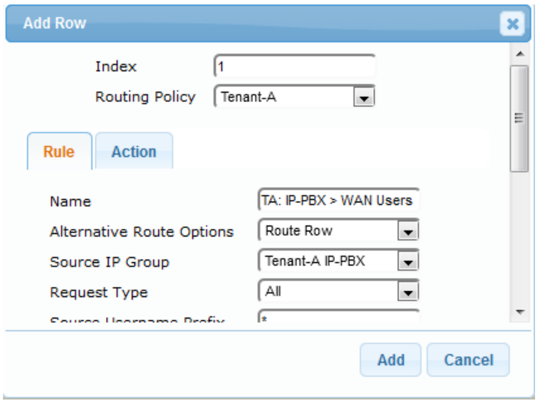
Index	0
Routing Policy	Tenant-A
Name	TA: App Server > IP-PBX
Alternative Route Options	Route Row
Source IP Group	Application-Server
Request Type	All
Source Username Prefix	*



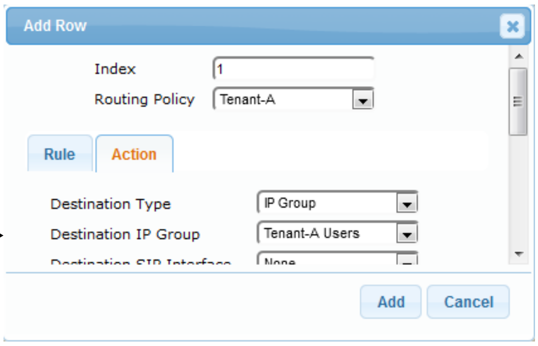
Index	0
Routing Policy	Tenant-A
Destination Type	IP Group
Destination IP Group	Tenant-A IP-PBX
Destination SIP Interface	None

b. Add a rule for routing calls from HQ IP PBX to WAN nomadic users:

Figure 7-34: Call Routing Rule - HQ IP PBX to WAN Nomadic Users for Tenant A



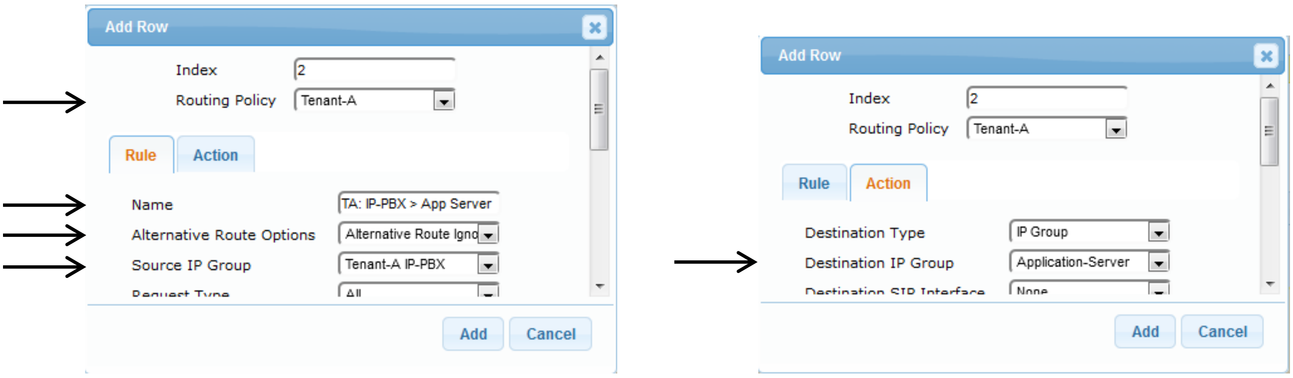
Index	1
Routing Policy	Tenant-A
Name	TA: IP-PBX > WAN Users
Alternative Route Options	Route Row
Source IP Group	Tenant-A IP-PBX
Request Type	All
Source Username Prefix	*



Index	1
Routing Policy	Tenant-A
Destination Type	IP Group
Destination IP Group	Tenant-A Users
Destination SIP Interface	None

c. Add a rule for routing calls from HQ IP-PBX to Application server, if unable to route to WAN nomadic users (alternative route for previous rule):

Figure 7-35: Alternative Routing Rule - HQ IP PBX to Application Server for Tenant A



Add Row

Index: 2
Routing Policy: Tenant-A

Rule | Action

Name: TA: IP-PBX > App Server
Alternative Route Options: Alternative Route Igno
Source IP Group: Tenant-A IP-PBX
Request Type: All

