Configuration Note

Stand-Alone Survivability (SAS) Application

Version 7.0

SAS
Stand Alone Survivability
Continuous VoIP Service

HD VoIP
Sounds Better

AudioCodes

Table of Contents

List of Figures

Notice

This document describes AudioCodes Stand-Alone Survivability (SAS) application.

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 the accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Updates to this document and other documents as well as software files can be viewed by registered customers at http://www.audiocodes.com/downloads.

This document is subject to change without notice.

Date Published: June-09-2015

Trademarks

AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, OSN, SmartTAP, VMAS, VocaNOM, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX and One Box 365 are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

WEEE EU Directive

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

Customer Support

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

Abbreviations and Terminology

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

Document Revision Record

LTRT	Description
29808	Initial document release for Version 7.0.
29809	Maximum SAS users per product added.
29810	SAS License Key not required for MP-1xx (provided by default).

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

The device's Stand-Alone Survivability (SAS) feature ensures telephony communication continuity (survivability) for enterprises using hosted IP services (such as IP Centrex) or IP-PBX in cases of failure of these entities. In case of failure of the IP Centrex, IP-PBX servers (or even WAN connection and access Internet modem), the enterprise typically loses its internal telephony service at any branch, between its offices, and with the external environment. Typically, these failures also lead to the inability to make emergency calls (e.g., 911 in North America). Despite these possible points of failure, the device's SAS feature ensures that the enterprise's telephony services (e.g., SIP IP phones or soft phones) are maintained, by routing calls to the PSTN (i.e., providing PSTN fallback).

Notes:

- Except for MP-1xx, the SAS application is available only if the device is installed with the SAS Software License Key.
- The maximum number of users supported by the SAS application depends on the AudioCodes product:
  - √ Mediant 3000: 3,000 (5000 Depopulated)
  - √ Mediant 2000: 250
  - √ Mediant 1000B: 600
  - √ Mediant 8xx Series: 200
  - √ Mediant 5xx Series: 200
  - √ MP-1xx Series: 25

  Some of the products listed above may not have been released in Version 7.0. For a list of products released in Version 7.0, refer to the *Release Notes Version 7.0*.
- Throughput this document, the term *user agent* (UA) refers to the Enterprise's LAN phone user (i.e., SIP telephony entities such as IP phones).
- Throughout this document, the term *proxy* or *proxy server* refers to the Enterprise's centralized IP Centrex or IP-PBX.
- Throughout this document, the term *SAS* refers to the SAS application running on the device.
- For a description of the SAS parameters, you can also refer to the *User's Manual*.

This page is intentionally left blank.

2 SAS Overview

2.1 SAS Operating Modes

The device's SAS application can be implemented in one of the following main modes:

- **Outbound Proxy:** In this mode, SAS receives SIP REGISTER requests from the enterprise's UAs and forwards these requests to the external proxy (i.e., outbound proxy). When a connection with the external proxy fails, SAS enters SAS emergency state and serves as a proxy, by handling internal call routing for the enterprise's UAs - routing calls between UAs and if setup, routing calls between UAs and the PSTN. For more information, see 'SAS Outbound Mode' on page 9.
- **Redundant Proxy:** In this mode, the enterprise's UAs register with the external proxy and establish calls directly through the external proxy, without traversing SAS (or the device per se'). Only when connection with the proxy fails, do the UAs register with SAS, serving now as the UAs redundant proxy. SAS then handles the calls between UAs, and between the UAs and the PSTN (if setup). This mode is operational only during SAS in emergency state. This mode can be implemented, for example, for proxies that accept only SIP messages that are sent directly from the UAs. For more information, see 'SAS Redundant Mode' on page 12.

Note: It is recommended to implement the SAS outbound mode.

2.1.1 SAS Outbound Mode

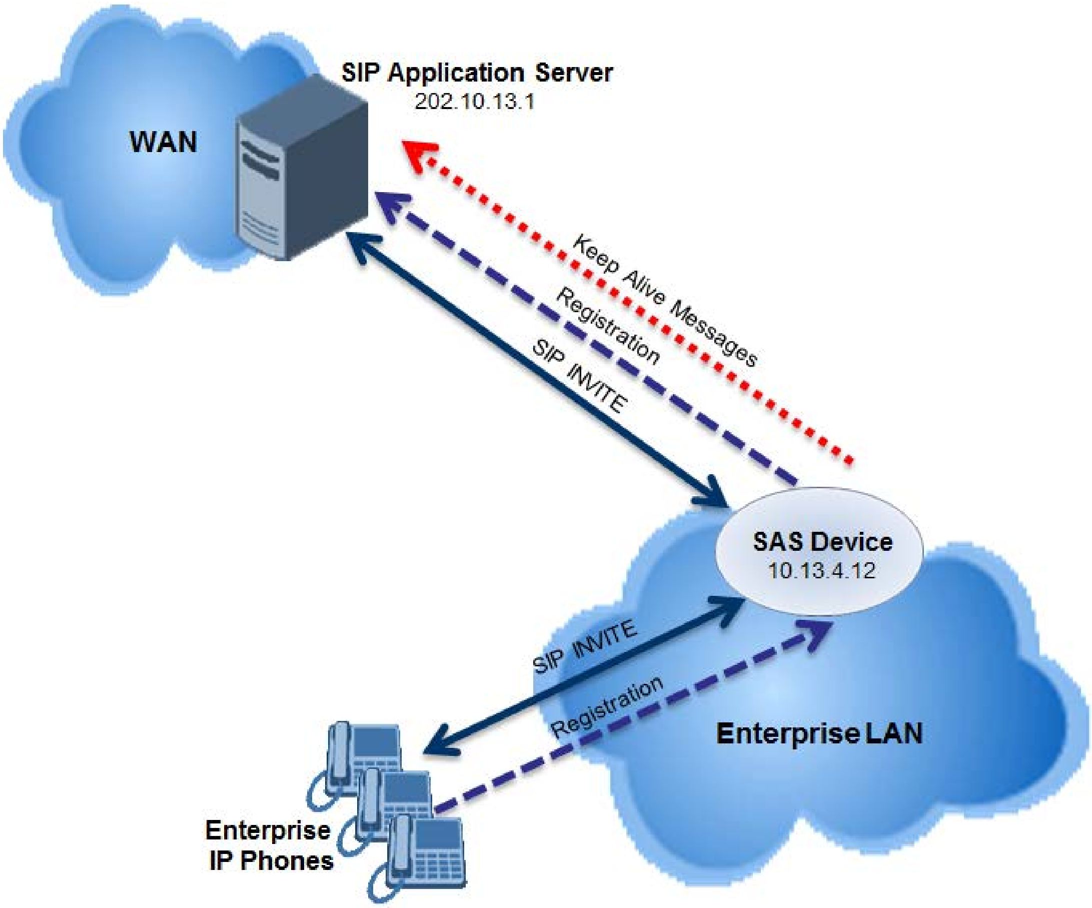
This section describes the SAS outbound mode, which includes the following states:

- Normal state (see 'Normal State' on page 10)
- Emergency state (see 'Emergency State' on page 11)

2.1.1.1 Normal State

In normal state, SAS receives REGISTER requests from the enterprise's UAs and forwards them to the external proxy (i.e., outbound proxy). Once the proxy replies with a SIP 200 OK, the device records the Contact and address of record (AOR) of the UAs in its internal SAS registration database. Therefore, in this mode, SAS maintains a database of all the registered UAs in the network. SAS also continuously maintains a keep-alive mechanism toward the external proxy, using SIP OPTIONS messages. The figure below illustrates the operation of SAS outbound mode in normal state:

Figure 2-1: SAS Outbound Mode in Normal State (Example)



2.1.1.2 Emergency State

When a connection with the external proxy fails (detected by the device's keep-alive messages), the device enters SAS emergency state. The device serves as a proxy for the UAs, by handling internal call routing of the UAs (within the LAN enterprise).

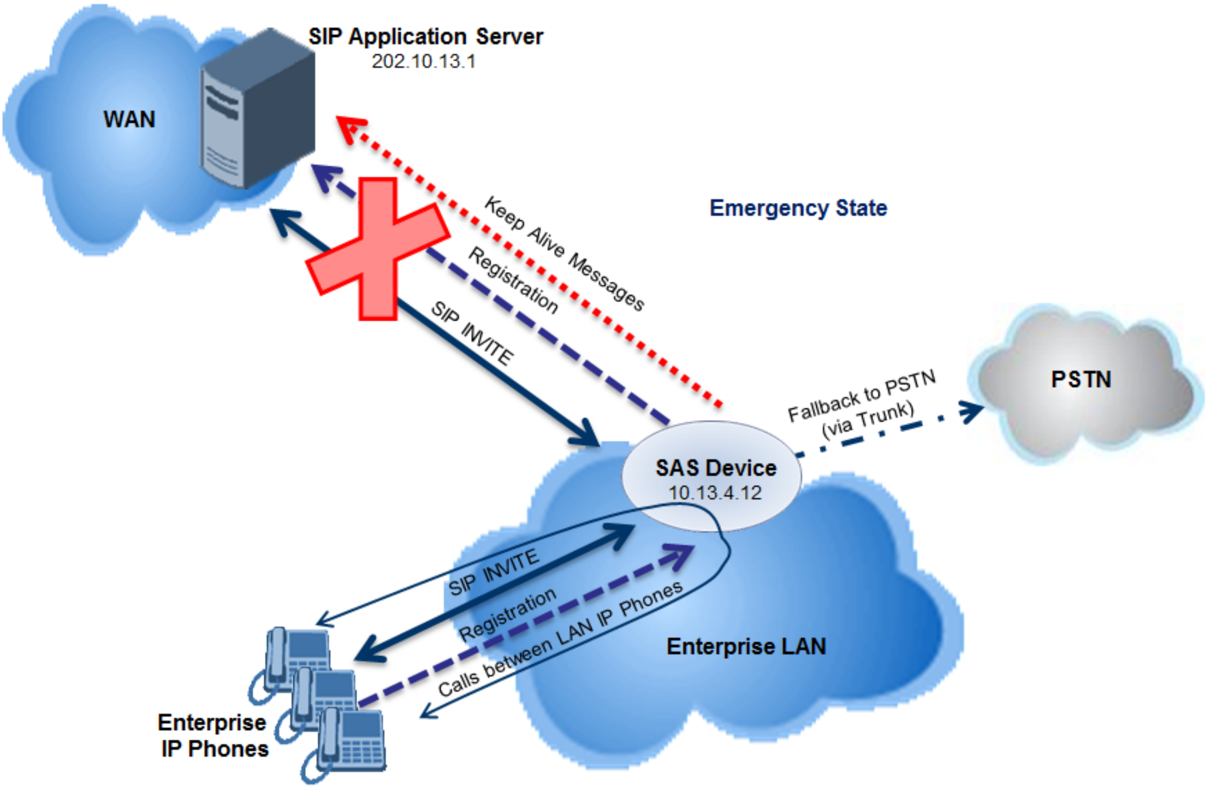
> **Note:** SAS can also enter Emergency state if no response is received from the proxy for sent OPTIONS, INVITE, or REGISTER messages. To configure this, set the SASEnteringEmergencyMode parameter to 1.

