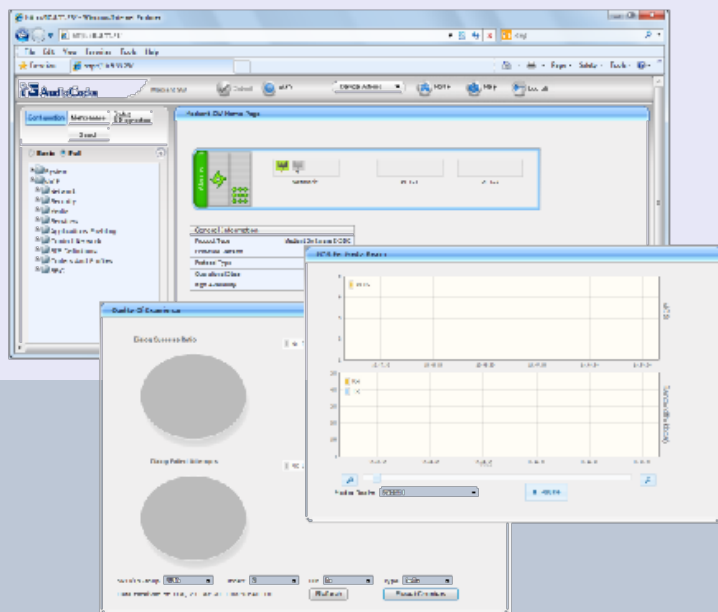


Mediant™ Software SBC

Session Border Controller

High-Availability System

User's Manual



Version 6.6

March 2014

Document # LTRT-41548



Table of Contents

1	Overview	15
<hr/>		
	Getting Started with Initial Connectivity.....	17
2	Installing the Software	19
3	Changing Default IP Address to Suit your Network Addressing Scheme....	21
4	Licensing the Device.....	23
<hr/>		
	Management Tools	25
5	Introduction	27
6	Web-Based Management.....	29
6.1	Getting Acquainted with the Web Interface.....	29
6.1.1	Computer Requirements.....	29
6.1.2	Accessing the Web Interface.....	30
6.1.3	Areas of the GUI	31
6.1.4	Toolbar Description.....	32
6.1.5	Navigation Tree	33
6.1.5.1	Displaying Navigation Tree in Basic and Full View	33
6.1.5.2	Showing / Hiding the Navigation Pane.....	34
6.1.6	Working with Configuration Pages	35
6.1.6.1	Accessing Pages.....	35
6.1.6.2	Viewing Parameters	36
6.1.6.3	Modifying and Saving Parameters	37
6.1.6.4	Working with Tables.....	38
6.1.7	Searching for Configuration Parameters	41
6.1.8	Creating a Login Welcome Message.....	42
6.1.9	Getting Help.....	43
6.1.10	Logging Off the Web Interface.....	44
6.2	Viewing the Home Page.....	44
6.3	Configuring Web User Accounts	46
6.3.1	Basic User Accounts Configuration	47
6.3.2	Advanced User Accounts Configuration.....	49
6.4	Displaying Login Information upon Login	52
6.5	Configuring Web Security Settings	53
6.6	Web Login Authentication using Smart Cards	53
6.7	Configuring Web and Telnet Access List	54
6.8	Configuring RADIUS Settings	55
7	CLI-Based Management.....	57
7.1	Enabling CLI using Telnet.....	57
7.2	Enabling CLI using SSH and RSA Public Key	57
7.3	Establishing a CLI Session	59
7.4	CLI Commands	60
7.4.1	Status Commands	60
7.4.2	Ping Command.....	62
7.4.3	Management Commands	63
7.4.4	Configuration Commands.....	63