Add | Cancel

Add Row

Index: 2
Routing Policy: Tenant-A

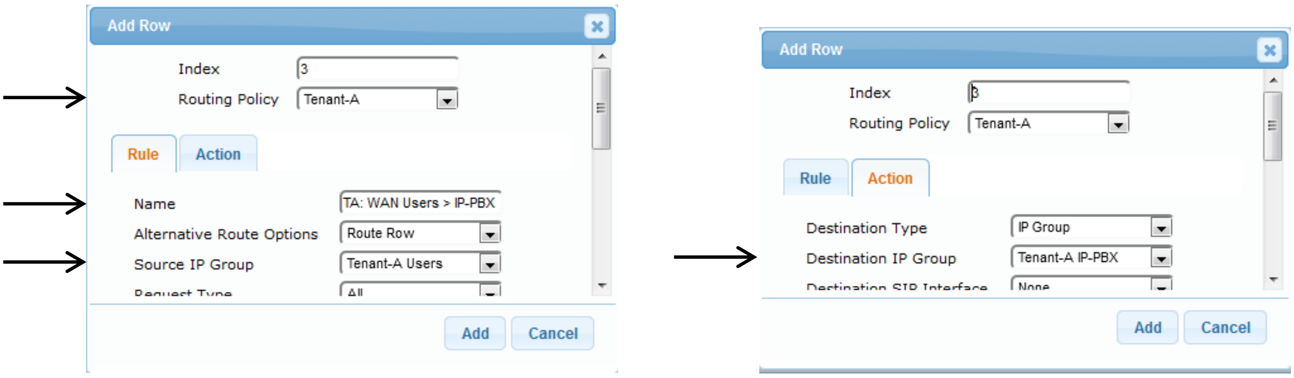
Rule | Action

Destination Type: IP Group
Destination IP Group: Application-Server
Destination SIP Interface: None

Add | Cancel

d. Add a rule for routing calls from WAN nomadic users to HQ IP-PBX:

Figure 7-36: Routing Rule - WAN Nomadic Users to HQ IP-PBX for Tenant A



Add Row

Index: 3
Routing Policy: Tenant-A

Rule | Action

Name: TA: WAN Users > IP-PBX
Alternative Route Options: Route Row
Source IP Group: Tenant-A Users
Request Type: All

Add | Cancel

Add Row

Index: 3
Routing Policy: Tenant-A

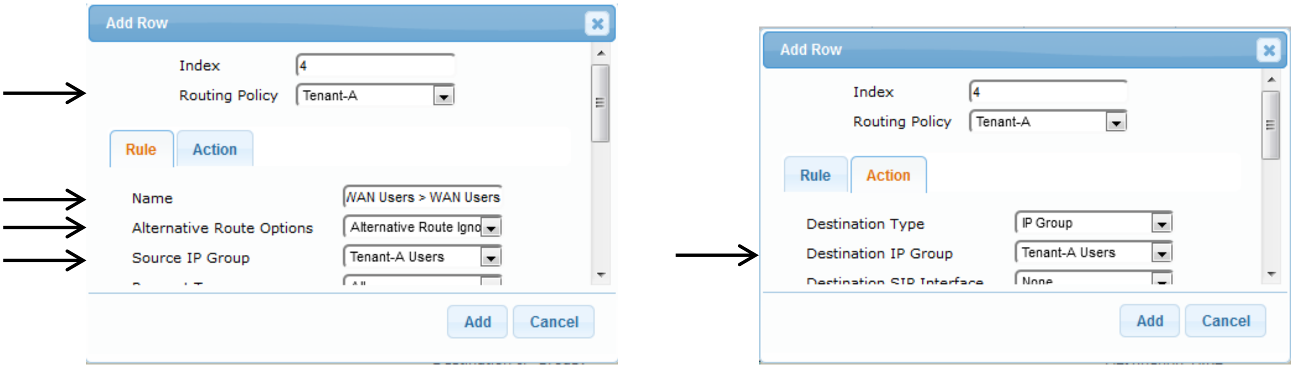
Rule | Action

Destination Type: IP Group
Destination IP Group: Tenant-A IP-PBX
Destination SIP Interface: None

Add | Cancel

e. Add a rule for routing calls between WAN nomadic users, if unable to route to HQ IP-PBX (alternative route for previous rule – call survivability):

Figure 7-37: Alternative Routing Rule – Call Survivability of WAN Nomadic Users for Tenant A



Add Row

Index: 4
Routing Policy: Tenant-A

Rule | Action

Name: WAN Users > WAN Users
Alternative Route Options: Alternative Route Igno
Source IP Group: Tenant-A Users