When the device receives calls, it searches its SAS registration database to locate the destination address (according to AOR or Contact). If the destination address is not found, SAS forwards the call to the default gateway. Typically, the default gateway is defined as the device itself (on which SAS is running), and if the device has PSTN interfaces, the enterprise preserves its capability for outgoing calls (from UAs to the PSTN network).

The routing logic of SAS in emergency state is described in detail in 'SAS Routing in Emergency State' on page 16.

The figure below illustrates the operation of SAS outbound mode in emergency state:

Figure 2-2: SAS Outbound Mode in Emergency State (Example)



When emergency state is active, SAS continuously attempts to communicate with the external proxy, using keep-alive SIP OPTIONS. Once connection to the proxy returns, the device exits SAS emergency state and returns to SAS normal state, as explained in 'Exiting Emergency and Returning to Normal State' on page 13.

2.1.2 SAS Redundant Mode

In SAS redundant mode, the enterprise's UAs register with the external proxy and establish calls directly through it, without traversing SAS (or the device per se'). Only when connection with the proxy fails, do the UAs register with SAS, serving now as the UAs redundant proxy. SAS then handles the calls between UAs, and between the UAs and the PSTN (if setup).

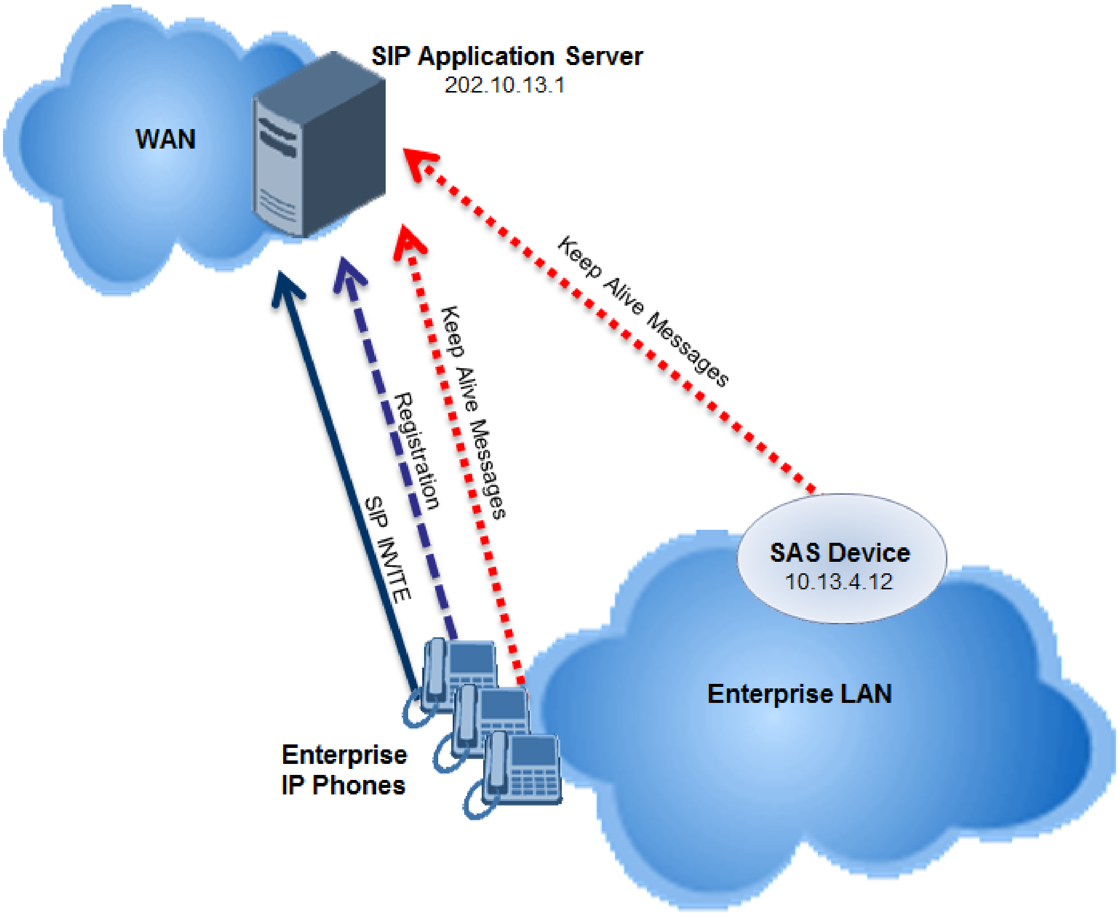
This mode is operational only during SAS in emergency state.

> **Note:** In this SAS deployment, the UAs (e.g., IP phones) must support configuration for primary and secondary proxy servers (i.e., proxy redundancy), as well as homing. Homing allows the UAs to switch back to the primary server from the secondary proxy once the connection to the primary server returns (UAs check this using keep-alive messages to the primary server). If homing is not supported by the UAs, you can configure SAS to ignore messages received from UAs in normal state (the 'SAS Survivability Mode' parameter must be set to 'Always Emergency' / 2) and thereby, “force” the UAs to switch back to their primary proxy.

2.1.2.1 Normal State

In normal state, the UAs register and operate directly with the external proxy.

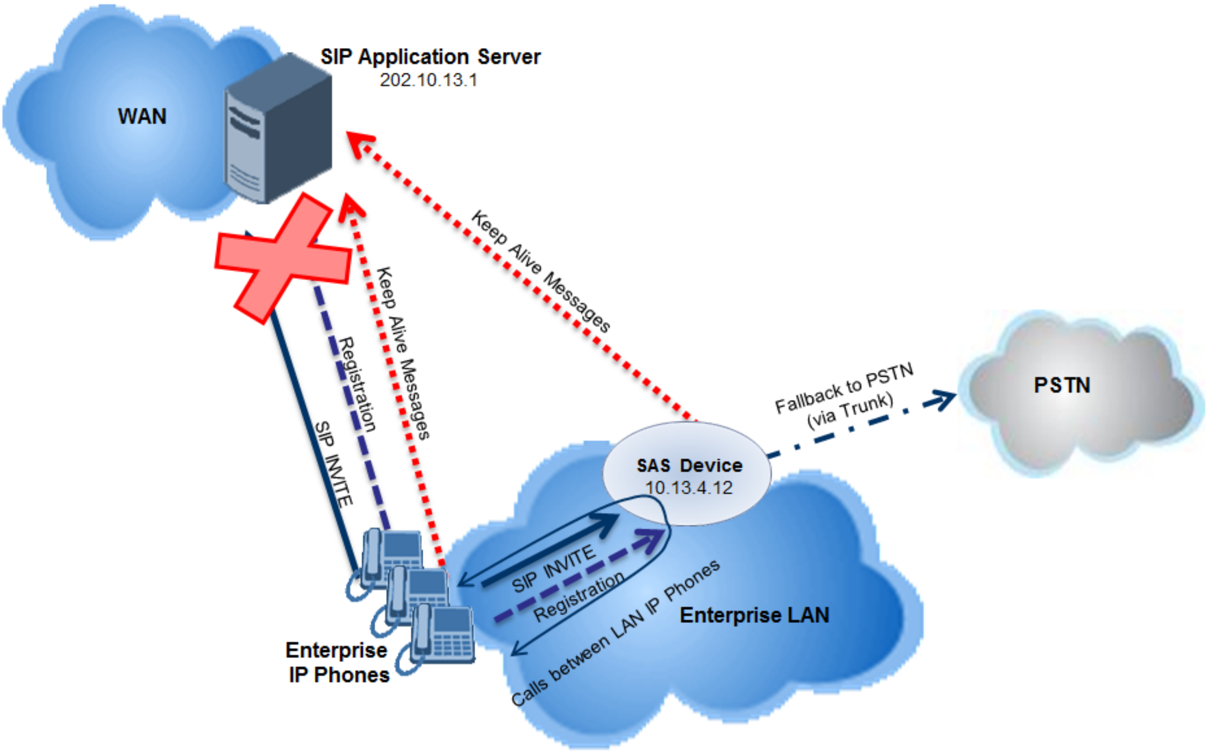
Figure 2-3: SAS Redundant Mode in Normal State (Example)



2.1.2.2 Emergency State

If the UAs detect that their primary (external) proxy does not respond, they immediately register to SAS and start routing calls to it.

Figure 2-4: SAS Redundant Mode in Emergency State (Example)



2.1.2.3 Exiting Emergency and Returning to Normal State

Once the connection with the primary proxy is re-established, the following occurs:

- **UAs:** Switch back to operate with the primary proxy.
- **SAS:** Ignores REGISTER requests from the UAs, forcing the UAs to switch back to the primary proxy.

  Note: This is applicable only if the 'SAS Survivability Mode' parameter is set to 'Always Emergency' (2).

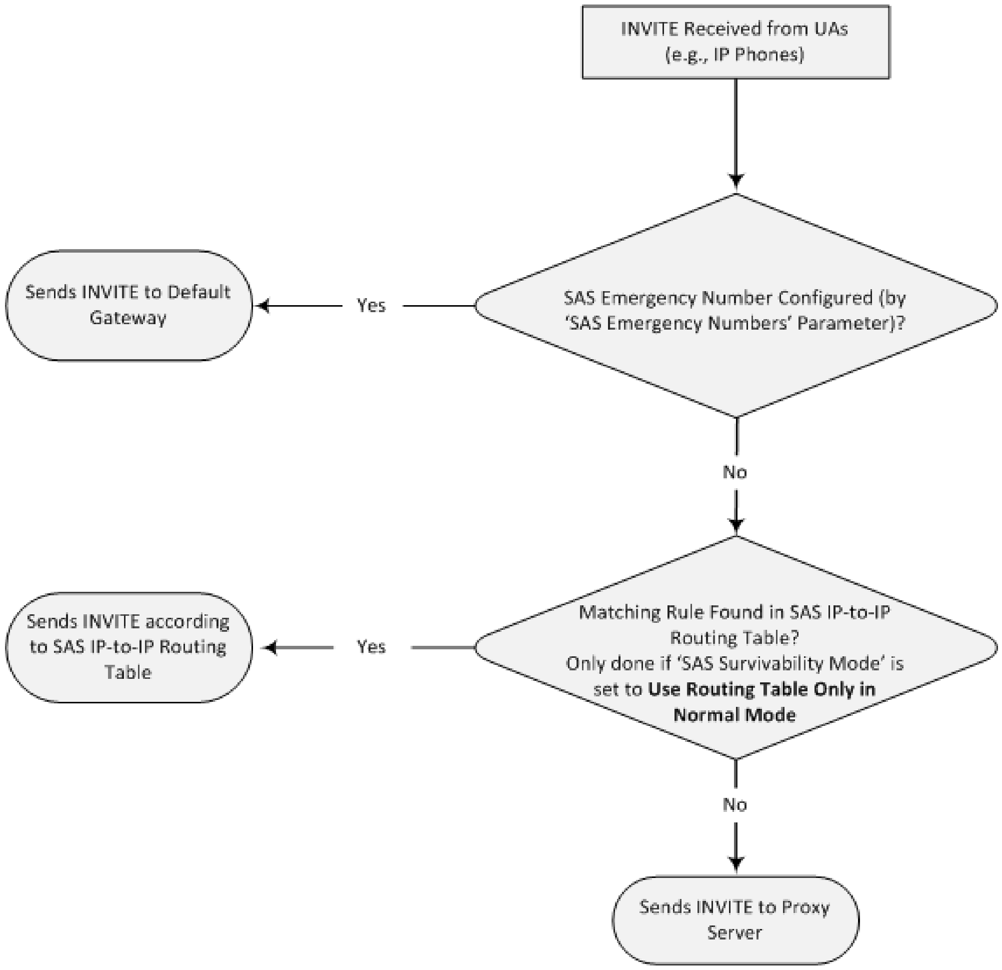
2.2 SAS Routing

This section provides flowcharts describing the routing logic for SAS in normal and emergency states.