7.4.5	LDAP Commands	64
8	SNMP-Based Management	65
8.1	Configuring SNMP Community Strings	65
8.2	Configuring SNMP Trap Destinations	66
8.3	Configuring SNMP Trusted Managers	67
8.4	Configuring SNMP V3 Users.....	68
9	INI File-Based Management.....	71
9.1	INI File Format	71
9.1.1	Configuring Individual ini File Parameters	71
9.1.2	Configuring Table ini File Parameters	71
9.1.3	General ini File Formatting Rules	73
9.2	Loading an ini File	73
9.3	Modifying an ini File	74
9.4	Secured Encoded ini File	74
General System Settings		75
10	Configuring Certificates	77
10.1	Replacing the Device's Certificate	77
10.2	Loading a Private Key	79
10.3	Mutual TLS Authentication	80
10.4	Configuring Certificate Revocation Checking (OCSP)	81
10.5	Self-Signed Certificates.....	81
10.6	Loading Certificate Chain for Trusted Root.....	82
11	Date and Time.....	83
11.1	Configuring Date and Time Manually.....	83
11.2	Automatic Date and Time through SNTP Server	83
General VoIP Configuration.....		85
12	Network.....	87
12.1	Configuring Physical Ethernet Ports	87
12.2	Configuring Tx/Rx for Ethernet Port-Pair Groups.....	88
12.3	Configuring IP Network Interfaces	90
12.3.1	Assigning NTP Services to Application Types	94
12.3.2	Multiple Interface Table Configuration Rules.....	94
12.3.3	Troubleshooting the Multiple Interface Table	95
12.3.4	Networking Configuration Examples	96
12.3.4.1	One VoIP Interface for All Applications	96
12.3.4.2	VoIP Interface per Application Type.....	96
12.3.4.3	VoIP Interfaces for Combined Application Types	97
12.3.4.4	VoIP Interfaces with Multiple Default Gateways	98
12.4	Configuring the IP Routing Table	99
12.4.1	Interface Column	101
12.4.2	Routing Table Configuration Summary and Guidelines	101
12.4.3	Troubleshooting the Routing Table	102
12.5	Configuring Quality of Service.....	102

12.6	Disabling ICMP Redirect Messages.....	104
12.7	DNS.....	104
12.7.1	Configuring the Internal DNS Table.....	104
12.7.2	Configuring the Internal SRV Table.....	106
12.8	Configuring NFS Settings.....	107
12.9	Network Address Translation Support	108
12.9.1	Device Located behind NAT	109
12.9.1.1	Configuring a Static NAT IP Address for All Interfaces.....	110
12.9.1.2	Configuring NAT Translation per IP Interface	110
12.9.2	Remote UA behind NAT	112
12.9.2.1	First Incoming Packet Mechanism	112
12.9.2.2	No-Op Packets	113
12.10	Robust Receipt of Media Streams	114
12.11	Multiple Routers Support.....	114
13	Security	115
13.1	Configuring Firewall Settings	115
13.2	Configuring General Security Settings	120
13.3	Intrusion Detection System	121
13.3.1	Enabling IDS.....	121
13.3.2	Configuring IDS Policies	122
13.3.3	Assigning IDS Policies.....	125
13.3.4	Viewing IDS Alarms	127
14	Media	129
14.1	Configuring RTP/RTCP Settings.....	129
14.1.1	Configuring RTP Base UDP Port.....	129
14.2	Configuring Media Realms.....	130
14.2.1	Configuring Quality of Experience per Media Realm	132
14.2.2	Configuring Bandwidth Management per Media Realm.....	135
14.3	Configuring Server for Media Quality of Experience	137
14.4	Configuring Media Security	138
15	Services	141
15.1	Routing Based on LDAP Active Directory Queries	141
15.1.1	Configuring the LDAP Server	141
15.1.2	Configuring the Device's LDAP Cache.....	142
15.1.3	Active Directory based Tel-to-IP Routing for Microsoft Lync.....	144
15.1.3.1	Querying the AD and Routing Priority	144
15.1.3.2	Configuring AD-Based Routing Rules.....	147
15.2	Least Cost Routing.....	149
15.2.1	Overview	149
15.2.2	Configuring LCR	151
15.2.2.1	Enabling the LCR Feature.....	152
15.2.2.2	Configuring Cost Groups.....	153
15.2.2.3	Configuring Time Bands for Cost Groups	154
15.2.2.4	Assigning Cost Groups to Routing Rules.....	156
16	Enabling Applications.....	157
17	Control Network	159
17.1	Configuring SRD Table	159
17.2	Configuring SIP Interface Table	161