Add | Cancel

Add Row

Index: 4
Routing Policy: Tenant-A

Rule | Action

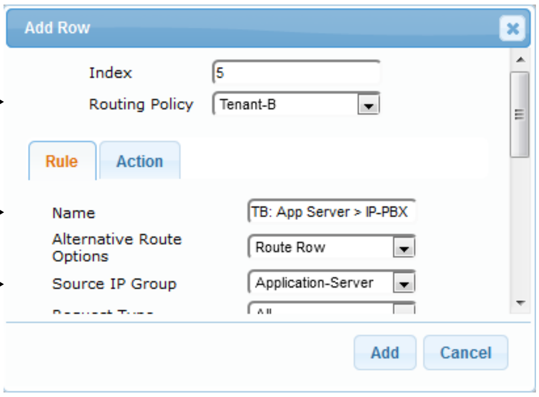
Destination Type: IP Group
Destination IP Group: Tenant-A Users
Destination SIP Interface: None

Add | Cancel

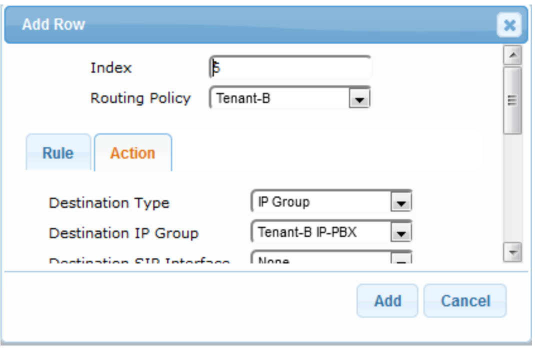
3. **Add routing rules for Tenant B:**

   a. Add a rule for routing calls from Application Server to the HQ IP PBX:

Figure 7-38: Call Routing Rule - Application Server to HQ IP PBX for Tenant B



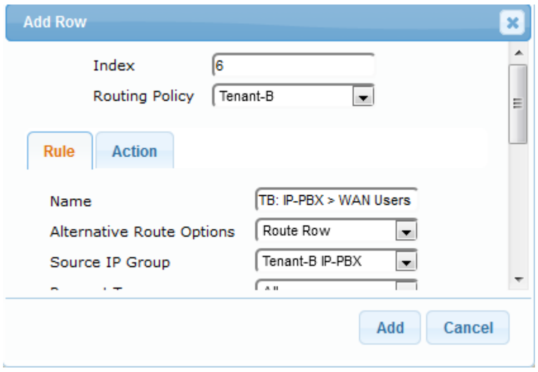
Index	5
Routing Policy	Tenant-B
Name	TB: App Server > IP-PBX
Alternative Route Options	Route Row
Source IP Group	Application-Server
Request Type	All



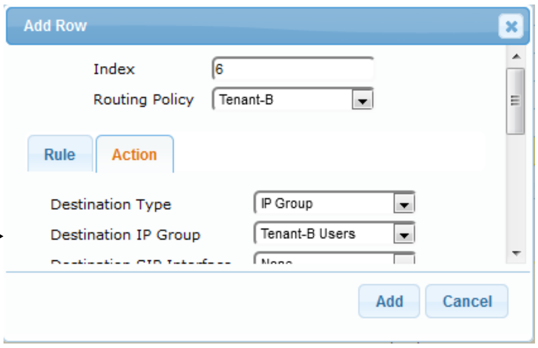
Index	5
Routing Policy	Tenant-B
Destination Type	IP Group
Destination IP Group	Tenant-B IP-PBX
Destination SIP Interface	None

   b. Add a rule for routing calls from HQ IP PBX to WAN nomadic users:

Figure 7-39: Call Routing Rule - HQ IP PBX to WAN Nomadic Users for Tenant B



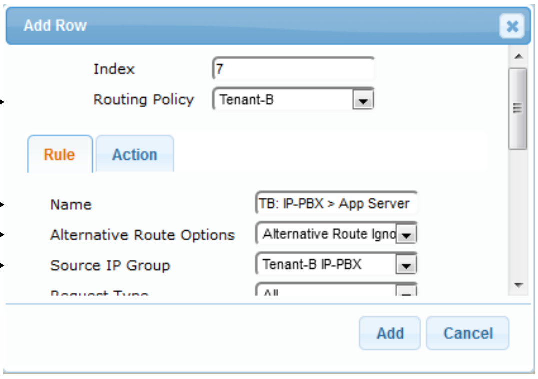
Index	6
Routing Policy	Tenant-B
Name	TB: IP-PBX > WAN Users
Alternative Route Options	Route Row
Source IP Group	Tenant-B IP-PBX
Request Type	All