2.2.1 SAS Routing in Normal State

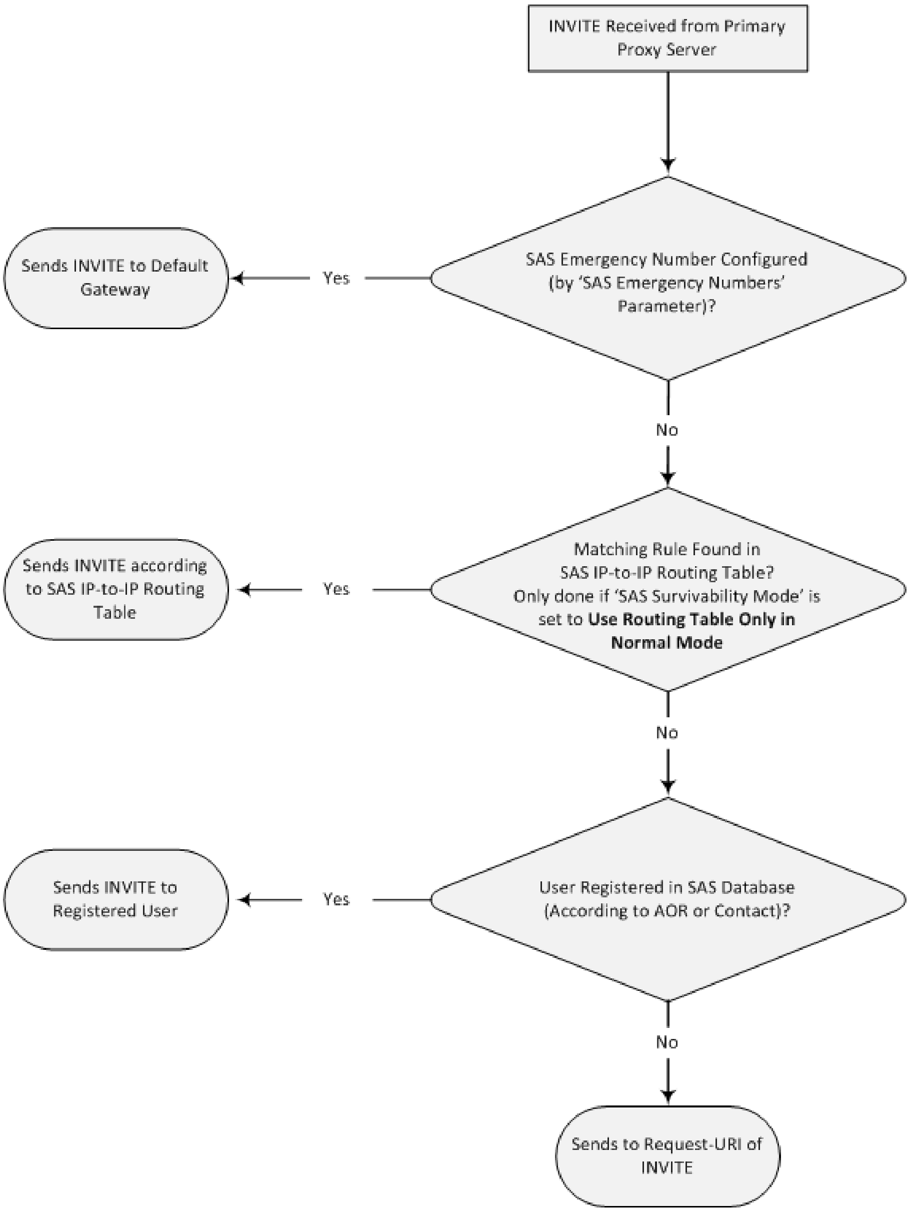
The flowchart below displays the routing logic for SAS in normal state for INVITE messages received from UAs:

Figure 2-5: Flowchart of INVITE from UA's in SAS Normal State


INVITE Received from UAs (e.g., IP Phones)
SAS Emergency Number Configured (by 'SAS Emergency Numbers' Parameter)?
Yes
Sends INVITE to Default Gateway
No
Matching Rule Found in SAS IP-to-IP Routing Table?
Only done if 'SAS Survivability Mode' is set to **Use Routing Table Only in Normal Mode**
Yes
Sends INVITE according to SAS IP-to-IP Routing Table
No
Sends INVITE to Proxy Server

The flowchart below displays the routing logic for SAS in normal state for INVITE messages received from the external proxy:

Figure 2-6: Flowchart of INVITE from Primary Proxy in SAS Normal State


INVITE Received from Primary Proxy Server
SAS Emergency Number Configured (by 'SAS Emergency Numbers' Parameter)?
Yes
Sends INVITE to Default Gateway
No
Matching Rule Found in SAS IP-to-IP Routing Table? Only done if 'SAS Survivability Mode' is set to **Use Routing Table Only in Normal Mode**
Yes
Sends INVITE according to SAS IP-to-IP Routing Table
No
User Registered in SAS Database (According to AOR or Contact)?
Yes
Sends INVITE to Registered User
No
Sends to Request-URI of INVITE

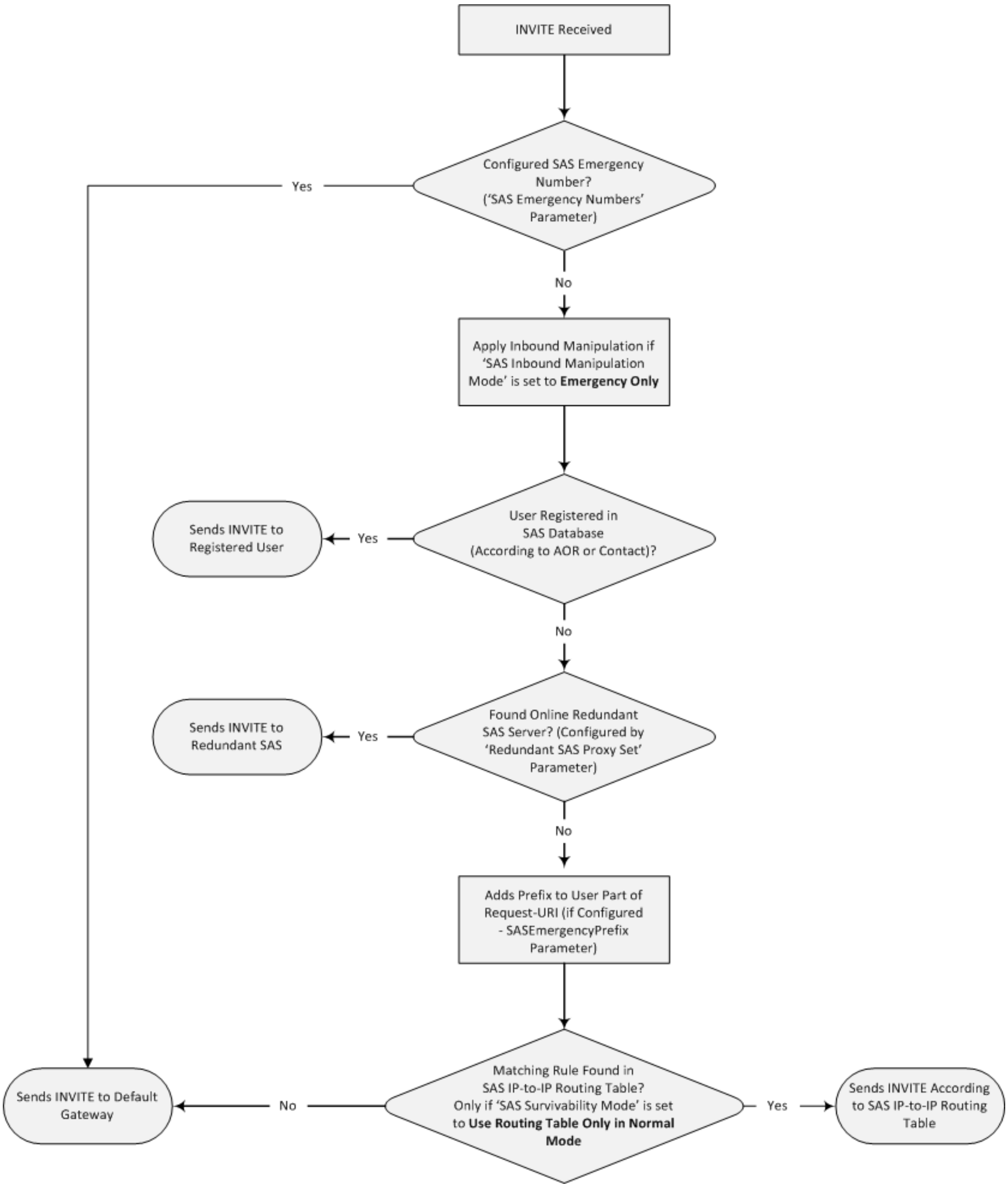
Note: When SAS receives a SIP request within a SIP dialog (i.e., To tag present in the To header), it routes the request as follows, depending on type of request:

- REGISTER requests: Request is always handled out-of-dialog, regardless of To-tag presence.
- Non-REGISTER requests:
  - √ If the request is from an active proxy or SAS is in Emergency mode, the routing is done according to the SAS database. If routing based on database is unsuccessful, SAS routes the request according to the Request-URI.
  - √ Otherwise, the request is routed according to the SASInDialogRequestMode parameter.
    [0] = (Standard) Request is sent according to the Request-URI.
    [1] = Request is sent to the Proxy (normal mode).

2.2.2 SAS Routing in Emergency State

The flowchart below shows the routing logic for SAS in emergency state:

Figure 2-7: Flowchart for SAS Emergency State


INVITE Received
Configured SAS Emergency Number? ('SAS Emergency Numbers' Parameter)
Yes
No
Apply Inbound Manipulation if 'SAS Inbound Manipulation Mode' is set to **Emergency Only**
User Registered in SAS Database (According to AOR or Contact)?
Yes
Sends INVITE to Registered User
No
Found Online Redundant SAS Server? (Configured by 'Redundant SAS Proxy Set' Parameter)
Yes
Sends INVITE to Redundant SAS
No
Adds Prefix to User Part of Request-URI (if Configured - SASEmergencyPrefix Parameter)
Matching Rule Found in SAS IP-to-IP Routing Table? Only if 'SAS Survivability Mode' is set to **Use Routing Table Only in Normal Mode**
No
Sends INVITE to Default Gateway
Yes
Sends INVITE According to SAS IP-to-IP Routing Table

3 SAS Configuration

SAS supports various configuration possibilities, depending on how the device is deployed in the network and the network architecture requirements. This section provides step-by-step procedures on configuring the SAS application, using the device's Web interface.