17.3	Configuring IP Groups.....	164
17.4	Configuring Proxy Sets Table	171
18	SIP Definitions	177
18.1	Configuring SIP Parameters	177
18.2	Configuring Account Table.....	177
18.3	Configuring Proxy and Registration Parameters.....	179
18.3.1	SIP Message Authentication Example	180
18.4	Configuring SIP Message Manipulation	182
18.5	Configuring SIP Message Policy Rules.....	186
19	Configuring IP Profiles	189
Session Border Controller Application.....		197
20	SBC Overview.....	199
20.1	SIP Network Definitions	200
20.2	SIP Dialog Initiation Process.....	200
20.3	User Registration and Internal Database	202
20.3.1	Initial Registration Request Processing.....	203
20.3.2	Internal Database	203
20.3.3	Routing using Internal Database	204
20.3.4	Registration Refreshes	204
20.3.5	Notification of Expired User Registration to SIP Proxy / Registrar	204
20.3.6	Registration Restriction Control.....	205
20.4	SBC Media Handling.....	205
20.4.1	Media Anchoring without Transcoding (Transparent)	207
20.4.2	No Media Anchoring	207
20.4.3	Restricting Coders	209
20.4.4	Prioritizing Coder List in SDP Offer	210
20.4.5	SRTP-RTP and SRTP-SRTP Transcoding	210
20.4.6	Multiple RTP Media Streams per Call Session	211
20.5	Limiting SBC Call Duration.....	211
20.6	SIP Authentication Server for SBC Users	211
20.7	Interworking SIP Signaling.....	212
20.7.1	Interworking SIP 3xx Redirect Responses	212
20.7.1.1	Resultant INVITE Traversing Device	212
20.7.1.2	Local Handling of SIP 3xx	213
20.7.2	Interworking SIP Diversion and History-Info Headers	214
20.7.3	Interworking SIP REFER Messages.....	214
20.7.4	Interworking SIP PRACK Messages	215
20.7.5	Interworking SIP Session Timer	215
20.7.6	Interworking SIP Early Media	216
20.7.7	Interworking SIP re-INVITE Messages.....	217
20.7.8	Interworking SIP UPDATE Messages	217
20.7.9	Interworking SIP re-INVITE to UPDATE.....	218
20.7.10	Interworking Delayed Offer	218
20.7.11	Interworking Call Hold.....	218
20.8	Call Survivability	218
20.8.1	Auto-Provisioning of Subscriber-Specific Information for BroadWorks Server for Survivability.....	218
20.8.2	BroadSoft's Shared Phone Line Call Appearance for SBC Survivability.....	219
20.8.3	Call Survivability for Call Centers	221
20.8.4	Survivability Mode Display on Aastra IP Phones	223