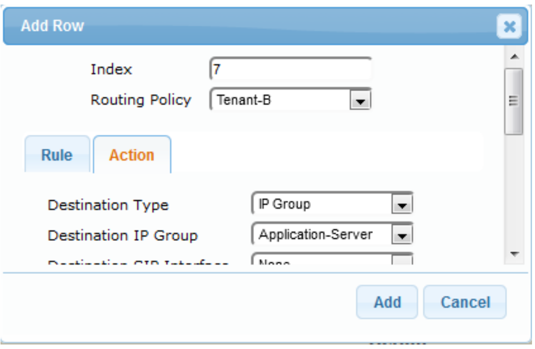
Index	6
Routing Policy	Tenant-B
Destination Type	IP Group
Destination IP Group	Tenant-B Users
Destination SIP Interface	None

   c. Add a rule for routing calls from HQ IP-PBX to Application server, if unable to route to WAN nomadic users (alternative route for previous rule):

Figure 7-40: Alternative Routing Rule - HQ IP PBX to Application Server for Tenant B



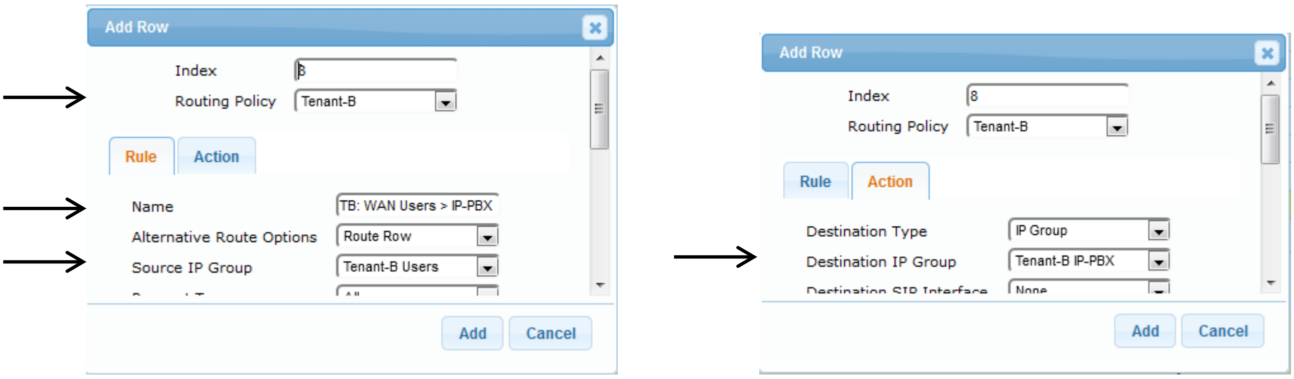
Index	7
Routing Policy	Tenant-B
Name	TB: IP-PBX > App Server
Alternative Route Options	Alternative Route Ignd
Source IP Group	Tenant-B IP-PBX
Request Type	All



Index	7
Routing Policy	Tenant-B
Destination Type	IP Group
Destination IP Group	Application-Server
Destination SIP Interface	None

d. Add a rule for routing calls from WAN nomadic users to HQ IP-PBX:

Figure 7-41: Routing Rule - WAN Nomadic Users to HQ IP-PBX for Tenant B



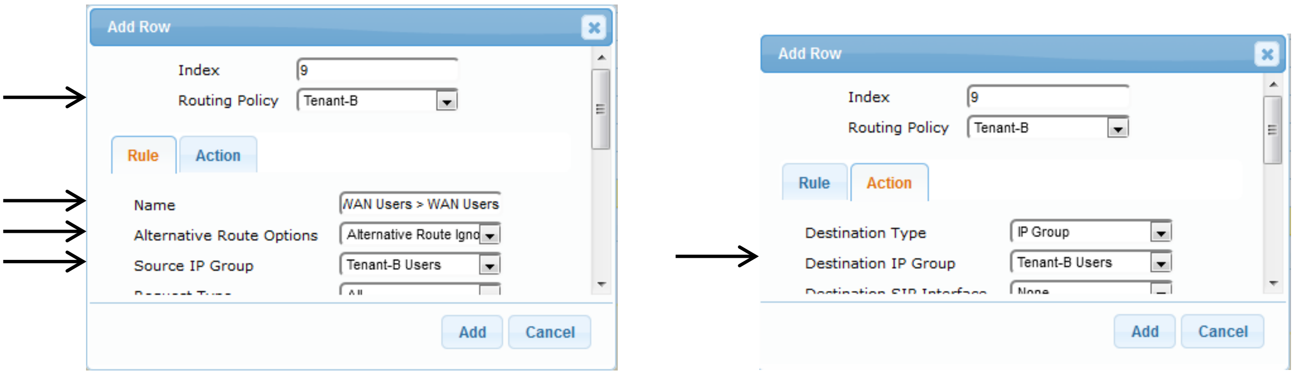
Index: 8
Routing Policy: Tenant-B

Rule tab:
Name: TB: WAN Users > IP-PBX
Alternative Route Options: Route Row
Source IP Group: Tenant-B Users
Request Type: All

Action tab:
Destination Type: IP Group
Destination IP Group: Tenant-B IP-PBX
Destination SIP Interface: None

e. Add a rule for routing calls between WAN nomadic users, if unable to route to HQ IP-PBX (alternative route for previous rule – call survivability):

Figure 7-42: Alternative Routing Rule – Call Survivability of WAN Nomadic Users for Tenant B



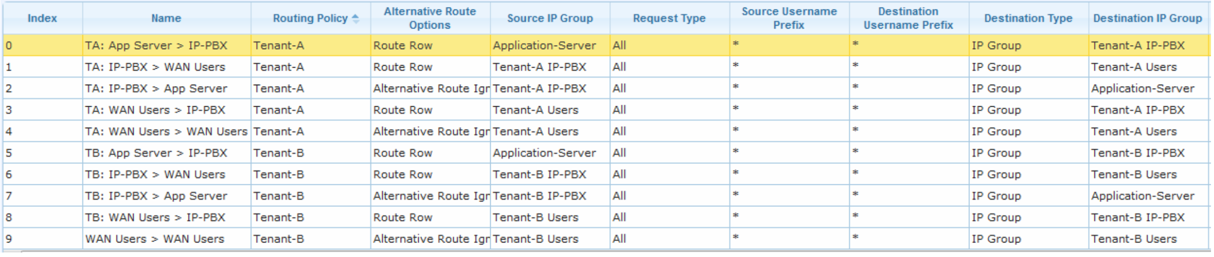
Index: 9
Routing Policy: Tenant-B

Rule tab:
Name: WAN Users > WAN Users
Alternative Route Options: Alternative Route Igno
Source IP Group: Tenant-B Users
Request Type: All

Action tab:
Destination Type: IP Group
Destination IP Group: Tenant-B Users
Destination SIP Interface: None

Once you have configured the IP-to-IP routing rules, the IP-to-IP Routing table should appear populated as shown below:

Figure 7-43: Configured IP-to-IP Routing Rules in the IP-to-IP Routing Table



Index	Name	Routing Policy	Alternative Route Options	Source IP Group	Request Type	Source Username Prefix	Destination Username Prefix	Destination Type	Destination IP Group
0	TA: App Server > IP-PBX	Tenant-A	Route Row	Application-Server	All	*	*	IP Group	Tenant-A IP-PBX
1	TA: IP-PBX > WAN Users	Tenant-A	Route Row	Tenant-A IP-PBX	All	*	*	IP Group	Tenant-A Users
2	TA: IP-PBX > App Server	Tenant-A	Alternative Route Igr	Tenant-A IP-PBX	All	*	*	IP Group	Application-Server
3	TA: WAN Users > IP-PBX	Tenant-A	Route Row	Tenant-A Users	All	*	*	IP Group	Tenant-A IP-PBX
4	TA: WAN Users > WAN Users	Tenant-A	Alternative Route Igr	Tenant-A Users	All	*	*	IP Group	Tenant-A Users
5	TB: App Server > IP-PBX	Tenant-B	Route Row	Application-Server	All	*	*	IP Group	Tenant-B IP-PBX
6	TB: IP-PBX > WAN Users	Tenant-B	Route Row	Tenant-B IP-PBX	All	*	*	IP Group	Tenant-B Users
7	TB: IP-PBX > App Server	Tenant-B	Alternative Route Igr	Tenant-B IP-PBX	All	*	*	IP Group	Application-Server
8	TB: WAN Users > IP-PBX	Tenant-B	Route Row	Tenant-B Users	All	*	*	IP Group	Tenant-B IP-PBX
9	WAN Users > WAN Users	Tenant-B	Alternative Route Igr	Tenant-B Users	All	*	*	IP Group	Tenant-B Users

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-31625