The SAS configuration includes the following:

- General SAS configuration that is common to all SAS deployment types (see 'General SAS Configuration' on page 17)
- SAS outbound mode (see 'Configuring SAS Outbound Mode' on page 22)
- SAS redundant mode (see 'Configuring SAS Redundant Mode' on page 22)
- Optional, advanced SAS features (see 'Advanced SAS Configuration' on page 24)

3.1 General SAS Configuration

This section describes the general configuration required for the SAS application. This configuration is applicable to all SAS modes.

3.1.1 Enabling the SAS Application

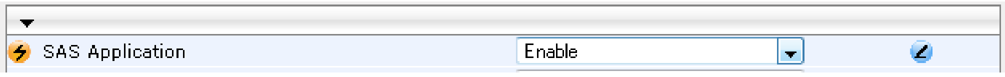
Before you can configure SAS, you need to enable the SAS application on the device. Once enabled, the **SAS** menu and related pages appear in the device's Web interface.

Note: The SAS application is available only if the device is installed with the SAS Software License Key. If your device is not installed with the SAS feature, contact your AudioCodes representative.

➢ **To enable the SAS application:**

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

Figure 3-1: Enabling SAS



SAS Application: Enable

3. Click **Submit**, and then reset the device with a burn-to-flash for your settings to take effect

3.1.2 Configuring a SIP Interface for SAS

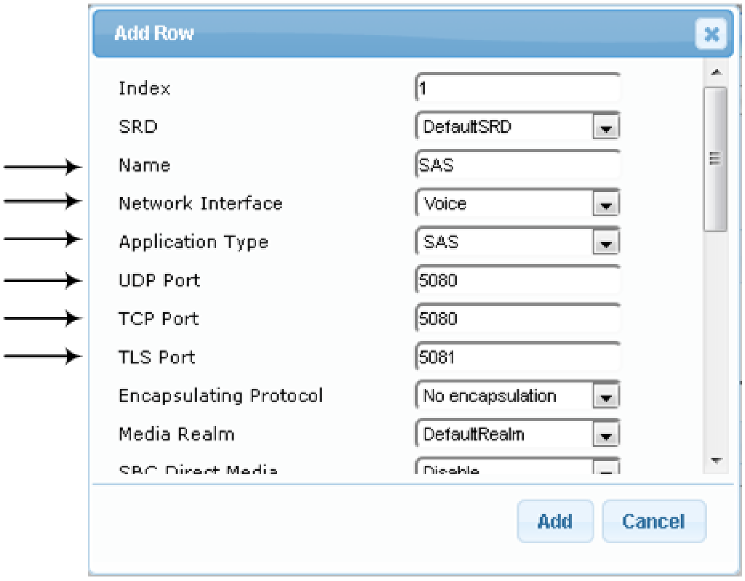
The SIP Interface defines the local port used for SIP signaling related to the SAS application.

Note: Make sure that you use a different port for the SAS application and for the Gateway application. The default SIP Interface (at Index 0) defines the SIP interface used for the Gateway application.

➢ **To configure a SAS SIP Interface:**

1. Open the SIP Interface table (**Configuration** tab > **VoIP** menu > **VoIP Network** > **SIP Interface Table**).
2. Click **Add**, and then configure the following parameters for Index 1:

Figure 3-2: Configuring a SIP Interface for SAS



Index	1
SRD	DefaultSRD
Name	SAS
Network Interface	Voice
Application Type	SAS
UDP Port	5080
TCP Port	5080
TLS Port	5081
Encapsulating Protocol	No encapsulation
Media Realm	DefaultRealm
SBC Direct Media	Disable

- 'Network Interface': Assign an IP network interface (configured in the Interface table) for SAS traffic.
- 'Application Type': Select **SAS**.
- 'UDP/TCP/TLS Port': Configure the local ports used for SAS.

3. Click **Add** to apply your settings.

3.1.3 Configuring a Proxy Set for SAS

A Proxy Set must be configured only for the following SAS modes:

- **Outbound mode:** In SAS normal state, SAS forwards SIP REGISTER and INVITE messages, received from the UAs, to the proxy server as defined by the Proxy Set.
- **Redundant mode and only if UAs don't support homing:** SAS sends keep-alive messages to the proxy and if it detects that the proxy connection has resumed, it ignores the REGISTER messages received from the UAs, forcing them to send their messages directly to the proxy.

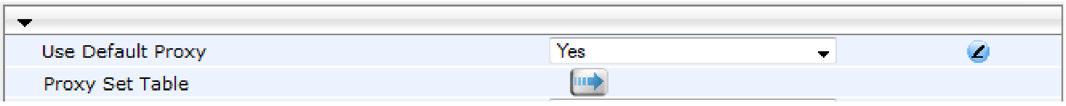
Once you have configured the Proxy Set, you must assign it to the SAS application using the 'SAS Proxy Set' parameter, as described in Configuring Common SAS Parameters on page 21.

Note: The device provides a default Proxy Set at Index 0 for the Gateway application. This can also be used for the SAS application, as described in the procedure below.

➢ **To configure a SAS Proxy Set:**

1. Open the Proxy & Registration page (**Configuration** tab > **VoIP** > **SIP Definitions** > **Proxy & Registration**).
2. From the 'Use Default Proxy' drop-down list, select **Yes**, and then click the **Proxy Set Table** arrow button to open the Proxy Sets table (**Configuration** tab > **VoIP** menu > **VoIP Network** > **Proxy Sets Table**):

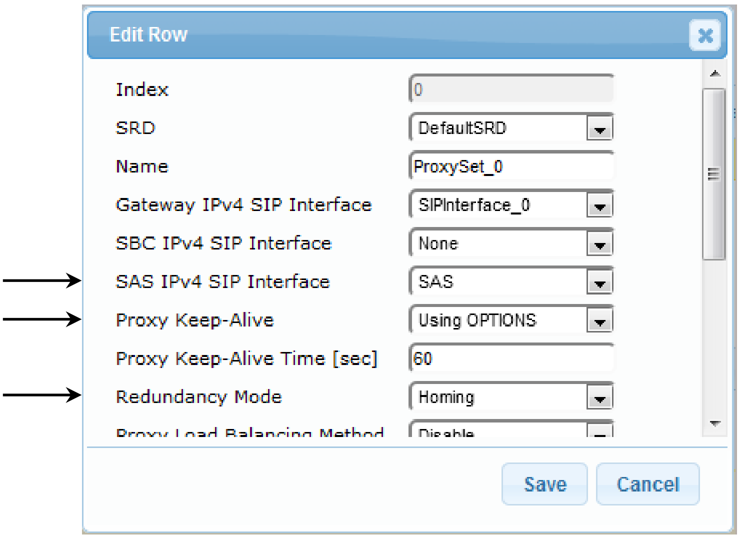
Figure 3-3: Enabling use of Default Proxy Set



Use Default Proxy	Yes
Proxy Set Table	

3. In the Proxy Sets table, select the default Proxy Set (Index 0), click **Edit**, and then modify the Proxy Set as shown below:

Figure 3-4: Configuring Default Proxy Set for SAS



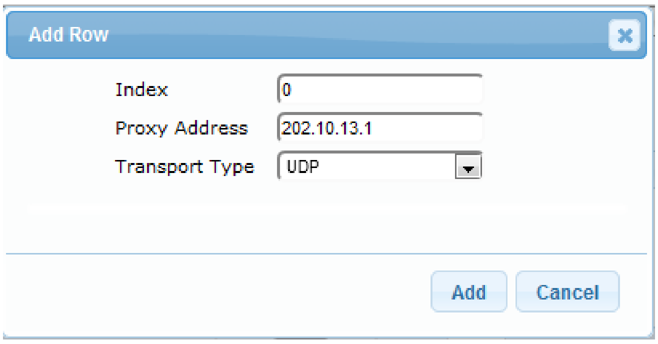
Index	0
SRD	DefaultSRD
Name	ProxySet_0
Gateway IPv4 SIP Interface	SIPInterface_0
SBC IPv4 SIP Interface	None
SAS IPv4 SIP Interface	SAS
Proxy Keep-Alive	Using OPTIONS
Proxy Keep-Alive Time [sec]	60
Redundancy Mode	Homing
Proxy Load Balancing Method	Disable

- 'SAS IPv4 SIP Interface': Assign the SIP Interface that you configured for SAS in Configuring a SIP Interface for SAS on page 18.

- 'Proxy Keep-Alive': Select **Using OPTIONS**, which enables the <device> to send SIP OPTIONS messages to the proxy for the keep-alive mechanism.
- For SAS Redundant Mode: From the 'Redundancy Mode' drop-down list, select **Homing** to enable the SAS device to re-connect to the SAS proxy server once connectivity is restored.

4. Click **Save**.
5. Select the table row of the Proxy Set that you edited above, and then click the **Proxy Address Table** link located below the table; the Proxy Address table opens.
6. Click **Add**, and then configure the IP address of the external SIP proxy server used for SAS:

Figure 3-5: Configuring IP Address for SAS Proxy Server



Index 0
Proxy Address 202.10.13.1
Transport Type UDP

7. Click **Add**.

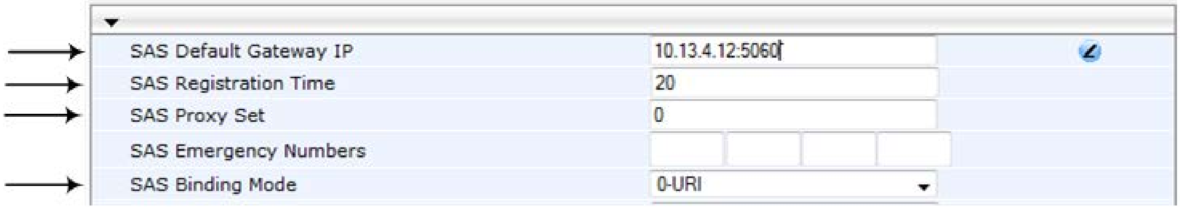
3.1.4 Configuring Common SAS Parameters

The following procedure describes how to configure SAS settings that are common to all SAS modes. The procedure also includes configuration for running both the Gateway and SAS applications on the device.

➢ **To configure common SAS settings:**

1. Open the SAS Configuration page (**Configuration** tab > **VoIP** menu > **SAS** > **Stand Alone Survivability**):

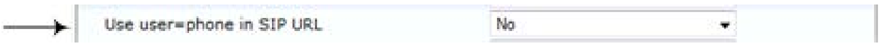
Figure 3-6: Configuring Common SAS Settings



SAS Default Gateway IP	10.13.4.12:5060
SAS Registration Time	20
SAS Proxy Set	0
SAS Emergency Numbers	
SAS Binding Mode	0-URI

2. For the Gateway application:
   a. In the 'SAS Default Gateway IP' field, enter the IP address and port (in the format x.x.x.x:port) of the device (i.e., Gateway application).
   b. Disable the use of the 'user=phone' parameter in the SIP URL for the Gateway application. This ensures that REGISTER and INVITE messages use SIP URI. By default, REGISTER messages are sent with the 'sip:' URI and INVITE messages with the 'tel:' URI.
      a. Open the SIP General Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** submenu > **General Parameters**).
      b. From the 'Use user=phone in SIP URL' drop-down list, select **No**.