20.9	Call Forking	223
20.9.1	Initiating SIP Call Forking	223
20.9.2	SIP Forking Initiated by SIP Proxy Server	224
20.10	Alternative Routing on Detection of Failed SIP Response	224
21	SBC Configuration	225
21.1	Configuring General Settings	225
21.2	Configuring Admission Control	226
21.3	Configuring Allowed Coder Groups	228
21.4	Routing SBC	229
21.4.1	Configuring Classification Rules	230
21.4.1.1	Classification Based on URI of Selected Header Example	234
21.4.2	Configuring Condition Rules	235
21.4.3	Configuring SBC IP-to-IP Routing	236
21.4.4	Configuring Alternative Routing Reasons	243
21.5	SBC Manipulations	244
21.5.1	Configuring IP-to-IP Inbound Manipulations	246
21.5.2	Configuring IP-to-IP Outbound Manipulations	249
	Stand-Alone Survivability Application	255
22	SAS Overview	257
22.1	SAS Operating Modes	257
22.1.1	SAS Outbound Mode	258
22.1.1.1	Normal State	258
22.1.1.2	Emergency State	258
22.1.2	SAS Redundant Mode	259
22.1.2.1	Normal State	260
22.1.2.2	Emergency State	260
22.1.2.3	Exiting Emergency and Returning to Normal State	260
22.2	SAS Routing	261
22.2.1	SAS Routing in Normal State	261
22.2.2	SAS Routing in Emergency State	263
23	SAS Configuration	265
23.1	General SAS Configuration	265
23.1.1	Enabling the SAS Application	265
23.1.2	Configuring Common SAS Parameters	266
23.2	Configuring SAS Outbound Mode	268
23.3	Configuring SAS Redundant Mode	269
23.4	Configuring Gateway Application with SAS	269
23.4.1	Gateway with SAS Outbound Mode	270
23.4.2	Gateway with SAS Redundant Mode	271
23.5	Advanced SAS Configuration	273
23.5.1	Manipulating URI user part of Incoming REGISTER	273
23.5.2	Manipulating Destination Number of Incoming INVITE	274
23.5.3	SAS Routing Based on IP-to-IP Routing Table	277
23.5.4	Blocking Calls from Unregistered SAS Users	282
23.5.5	Configuring SAS Emergency Calls	282
23.5.6	Adding SIP Record-Route Header to SIP INVITE	283
23.5.7	Re-using TCP Connections	284
23.5.8	Replacing Contact Header for SIP Messages	284

23.6 Viewing Registered SAS Users.....	284
24 SAS Cascading.....	285
High Availability System	287
25 Overview	289
25.1 Connectivity and Synchronization between Devices.....	289
25.2 Device Switchover upon Failure.....	290
25.3 HA Status	291
26 HA Configuration.....	293
26.1 Initial HA Configuration	293
26.1.1 Network Topology Types	293
26.1.1.1 Tx/Rx Port Settings	293
26.1.2 Configuring the HA Devices	295
26.1.2.1 Step 1: Configure the First Device	295
26.1.2.2 Step 2: Configure the Second Device	297
26.1.2.3 Step 3: Initialize HA on the Devices	298
26.2 Configuration while HA is Operational	298
26.3 Configuring Firewall Allowed Rules.....	299
27 HA Maintenance	301
27.1 Maintenance of Redundant Device	301
27.2 Replacing a Failed Device	301
27.3 Forcing a Switchover.....	301
27.4 Software Upgrade	301
Maintenance.....	303
28 Basic Maintenance	305
28.1 Resetting the Device	305
28.2 Remotely Resetting Device using SIP NOTIFY	306
28.3 Locking and Unlocking the Device	307
28.4 Saving Configuration.....	308
29 High Availability Maintenance.....	309
30 Software Upgrade.....	311
30.1 Loading Auxiliary Files	311
30.1.1 Call Progress Tones File	312
30.1.2 Dial Plan File.....	315
30.1.2.1 Creating a Dial Plan File.....	315
30.1.2.2 Obtaining IP Destination from Dial Plan File	315
30.1.3 User Information File	316
30.1.3.1 User Information File for SBC User Database	316
30.1.3.2 Enabling the User Info Table.....	317
30.2 Software License Key	317
30.2.1 Obtaining the Software License Key File.....	317
30.2.2 Installing the Software License Key.....	318
30.2.2.1 Installing Software License Key using Web Interface	319
30.3 Software Upgrade Wizard	320