Figure 3-7: Disabling user=phone in SIP URL



Use user=phone in SIP URL: No

3. In the 'SAS Registration Time' field, enter the value for the SIP Expires header, which is sent in the SIP 200 OK in response to an incoming REGISTER message when SAS is in Emergency state.

4. From the 'SAS Binding Mode' drop-down list, select the database binding mode:
   - **0-URI:** If the incoming AOR in the REGISTER request uses a 'tel:' URI or 'user=phone', the binding is done according to the Request-URI user part only; otherwise, the binding is done according to the entire Request-URI (i.e., user and host parts - user@host).
   - **1-User Part Only:** Binding is done according to the user part only.

   You must select **1-User Part Only** in cases where the UA sends REGISTER messages as SIP URI, but the INVITE messages sent to this UA include a Tel URI. For example, when the AOR of an incoming REGISTER is sip:3200@domain.com, SAS adds the entire SIP URI (e.g., sip:3200@domain.com) to its database (when the parameter is set to '0-URI'). However, if a subsequent Request-URI of an INVITE message for this UA arrives with sip:3200@10.1.2.3 user=phone, SAS searches its database for "3200", which it does not find. Alternatively, when the parameter is set to **1-User Part Only**, upon the receipt of a REGISTER message with sip:3200@domain.com, SAS adds only the user part (i.e., "3200") to its database. Therefore, if a Request-URI of an INVITE message for this UA arrives with sip:3200@10.1.2.3 user=phone, SAS can successfully locate the UA in its database.

5. In the 'SAS Proxy Set' field, assign the Proxy Set that you configured in Configuring a SAS Proxy Set on page 19. By default, Proxy Set at Index 0 is selected, which is the Proxy Set that is used for SAS. Thus, you can leave the parameter at its default value. Proxy Set defines the address of the UAs' external proxy and is applicable only to the

following SAS modes:

- **Outbound mode:** In SAS normal state, SAS forwards REGISTER and INVITE messages received from the UAs to the proxy servers defined in this Proxy Set.
- Redundant mode and only if UAs don't support homing: **SAS sends keep-alive messages** to this proxy and if it detects that the proxy connection has resumed, it ignores the REGISTER messages received from the UAs, forcing them to send their messages directly to the proxy.

6. Click **Submit** to apply your settings.

3.2 Configuring SAS Outbound Mode

This section describes how to configure the SAS outbound mode. These settings are in addition to the ones described in 'Configuring Common SAS Parameters' on page 18.

> **Note:** The VoIP CPEs (such as IP phones or residential gateways) need to be defined so that their proxy and registrar destination addresses and ports are the same as that configured for the device's SAS IP address and SAS local SIP port. In some cases, on the UAs, it is also required to define SAS as their outbound proxy, meaning that messages sent by the UAs include the host part of the external proxy, but are sent (on Layer 3/4) to the IP address / UDP port of SAS.

➢ **To configure SAS outbound mode:**

1. Open the SAS Configuration page (**Configuration** tab > **VoIP** menu > **SAS** > **Stand Alone Survivability**).
2. From the 'SAS Survivability Mode' drop-down list, select **Standard**.
3. Click **Submit**.

3.3 Configuring SAS Redundant Mode

This section describes how to configure the SAS redundant mode. These settings are in addition to the ones described in 'Configuring Common SAS Parameters' on page 18.

> **Note:** The VoIP CPEs (such as IP phones or residential gateways) need to be defined so that their primary proxy is the external proxy, and their redundant proxy destination addresses and port is the same as that configured for the device's SAS IP address and SAS SIP port.

➢ **To configure SAS redundant mode:**

1. Open the SAS Configuration page (**Configuration** tab > **VoIP** menu > **SAS** > **Stand Alone Survivability**).
2. From the 'SAS Survivability Mode' drop-down list, select one of the following, depending on whether the UAs support homing (i.e., they always attempt to operate with the primary proxy, and if using the redundant proxy, they switch back to the primary proxy whenever it's available):

   - **UAs support homing:** Select **Always Emergency**. This is because SAS does not need to communicate with the primary proxy of the UAs; SAS serves only as the redundant proxy of the UAs. When the UAs detect that their primary proxy is available, they automatically resume communication with it instead of with SAS.

- **UAs do not support homing:** Select **Ignore REGISTER**. SAS uses the keep-alive mechanism to detect availability of the primary proxy (defined by the SAS Proxy Set). If the connection with the primary proxy resumes, SAS ignores the messages received from the UAs, forcing them to send their messages directly to the primary proxy.

3. Click **Submit**.

3.4 Advanced SAS Configuration

This section describes the configuration of advanced SAS features that can optionally be implemented in your SAS deployment.

3.4.1 Manipulating URI user part of Incoming REGISTER

There are scenarios in which the UAs register to the proxy server with their full phone number (for example, "976653434"), but can receive two types of INVITE messages (calls):

- INVITEs whose destination is the UAs' full number (when the call arrives from outside the enterprise)
- INVITES whose destination is the last four digits of the UAs' phone number ("3434" in our example) when it is an internal call within the enterprise

Therefore, it is important that the device registers the UAs in the SAS registered database with their extension numbers (for example, "3434") in addition to their full numbers. To do this, you can define a manipulation rule to manipulate the SIP Request-URI user part of the AOR (in the To header) in incoming REGISTER requests. Once manipulated, it is saved in this manipulated format in the SAS registered users database in addition to the original (un-manipulated) AOR.

For example: Assume the following incoming REGISTER message is received and that you want to register in the SAS database the UA's full number as well as the last four digits from the right of the SIP URI user part:

```
REGISTER sip:10.33.38.2 SIP/2.0
Via: SIP/2.0/UDP 10.33.4.226:5050;branch=z9hG4bKac10827
Max-Forwards: 70
From: <sip: 976653434@10.33.4.226>;tag=1c30219
To: <sip: 976653434@10.33.4.226>
Call-ID: 16844@10.33.4.226
CSeq: 1 REGISTER
Contact: <sip: 976653434@10.10.10.10:5050>;expires=180
Allow:
REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUB
SCRIBE,UPDATE
Expires: 180
User-Agent: Audiocodes-Sip-Gateway-/v.
Content-Length: 0
```

After manipulation, SAS registers the user in its database as follows:

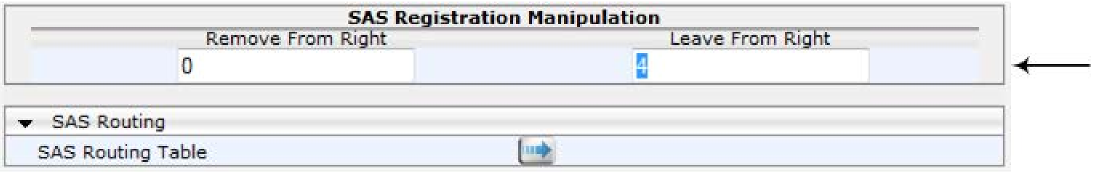
- **AOR:** 976653434@10.33.4.226
- **Associated AOR:** 3434@10.33.4.226 (after manipulation, in which only the four digits from the right of the URI user part are retained)
- **Contact:** 976653434@10.10.10.10

The procedure below describes how to configure the above manipulation example.

➢ **To manipulate incoming Request-URI user part of REGISTER message:**

1. Open the SAS Configuration page (**Configuration** tab > **VoIP** menu > **SAS** > **Stand Alone Survivability**).
2. Under the **SAS Registration Manipulation** group, in the 'Leave From Right' field, enter the number of digits (e.g., "4") to leave from the right side of the user part. This field defines the number of digits to retain from the right side of the user part; all other digits in the user part are removed.

Figure 3-8: Manipulating User Part in Incoming REGISTER



SAS Registration Manipulation

Remove From Right	Leave From Right
0	4

3. Click **Submit**.

Note:

- The device first does manipulation according to the Remove From Right parameter and only then according to the Leave From Right parameter.
- Only one manipulation rule can be configured.
- You can also configure SAS registration manipulation using the ini file parameter, SASRegistrationManipulation or the CLI command, configure voip > sas sasregistrationmanipulation.

3.4.2 Manipulating Destination Number of Incoming INVITE

You can define a manipulation rule to manipulate the destination number in the Request-URI of incoming INVITE messages when SAS is in emergency state. This is required, for example, if the call is destined to a registered user but the destination number in the received INVITE is not the number assigned to the registered user in the SAS registration database. To overcome this and successfully route the call, you can define manipulation rules to change the INVITE's destination number so that it matches that of the registered user in the database. This is done using the IP to IP Inbound Manipulation table.

For example, in SAS emergency state, assume an incoming INVITE has a destination number "7001234" which is destined to a user registered in the SAS database as "552155551234". In this scenario, the received destination number needs to be manipulated to the number "552155551234". The outgoing INVITE sent by the device then also contains this number in the Request-URI user part.

In normal state, the numbers are not manipulated. In this state, SAS searches the number 552155551234 in its database and if found, it sends the INVITE containing this number to the UA.

➢ **To manipulate the destination number in SAS emergency state:**

1. Open the SAS Configuration page (**Configuration** tab > **VoIP** menu > **SAS** > **Stand Alone Survivability**).
2. From the 'SAS Inbound Manipulation Mode' (*SASInboundManipulationMode*) drop-down list, select **Emergency Only**.
3. Click **Submit**; the **SAS Inbound Manipulation Mode Table** ➡ button appears on the page.
4. Click this button to open the IP to IP Inbound Manipulation page.

5. Add your SAS manipulation rule as required. See the table below for descriptions of the parameters.
6. Click **Submit** to save your changes.

Notes:

- The following fields in the IP-to-IP Inbound Manipulation table are not applicable to SAS and must be left at their default values:
  - √ 'Additional Manipulation' - default is **0**
  - √ 'Manipulation Purpose' - default is **Normal**
  - √ 'Source IP Group' - default is **-1**
- The IP to IP Inbound Manipulation table can also be configured using the table ini file parameter, IPInboundManipulation or CLI command, **configure voip** > **sbc manipulations ip-inbound-manipulation**.

SAS IP to IP Inbound Manipulation Parameters

Parameter	Description
Matching Characteristics (Rule)	
Additional Manipulation CLI: is-additional-manipulation **[IPInboundManipulation_IsAdditionalManipulation]**	Determines whether additional SIP URI user part manipulation is done for the table entry rule listed directly above it. ▪ **[0]** No = (Default) Regular manipulation rule (not done in addition to the rule above it). ▪ **[1]** Yes = If the above row entry rule matched the call, consider this row entry as a match as well and perform the manipulation specified by this rule. **Note:** Additional manipulation can only be done on a different SIP URI, source or destination, to the rule configured in the row above as configured by the 'Manipulated URI' parameter (see below).
Manipulation Purpose CLI: purpose **[IPInboundManipulation_ManipulationPurpose]**	Defines the purpose of the manipulation: ▪ **[0]** Normal = (Default) Inbound manipulations affect the routing input and source and/or destination number. ▪ **[1]** Routing input only = Inbound manipulations affect the routing input only, retaining the original source and destination number. ▪ **[2]** Shared Line = Used for BroadSoft's Shared-Line Appearance feature. This manipulation is for registration requests to change the destination number of the secondary extension numbers to the primary extension. For more information, refer to the *User's Manual*.
Source IP Group ID CLI: src-ip-group-id **[IPInboundManipulation_SrcIpGroup]**	Defines the IP Group from where the incoming INVITE is received. For any IP Group, enter the value "-1".
Source Username Prefix CLI: src-user-name-prefix **[IPInboundManipulation_SrcUsernamePrefix]**	Defines the prefix of the source SIP URI user name (usually in the From header). For any prefix, enter the asterisk "*" symbol (default). **Note:** The prefix can be a single digit or a range of digits. For available notations, refer to the *User's Manual*.
Source Host CLI: src-host **[IPInboundManipulation_SrcHost]**	Defines the source SIP URI host name - full name (usually in the From header). For any host name, enter the asterisk "*" symbol (default).