30.4	Backing Up and Loading Configuration File	324
31	Returning the System to a Previous State	325
31.1	Taking a Snapshot	325
31.2	Returning to a Snapshot State	326
31.3	Automatic Recovery to Default Snapshot	326
32	Automatic Update.....	327
32.1	Configuring Automatic Update	327
32.2	Automatic Configuration Methods	330
32.2.1	DHCP-based Configuration Server	330
32.2.2	HTTP-based Automatic Updates	330
32.2.3	Configuration using FTP or NFS	331
32.3	Loading Files Securely (Disabling TFTP).....	332
32.4	Remotely Triggering Auto Update using SIP NOTIFY	332
33	Restoring Factory Defaults	333
33.1	Restoring Defaults using CLI	333
33.2	Restoring Defaults using an ini File.....	334
Status, Performance Monitoring and Reporting		335
34	System Status	337
34.1	Viewing Device Information.....	337
34.2	Viewing Ethernet Port Information	338
35	Carrier-Grade Alarms.....	339
35.1	Viewing Active Alarms.....	339
35.2	Viewing Alarm History	339
36	Performance Monitoring.....	341
36.1	Viewing MOS per Media Realm	341
36.2	Viewing Quality of Experience	342
36.3	Viewing Average Call Duration	343
37	VoIP Status	345
37.1	Viewing Active IP Interfaces.....	345
37.2	Viewing Registered Users.....	345
38	Reporting Information to External Party	347
38.1	RTP Control Protocol Extended Reports (RTCP XR)	347
38.2	Generating Call Detail Records.....	350
38.2.1	Configuring CDR Reporting	350
38.2.2	CDR Field Description	351
38.2.2.1	CDR Fields for SBC Signaling	351
38.2.2.2	CDR Fields for SBC Media	353
38.3	Configuring RADIUS Accounting	354
Diagnostics		359

39	Syslog and Debug Recordings	361
39.1	Syslog Message Format	361
39.1.1	Event Representation in Syslog Messages	362
39.1.2	Identifying AudioCodes Syslog Messages using Facility Levels	364
39.1.3	SNMP Alarms in Syslog Messages	364
39.2	Configuring Syslog Settings	365
39.3	Configuring Debug Recording	366
39.4	Filtering Syslog Messages and Debug Recordings	367
39.4.1	Filtering IP Network Traces	368
39.5	Viewing Syslog Messages	370
39.6	Collecting Debug Recording Messages	371
40	Testing SIP Signaling Calls	373
40.1	Configuring Test Call Endpoints	373
40.1.1	Starting, Stopping and Restarting Test Calls	376
40.1.2	Viewing Test Call Statistics	377
40.2	Configuring DTMF Tones for Test Calls	378
40.3	Configuring SBC Test Call with External Proxy	379
40.4	Test Call Configuration Examples	380
Appendix		383
41	Dialing Plan Notation for Routing and Manipulation	385
42	Configuration Parameters Reference	387
42.1	Networking Parameters	387
42.1.1	Ethernet Parameters	387
42.1.2	Multiple VoIP Network Interfaces and VLAN Parameters	388
42.1.3	Routing Parameters	388
42.1.4	Quality of Service Parameters	389
42.1.5	NAT and STUN Parameters	390
42.1.6	NFS Parameters	390
42.1.7	DNS Parameters	391
42.1.8	DHCP Parameters	392
42.1.9	NTP and Daylight Saving Time Parameters	393
42.2	Management Parameters	394
42.2.1	General Parameters	394
42.2.2	Web Parameters	394
42.2.3	Telnet Parameters	397
42.2.4	SNMP Parameters	398
42.2.5	Serial Parameters	400
42.3	Debugging and Diagnostics Parameters	401
42.3.1	General Parameters	401
42.3.2	SIP Test Call Parameters	401
42.3.3	Syslog, CDR and Debug Parameters	402
42.3.4	Resource Allocation Indication Parameters	406
42.4	Security Parameters	407
42.4.1	General Parameters	407
42.4.2	HTTPS Parameters	407
42.4.3	SRTP Parameters	409
42.4.4	TLS Parameters	411
42.4.5	SSH Parameters	413
42.4.6	OCSP Parameters	414

42.4.7	IDS Parameters	415
42.5	RADIUS Parameters	416
42.6	SIP Media Realm Parameters.....	418
42.7	Control Network Parameters.....	420
42.7.1	IP Group, Proxy, Registration and Authentication Parameters	420
42.7.2	Network Application Parameters	427
42.8	General SIP Parameters	429
42.9	Profile Parameters	447
42.10	Channel Parameters	448
42.10.1	RTP, RTCP and T.38 Parameters.....	448
42.11	Least Cost Routing Parameters	450
42.12	LDAP Parameters	451
42.13	SBC Parameters	453
42.14	Standalone Survivability Parameters	465
42.15	IP Media Parameters	469
42.16	Auxiliary and Configuration File Name Parameters	470
42.17	Automatic Update Parameters	471
43	Specifications	473

Reader's Notes

Notice

This document describes the AudioCodes Mediant Software SBC.

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Before consulting this document, check the corresponding Release Notes regarding feature preconditions and/or specific support in this release. In cases where there are discrepancies between this document and the Release Notes, the information in the Release Notes supersedes that in this document. Updates to this document and other documents as well as software files can be downloaded by registered customers at <http://www.audiocodes.com/downloads>.

© Copyright 2014 AudioCodes Ltd. All rights reserved.

This document is subject to change without notice.

Date Published: March-03-2014

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 manual, unless otherwise specified, the term *device* refers to the Mediant Software SBC.

Related Documentation

Manual Name
SIP CPE Release Notes
Mediant Software E-SBC Virtual Edition Installation Manual
Mediant Software E-SBC Server Edition Installation Manual
SBC Design Guide

Notes and Warnings



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 should refer to AudioCodes *Recommended Security Guidelines* document.



Note: Before configuring the device, ensure that it is installed correctly as instructed in the *Installation Manual*.



Legal Notice:

- By default, the device supports export-grade (40-bit and 56-bit) encryption due to US government restrictions on the export of security technologies. To enable 128-bit and 256-bit encryption on your device, contact your AudioCodes sales representative.
- This device includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>).
- This device includes cryptographic software written by Eric Young (eay@cryptsoft.com).

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 Overview

AudioCodes' Mediant Software Enterprise Session Border Controller (E-SBC) is a pure-software, server-based product enabling connectivity and security between Enterprises' and Service Providers' VoIP networks. The Mediant Software E-SBC provides perimeter defense as a way of protecting companies from malicious VoIP attacks; mediation for allowing the connection of any PBX and / or IP-PBX to any Service Provider; and service assurance for service quality and manageability.

The device offers call "survivability" using its Stand Alone Survivability (SAS) application, which ensures service continuity to enterprises served by a centralized SIP-based IP-Centrex server or branch offices of distributed enterprises. SAS enables internal office communication between SIP clients in the case of disconnection from the centralized SIP IP-Centrex server or IP-PBX.

The device allows full management through its HTTP/S-based Web server. This user-friendly Web interface allows remote configuration using any standard Web browser (such as Microsoft™ Internet Explorer™).