Parameter	Description
Destination Username Prefix CLI: dst-user-name-prefix **[IPInboundManipulation_DestUsernamePrefix]**	Defines the prefix of the destination SIP URI user name (usually in the Request-URI). For any prefix, enter the asterisk "*" symbol (default). **Note:** The prefix can be a single digit or a range of digits. For available notations, refer to the *User's Manual*.
Destination Host CLI: dst-host **[IPInboundManipulation_DestHost]**	Defines the destination SIP URI host name - full name (usually in the Request URI). For any host name, enter the asterisk "*" symbol (default).
Request Type CLI: request-type **[IPInboundManipulation_RequestType]**	Defines the SIP request type to which the manipulation rule is applied. ▪ **[0]** All = (Default) All SIP messages. ▪ **[1]** INVITE = All SIP messages except REGISTER and SUBSCRIBE. ▪ **[2]** REGISTER = Only REGISTER messages. ▪ **[3]** SUBSCRIBE = Only SUBSCRIBE messages. ▪ **[4]** INVITE and REGISTER = All SIP messages except SUBSCRIBE. ▪ **[5]** INVITE and SUBSCRIBE = All SIP messages except REGISTER.
Manipulated URI CLI: manipulated-uri **[IPInboundManipulation_ManipulatedURI]**	Determines whether the source or destination SIP URI user part is manipulated. ▪ **[0]** Source = (Default) Manipulation is done on the source SIP URI user part. ▪ **[1]** Destination = Manipulation is done on the destination SIP URI user part.
Operation Rule (Action)	
Remove From Left CLI: remove-from-left **[IPInboundManipulation_RemoveFromLeft]**	Defines the number of digits to remove from the left of the user name prefix. For example, if you enter 3 and the user name is "john", the new user name is "n".
Remove From Right CLI: remove-from-right **[IPInboundManipulation_RemoveFromRight]**	Defines the number of digits to remove from the right of the user name prefix. For example, if you enter 3 and the user name is "john", the new user name is "j". **Note:** If both 'Remove From Right' and 'Leave From Right' parameters are configured, the 'Remove From Right' setting is applied first.
Leave From Right CLI: leave-from-right **[IPInboundManipulation_LeaveFromRight]**	Defines the number of characters that you want retained from the right of the user name. **Note:** If both 'Remove From Right' and 'Leave From Right' parameters are configured, the 'Remove From Right' setting is applied first.
Prefix to Add CLI: prefix-to-add **[IPInboundManipulation_Prefix2Add]**	Defines the number or string that you want added to the front of the user name. For example, if you enter 'user' and the user name is "john", the new user name is "userjohn".
Suffix to Add CLI: suffix-to-add **[IPInboundManipulation_Suffix2Add]**	Defines the number or string that you want added to the end of the user name. For example, if you enter '01' and the user name is "john", the new user name is "john01".

3.4.3 SAS Routing Based on IP-to-IP Routing Table

SAS routing that is based on SAS Routing table rules is applicable for the following SAS states:

- Normal, if the 'SAS Survivability Mode' parameter is set to **Use Routing Table only in Normal mode**.
- Emergency, if the 'SAS Survivability Mode' parameter is **not** set to **Use Routing Table only in Normal mode**.

The SAS routing rule destination can be an IP Group, IP address, Request-URI, or ENUM query.

The IP-to-IP Routing table allows you to configure up to 120 SAS routing rules (for Normal and Emergency modes). The device routes the SAS call (received SIP INVITE message) once a rule in this table is matched. If the characteristics of an incoming call do not match the first rule, the call characteristics is then compared to the settings of the second rule, and so on until a matching rule is located. If no rule is matched, the call is rejected.

When SAS receives a SIP INVITE request from a proxy server, the following routing logic is performed:

a. Sends the request according to rules configured in the IP-to-IP Routing table.

b. If no matching routing rule exists, the device sends the request according to its SAS registration database.

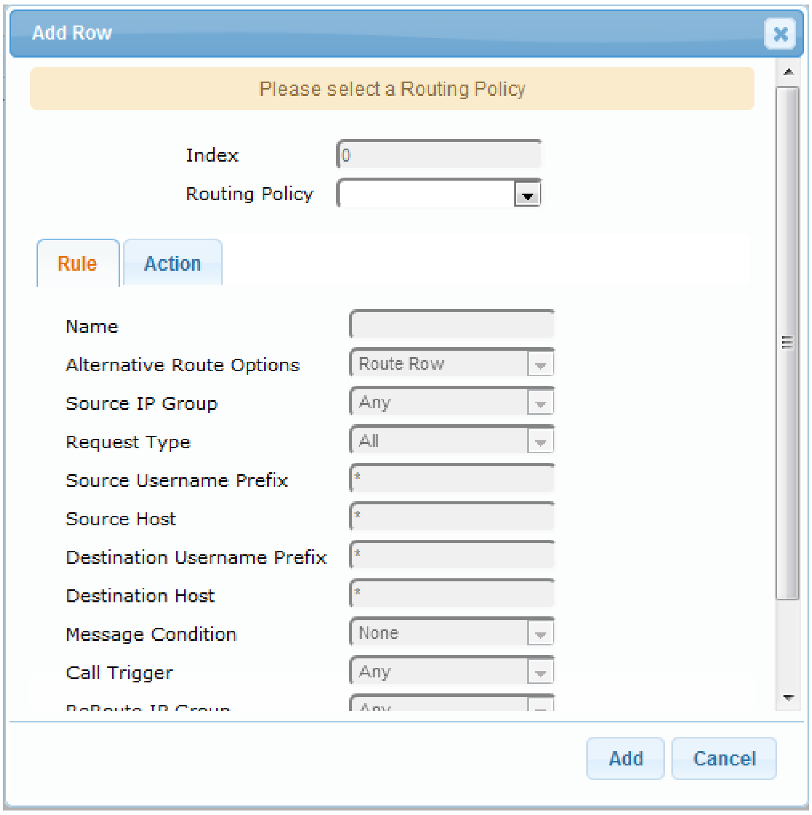
c. If no routing rule is located in the database, the device sends the request according to the Request-URI header.

Note: The IP-to-IP Routing table can also be configured using the table *ini* file parameter, IP2IPRouting or CLI command, configure voip/sbc routing ip2ip-routing.

➢ To configure the IP-to-IP Routing table for SAS:

1. In the SAS Configuration page, click the **SAS Routing Table** button; the IP-to-IP Routing Table page appears.
2. Click **Add**; the Add Record dialog box appears:

Figure 3-9: Configuring SAS Routing in IP-to-IP Routing Table



Add Row

Please select a Routing Policy

Index	0
Routing Policy	

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

3. Configure a routing rule according to the parameters described in the table below.
4. Click **Ad** to apply your changes.

Note: The following parameters are not applicable to SAS and must be ignored:

- 'Routing Policy'
- 'Source IP Group'
- 'Destination IP Group'
- 'Alternative Route Options'

SAS IP-to-IP Routing Table Parameters

Parameter	Description
Index [IP2IPRouting_Index]	Defines an index number for the new table row. **Note:** Each row must be configured with a unique index.
Name route-name [IP2IPRouting_RouteName]	Defines an arbitrary name to easily identify the row. The valid value is a string of up to 20 characters. By default, no value is defined.
Rule (Matching Characteristics)	
Request Type request-type [IP2IPRouting_RequestType]	Defines the SIP dialog request type (SIP Method) of the incoming SIP dialog. ▪ [0] All (default) ▪ [1] INVITE ▪ [2] REGISTER ▪ [3] SUBSCRIBE ▪ [4] INVITE and REGISTER ▪ [5] INVITE and SUBSCRIBE ▪ [6] OPTIONS
Source Username Prefix src-user-name-prefix [IP2IPRouting_SrcUsernamePrefix]	Defines the prefix of the user part of the incoming SIP dialog's source URI (usually the From URI). You can use special notations for denoting the prefix. To denote calls without a user part in the URI, use the $ sign. The default is the asterisk (*) symbol (i.e., any prefix). If this rule is not required, leave this field empty.
Source Host src-host [IP2IPRouting_SrcHost]	Defines the host part of the incoming SIP dialog's source URI (usually the From URI). The default is the asterisk (*) symbol (i.e., any host name). If this rule is not required, leave this field empty.
Destination Username Prefix dst-user-name-prefix [IP2IPRouting_DestUsernamePrefix]	Defines the prefix of the incoming SIP dialog's destination URI (usually the Request URI) user part. You can use special notations for denoting the prefix. To denote calls without a user part in the URI, use the $ sign. The default is the asterisk (*) symbol (i.e., any prefix). If this rule is not required, leave this field empty.
Destination Host dst-host [IP2IPRouting_DestHost]	Defines the host part of the incoming SIP dialog’s destination URI (usually the Request-URI). The default is the asterisk (*) symbol (i.e., any destination host). If this rule is not required, leave this field empty.
Message Condition message-condition-name [IP2IPRouting_MessageConditionName]	Assigns a SIP Message Condition rule to the IP-to-IP Routing rule.
Call Trigger trigger [IP2IPRouting_Trigger]	Defines the reason (i.e., trigger) for re-routing the SIP request: ▪ **[0]** Any = (Default) This routing rule is used for all scenarios (re-routes and non-re-routes). ▪ **[1]** 3xx = Re-routes the request if it was triggered as a result of a SIP 3xx response. ▪ **[2]** REFER = Re-routes the INVITE if it was triggered as a result of a REFER request.