Mediant Software E-SBC is available in the following editions:

- **Server Edition** - x86 server based platform. The Server Edition must be installed on a server with the following hardware requirements:
 - Platform – any of the following:
 - ◆ HP ProLiant DL120 G7
 - ◆ HP ProLiant DL320e G8
 - Processor: Intel Xeon E3-1220 or E3-1220v2 (4 cores, 3.1 GHz, 8M Cache)
 - Memory: 4 GB
 - Disk space: 72 GB or more
 - Installation from CD/DVD drive
 - Installation interface: VGA Monitor and Keyboard
- **Virtual Edition** - installed and hosted in a virtual machine environment. The Mediant Software E-SBC Virtual Edition can be installed on a VMware ESXi host, with sufficient available resources, running version 5.0 or later:
 - Host OS: VMware ESXi version 5.0 or later
 - Processor: 2 Cores or more.
 - Memory: 4 GB or more
 - Disk space: 60 GB or more
 - Network: At least two virtual networks preconfigured



Notes:

- When upgrading from Version 6.4 to 6.6 using the Web interface, the Software Upgrade Wizard is not supported. Customers should back up the current configuration (ini file), install the new 6.6 version from the installation CD, and then restore configuration.
- Customers who upgrade to Version 6.6 need a new Software License Key. Refer to the *Installation Manual* on how to obtain the new Software License Key.

Reader's Notes

Part I

Getting Started with Initial Connectivity

2 Installing the Software

The Mediant Software E-SBC package consists of an installation CD containing Mediant Software E-SBC software, AudioCodes utilities, and related documentation.

For installing the device, refer to the following documents:

- **Server Edition:** *Mediant Software E-SBC Server Edition Installation Manual*
- **Virtual Edition:** *Mediant Software E-SBC Virtual Edition Installation Manual*

Reader's Notes

3 Changing Default IP Address to Suit your Network Addressing Scheme

After initial installation, the device is assigned the following default IP address:

- **IP Address:** 192.168.0.1
- **Subnet Mask:** 255.255.255.0

You can change this default IP address to suit your network addressing scheme. Once done, you can connect to the device's Web-based management tool (Web interface) using this new IP address.

➤ **To change the IP address using CLI:**

1. Establish a CLI session with the device:
 - **Server Edition:** Use a VGA monitor and keyboard to connect to the CLI management interface.
 - **Virtual Edition:** Click the VM's Console tab to connect to the CLI management interface.
2. At the CLI prompt, type the username (default is "Admin" - case sensitive), and then press Enter:

```
Username: Admin
```

3. At the prompt, type the password (default is "Admin" - case sensitive), and then press Enter:

```
Password: Admin
```

The following prompt appears:

```
Welcome to AudioCodes CLI
```

```
Username: Admin
```

```
Password:
```

```
Mediant SW>
```

4. At the prompt, type the following, and then press Enter:

```
# enable
```
5. At the prompt, type the password, and then press Enter:

```
Password: Admin
```
6. At the prompt, type the following commands to access the network interface configuration:

```
# configure voip
(config-voip)# interface network-if 0
(network-if-0)#
```



Note: To ensure that you type the correct command syntax, use the Tab key to auto-complete partially entered commands.

7. At the prompt, type the following commands to configure the IP address, prefix length and default gateway:

```
(network-if-0)# set ip <IP address, e.g. 10.4.212.155>
(network-if-0)# set prefix-length <prefix length, e.g., 16>
(network-if-0)# set gateway <default gateway, e.g., 10.4.0.1>
```

8. If the device is connected to the IP network that uses VLAN ID, type the following

command to configure it:

```
(network-if-0)# set vlan-id <VLAN ID>
```

9. At the prompt, type the following to complete configuration:

```
(network-if-0)# exit
```

```
(config-voip)# exit
```

10. At the prompt, make sure that Port #1 is connected (i.e., link is UP) using the **show voip ports** command. This port is mapped to network-if-0, by default. For more information on mapping physical ports to the logical configuration ports, see "Configuring Tx/Rx for Ethernet Port-Pair Groups" on page 88.
11. At the prompt, type the following to reset the device and activate the new configuration:

```
# reload now
```

Once you have assigned an IP address that suits your network environment, you can connect remotely with this IP address to the device's Web interface for management and configuration. To access the Web interface, see "Web-Based Management" on page 29.