Parameter	Description
	▪ **[3]** 3xx or REFER = Applies to options [1] and [2]. ▪ **[4]** Initial only = This routing rule is used for regular requests that the device forwards to the destination. This rule is not used for re-routing of requests triggered by the receipt of REFER or 3xx.
ReRoute IP Group re-route-ip-group-id [IP2IPRouting_ReRouteIPGroupName]	Defines the IP Group that initiated (sent) the SIP redirect response (e.g., 3xx) or REFER message. This parameter is typically used for re-routing requests (e.g., INVITEs) when interworking is required for SIP 3xx redirect responses or REFER messages. The parameter functions together with the 'Call Trigger' parameter (in the table). The default is **Any** (i.e., any IP Group).
Action	

Destination Type
dst-type
[IP2IPRouting_DestType]
	Determines the destination type to which the outgoing SIP dialog is sent.
	▪ **[0]** IP Group = (Default) The SIP dialog is sent to the IP Group's Proxy Set (SERVER-type IP Group) or registered contact from the database (if USER-type IP Group).
	▪ **[1]** Dest Address = The SIP dialog is sent to the address configured in the following fields: 'Destination SRD ID', 'Destination Address', 'Destination Port', and 'Destination Transport Type'.
	▪ **[2]** Request URI = The SIP dialog is sent to the address indicated in the incoming Request-URI. If the fields 'Destination Port' and 'Destination Transport Type' are configured, the incoming Request-URI parameters are overridden and these fields take precedence.
	▪ **[3]** ENUM = An ENUM query is sent to include the destination address. If the fields 'Destination Port' and 'Destination Transport Type' are configured, the incoming Request-URI parameters are overridden and these fields take precedence.
	▪ **[4]** Hunt Group = Used for call center survivability.
	▪ **[5]** Dial Plan = The IP destination is determined by a Dial Plan index of the loaded Dial Plan file. The syntax of the Dial Plan index in the Dial Plan file is as follows: <destination / called prefix number>,0,<IP destination>
	Note that the second parameter "0" is ignored. An example of a configured Dial Plan (# 6) in the Dial Plan file is shown below:
	`[ PLAN6 ]`
	`200,0,10.33.8.52     ; called prefix 200 is routed to destination 10.33.8.52`
	`201,0,10.33.8.52`
	`300,0,itsp.com       ; called prefix 300 is routed to destination itsp.com`
	Once the Dial Plan is defined, you need to assign it (0 to 7) to the routing rule as the destination in the 'Destination Address' parameter, where "0" denotes [PLAN1], "1" denotes [PLAN2], and so on.
	▪ [7] LDAP = LDAP-based routing. Make sure that the Routing Policy assigned to the routing rule is configured with the LDAP Server Group for defining the LDAP server(s) to query.
	▪ [8] Gateway = The device routes the SBC call to the Tel side (Gateway call) using an IP-to-Tel routing rule in the Inbound IP Routing table. The IP-to-Tel routing rule must be configured with the same call matching characteristics as this SBC IP-to-IP routing rule. This option is also used for alternative routing of an IP-to-IP route to the PSTN. In such a case, the IP-to-Tel routing rule must also be

Parameter	Description
	configured with the same call matching characteristics as this SBC IP-to-IP routing rule. ▪ [9] Routing Server = Device sends a request to a third-party routing server for an appropriate destination (next hop) for the matching call. ▪ [10] All Users = Device checks whether the Request-URI (i.e., destination user) in the incoming INVITE is registered in its' users' database, and if yes, it sends the INVITE to the address of the corresponding contact specified in the database. If the Request-URI is not registered, the call is rejected.
Destination SIP Interface dst-srd-id [IP2IPRouting_DestSIPInterfaceName]	Defines the destination SIP Interface to where the call is sent. By default, no value is defined (**None**). **Notes:** ▪ The parameter is applicable only if the 'Destination Type' parameter is configured to any value other than **IP Group**. If the 'Destination Type' parameter is configured to **IP Group**, the following SIP Interface is used: ✓ 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. ▪ For multi-tenancy, if the assigned SBC Routing Policy is not shared (i.e., the Routing Policy is associated with an Isolated SRD), the SIP Interface must be one that is associated with the Routing Policy or with a shared Routing Policy (i.e., the Routing Policy is associated with one or more Shared SRDs). If the Routing Policy is shared, the SIP Interface can be one that is associated with any SRD or Routing Policy (but it's recommended that it belong to the same SRD/Routing Policy or to shared SRD/Routing Policy to avoid "bleeding").
Destination Address dst-address [IP2IPRouting_DestAddress]	Defines the destination address to where the call is sent. The address can be an IP address or a domain name (e.g., domain.com). If ENUM-based routing is used (i.e., the 'Destination Type' parameter is set to **ENUM**) the parameter defines the IP address or domain name (FQDN) of the ENUM service, for example, e164.arpa, e164.customer.net or NRENum.net. The device sends the ENUM query containing the destination phone number to an external DNS server, configured in the Interface table. The ENUM reply includes a SIP URI (user@host) which is used as the destination Request-URI in this routing table. The valid value is a string of up to 50 characters (IP address or FQDN). By default, no value is defined. **Notes:** ▪ The parameter is applicable only if the 'Destination Type' parameter is set to **Dest Address** [1] or **ENUM** [3]. ▪ When using domain names, enter a DNS server IP address or alternatively, define these names in the Internal DNS table. ▪ To terminate SIP OPTIONS messages at the device (i.e., to handle them locally), set the parameter to "internal".
Destination Port dst-port [IP2IPRouting_DestPort]	Defines the destination port to where the call is sent.
Destination Transport Type	Defines the transport layer type for sending the call: ▪ **[-1]** = (Default) Not configured - the transport type is determined by

Parameter	Description
dst-transport-type [IP2IPRouting_DestTransportType]	the SIPTransportType global parameter. - **[0]** UDP - **[1]** TCP - **[2]** TLS
Call Setup Rules Set ID call-setup-rules-set-id [IP2IPRouting_CallSetupRulesSetId]	Assigns a Call Setup Rule Set ID to the routing rule. The device performs the Call Setup rules of this Set ID if the incoming call matches the characteristics of this routing rule. The device routes the call to the destination according to the routing rule's configured action, only after it has performed the Call Setup rules.
Group Policy group-policy [IP2IPRouting_GroupPolicy]	Defines whether the routing rule includes call forking. - **[0]** None = (Default) Call uses only this route (even if Forking Group members are configured in the rows below it). - **[1]** Forking = Call uses this route and the routes of Forking Group members, if configured (in the rows below it).
Cost Group cost-group [IP2IPRouting_CostGroup]	Assigns a Cost Group to the routing rule for determining the cost of the call. By default, no value is defined (**None**). **Notes:** - To implement LCR and its Cost Groups, you must enable LCR for the Routing Policy assigned to the routing rule. If LCR is disabled, the device ignores the parameter. - The Routing Policy also determines whether matched routing rules that are **not** assigned Cost Groups are considered as a higher or lower cost route compared to matching routing rules that are assigned Cost Groups. For example, if the 'Default Call Cost' parameter in the Routing Policy is configured to **Lowest Cost**, even if the device locates matching routing rules that are assigned Cost Groups, the first-matched routing rule without an assigned Cost Group is considered as the lowest cost route and thus, chosen as the preferred route.

3.4.4 Blocking Calls from Unregistered SAS Users

To prevent malicious calls, for example, service theft, it is recommended to configure the feature for blocking SIP INVITE messages received from SAS users that are not registered in the SAS database. This applies to SAS in normal and emergency states.

➢ **To block calls from unregistered SAS users:**

1. Open the SAS Configuration page (**Configuration** tab > **VoIP** menu > **SAS** > **Stand Alone Survivability**).
2. From the 'SAS Block Unregistered Users' drop-down list, select **Block**.
3. Click **Submit** to apply your changes.

3.4.5 Configuring SAS Emergency Calls

You can configure SAS to route emergency calls (such as 911 in North America) directly to the PSTN through its FXO interface or E1/T1 trunk. Thus, even during a communication failure with the external proxy, enterprise UAs can still make emergency calls.

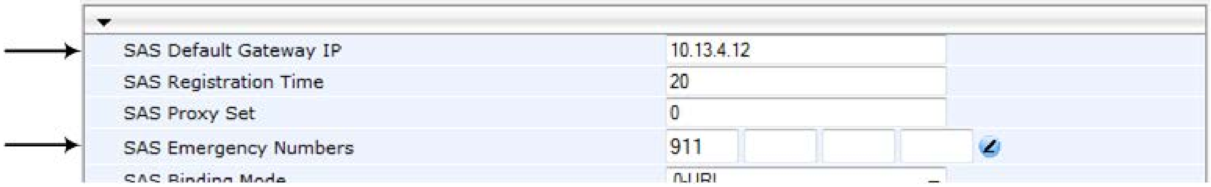
You can define up to four emergency numbers, where each number can include up to four digits. When SAS receives a SIP INVITE (from a UA) that includes one of the user-defined emergency numbers in the SIP user part, it forwards the INVITE directly to the default gateway (see 'SAS Routing in Emergency State' on page 16). The default gateway is defined in the 'SAS Default Gateway IP' field, and this is the device itself. The device then sends the call directly to the PSTN.

This feature is applicable to SAS in normal and emergency states.

➢ **To configure SAS emergency numbers:**

1. Open the SAS Configuration page (**Configuration** tab > **VoIP** menu > **SAS** > **Stand Alone Survivability**).
2. In the 'SAS Default Gateway IP' field, define the IP address and port (in the format *x.x.x.x:port*) of the device (Gateway application).
3. In the 'SAS Emergency Numbers' field, enter an emergency number in each field box.

Figure 3-10: Configuring SAS Emergency Numbers



SAS Default Gateway IP	10.13.4.12			
SAS Registration Time	20			
SAS Proxy Set	0			
SAS Emergency Numbers	911			
SAS Binding Mode	0-URI			

4. Click **Submit** to apply your changes.

3.4.6 Adding SIP Record-Route Header to SIP INVITE

You can configure SAS to add the SIP Record-Route header to SIP requests (e.g. INVITE) received from enterprise UAs. SAS then sends the request with this header to the proxy. The Record-Route header includes the IP address of the SAS application. This ensures that future requests in the SIP dialog session from the proxy to the UAs are routed through the SAS application. If not configured, future request within the dialog from the proxy are sent directly to the UAs (and do not traverse SAS). When this feature is enabled, the SIP Record-Route header includes the URI "lr" parameter, indicating loose routing, as shown in the following example:

```
Record-Route: <sip:server10.biloxi.com;lr>
```

Note: This feature is applicable only to the SAS Outbound mode.

➢ **To enable the Record-Route header:**

1. Open the SAS Configuration page (**Configuration** tab > **VoIP** menu > **SAS** > **Stand Alone Survivability**).
2. From the ‘Enable Record-Route' drop-down list, select **Enable**.
3. Click **Submit** to apply your changes.

3.4.7 Re-using TCP Connections

You can enable the SAS application to re-use the same TCP connection for sessions (multiple SIP requests / responses) with the same SIP UA. The benefits of this feature include less CPU and memory usage because fewer TCP connections are open and reduced network congestion. For example, assume User A sends a REGISTER message to SAS with transport=TCP, and User B sends an INVITE message to A using SAS. In this scenario, the SAS application forwards the INVITE request using the same TCP connection that User A initially opened with the REGISTER message.

➢ **To re-use TCP connection sessions in SAS**

1. Open the SAS Configuration page (**Configuration** tab > **VoIP** menu > **SAS** > **Stand Alone Survivability**).
2. From the ‘SAS Connection Reuse' drop-down list, select **Enable**.
3. Click **Submit** to apply your changes.

3.4.8 Replacing Contact Header for SIP Messages

You can configure SAS to change the SIP Contact header so that it points to the SAS host. This ensures that in the message, the top-most SIP Via header and the Contact header point to the same host.

Notes:

- This feature is applicable only to the SAS Outbound mode.
- The device may become overloaded if this feature is enabled, as all incoming SIP dialog requests traverse the SAS application.

Currently, this feature can be configured only by the *ini* file parameter, SASEnableContactReplace or the CLI command, configure voip > sas stand-alone-survivability > sas-contact-replace:

- **[0]** (Default): Disable - when relaying requests, SAS adds a new Via header (with the IP address of the SAS application) as the top-most Via header and retains the original Contact header. Thus, the top-most Via header and the Contact header point to different hosts.
- **[1]**: Enable - SAS changes the Contact header so that it points to the SAS host and therefore, the top-most Via header and the Contact header point to the same host.

3.4.9 Handling Incoming SIP Dialogs from SAS Users

You can configure how the device sends incoming SIP dialog requests received from users when not in SAS Emergency mode. This is done using the ini file parameter SASInDialogRequestMode:

- [0] = (Default) Send according to the SIP Request-URI.
- [1] = Send to Proxy server.

4 Viewing Registered SAS Users

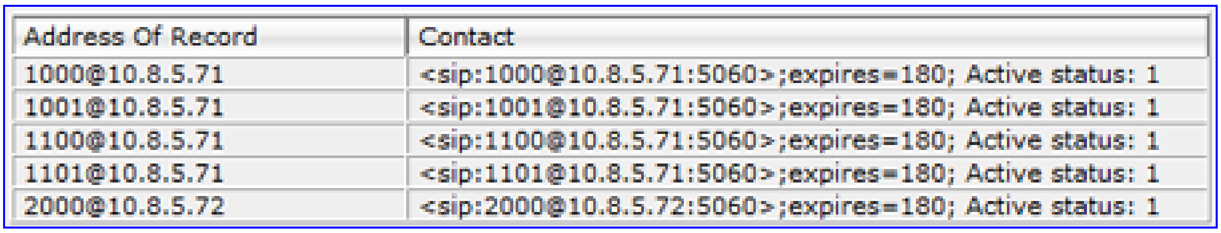
You can view all the users that are registered in the SAS registration database. This is displayed in the 'SAS/SBC Registered Users page..

> **Note:** You can increase the maximum number of registered SAS users, by implementing the SAS Cascading feature, as described in 'SAS Cascading' on page 39.

➢ **To view registered SAS/SBC users:**

- Open the Registration Status page (**Status & Diagnostics** tab > **VoIP Status** menu > **SAS/SBC Registered Users**).

Figure 4-1: Viewing Registered SAS Users



Address Of Record	Contact
1000@10.8.5.71	<sip:1000@10.8.5.71:5060>;expires=180; Active status: 1
1001@10.8.5.71	<sip:1001@10.8.5.71:5060>;expires=180; Active status: 1
1100@10.8.5.71	<sip:1100@10.8.5.71:5060>;expires=180; Active status: 1
1101@10.8.5.71	<sip:1101@10.8.5.71:5060>;expires=180; Active status: 1
2000@10.8.5.72	<sip:2000@10.8.5.72:5060>;expires=180; Active status: 1

SAS/SBC Registered Users Parameters

Column Name	Description
Address of Record	An address-of-record (AOR) is a SIP or SIPS URI that points to a domain with a location service that can map the URI to another URI (Contact) where the user might be available.
Contact	SIP URI that can be used to contact that specific instance of the User Agent for subsequent requests.

This page is intentionally left blank.

5 SAS Cascading

The SAS Cascading feature allows you to increase the number of SAS users above the maximum supported by the SAS gateway. This is achieved by deploying multiple SAS gateways in the network. For example, if the SAS gateway supports up to 600 users, but your enterprise has 1,500 users, you can deploy three SAS gateways to accommodate all users: the first SAS gateway can service 600 registered users, the second SAS gateway the next 600 registered users, and the third SAS gateway the rest (i.e., 300 registered users).

In SAS Cascading, the SAS gateway first attempts to locate the called user in its SAS registration database. Only if the user is not located, does the SAS gateway send it on to the next SAS gateway according to the SAS Cascading configuration.

There are two methods for configuring SAS Cascading. This depends on whether the users can be identified according to their phone extension numbers:

- **SAS Routing Table:** If users can be identified with unique phone extension numbers, then the SAS Routing table is used to configure SAS Cascading. This SAS Cascading method routes calls directly to the SAS Gateway (defined by IP address) to which the called SAS user is registered.

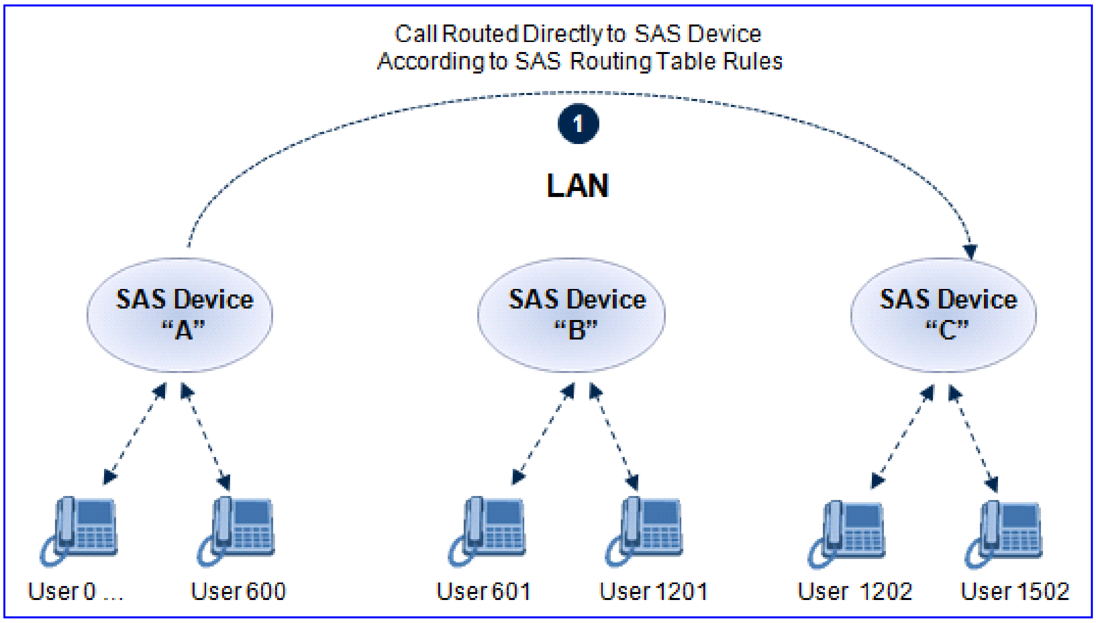
  The following is an example of a SAS Cascading deployment of users with unique phone extension numbers:

  - Users registered to the first SAS gateway start with extension number “40”
  - Users registered to the second SAS gateway start with extension number “20”
  - Users registered to the third SAS gateway start with extension number “30”

  The SAS Routing table rules for SAS Cascading are created using the destination (called) extension number prefix (e.g., “30”) and the destination IP address of the SAS gateway to which the called user is registered. Such SAS routing rules must be configured at each SAS gateway to allow routing between the SAS users. The routing logic for SAS Cascading is similar to SAS routing in Emergency state (see the flowchart in 'SAS Routing in Emergency State' on page 16). For a description on the SAS Routing table, see 'SAS Routing Based on IP-to-IP Routing Table' on page 28.

  The figure below illustrates an example of a SAS Cascading call flow configured using the SAS Routing table. In this example, a call is routed from SAS Gateway (A) user to a user on SAS Gateway (B).

Figure 5-1: SAS Cascading Using SAS Routing Table - Example

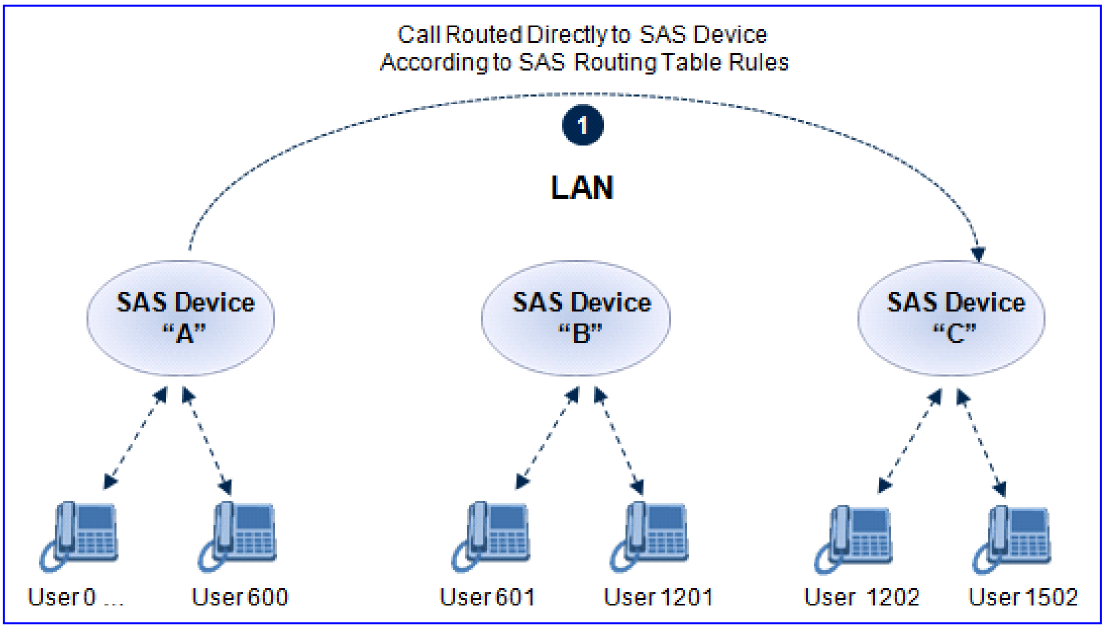


- **SAS Redundancy mode:** If users cannot be distinguished (i.e., associated to a specific SAS gateway), then the SAS Redundancy feature is used to configure SAS Cascading. This mode routes the call in a loop fashion, from one SAS gateway to the next, until the user is located. Each SAS gateway serves as the redundant SAS gateway ("redundant SAS proxy server") for the previous SAS gateway (in a one-way direction). For example, if a user calls a user that is not registered on the same SAS gateway, the call is routed to the second SAS gateway, and if not located, it is sent to the third SAS gateway. If the called user is not located on the third (or last) SAS gateway, it is then routed back to the initial SAS gateway, which then routes the call to the default gateway (i.e., to the PSTN).

Each SAS gateway adds its IP address to the SIP via header in the INVITE message before sending it to the next ("redundant") SAS gateway. If the SAS gateway receives an INVITE and its IP address appears in the SIP via header, it sends it to the default gateway (and not to the next SAS gateway), as defined by the SASDefaultGatewayIP parameter. Therefore, this mode of operation prevents looping between SAS gateways when a user is not located on any of the SAS gateways.

The figure below illustrates an example of a SAS Cascading call flow when configured using the SAS Redundancy feature. In this example, a call is initiated from a SAS Gateway (A) user to a user that is not located on any SAS gateway. The call is subsequently routed to the PSTN.

Figure 5-2: SAS Cascading Using SAS Redundancy Mode - Example



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

AudioCodes