For initial setup, it is recommended to configure the following network settings:

- To modify and configure IP network interfaces, see "Configuring IP Network Interface" on page 90
- To configure the used physical Ethernet ports (Native VLAN, speed, and mode), see "Configuring Physical Ethernet Ports" on page 87.

4 Licensing the Device

The device is shipped by default with a pre-installed Software License Key that enables **only one** call session. After installation has completed successfully, you need to load the Software License Key file supplied in the package, to enable the call capacity and features that you ordered.

For loading a Software License Key to the device, see 'Software License Key' on page [317](#).

Reader's Notes

Part II

Management Tools

5 Introduction

This part provides an overview of the various management tools that can be used to configure the device. It also provides step-by-step procedures on how to configure the management settings.

The following management tools can be used to configure the device:

- Embedded HTTP/S-based Web server - see "Web-based Management" on page [29](#)
- Command Line Interface (CLI) - see "CLI-Based Management" on page [57](#)
- Simple Network Management Protocol (SNMP) browser software - see "SNMP-Based Management" on page [65](#)
- Configuration *ini* file - see "INI File-Based Management" on page [71](#)

**Notes:**

- Some configuration settings can only be done using a specific management tool. For example, some configuration can only be done using the Configuration *ini* file method.
- Throughout this manual, where a parameter is mentioned, its corresponding Web and ini parameter is mentioned. The *ini* file parameters are enclosed in square brackets [...].
- For a list and description of all the configuration parameters, see "Configuration Parameters Reference" on page [387](#).

Reader's Notes

6 Web-Based Management

The device provides an embedded Web server (hereafter referred to as *Web interface*), supporting fault management, configuration, accounting, performance, and security (FCAPS), including the following:

- Full configuration
- Software and configuration upgrades
- Loading auxiliary files, for example, the Call Progress Tones file
- Real-time, online monitoring of the device, including display of alarms and their severity
- Performance monitoring of voice calls and various traffic parameters

The Web interface provides a user-friendly, graphical user interface (GUI), which can be accessed using any standard Web browser (e.g., Microsoft™ Internet Explorer).

Access to the Web interface is controlled by various security mechanisms such as login user name and password, read-write privileges, and limiting access to specific IP addresses.



Notes:

- The Web interface allows you to configure most of the device's settings. However, additional configuration parameters may exist that are not available in the Web interface and which can only be configured using other management tools.
- Some Web interface pages and/or parameters are available only for certain hardware configurations or software features. The software features are determined by the installed Software License Key (see "Loading Software License Key" on page 320).

6.1 Getting Acquainted with the Web Interface

This section provides a description of the Web interface.

6.1.1 Computer Requirements

The client computer requires the following to work with the Web interface of the device:

- A network connection to the device
- One of the following Web browsers:
 - Microsoft™ Internet Explorer™ (Version 6.0 and later)
 - Mozilla Firefox® (Versions 5 through 9.0)
- Recommended screen resolutions: 1024 x 768 pixels, or 1280 x 1024 pixels



Note: Your Web browser must be JavaScript-enabled to access the Web interface.

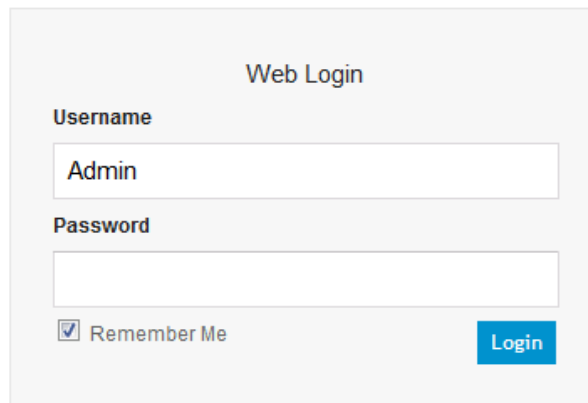
6.1.2 Accessing the Web Interface

The procedure below describes how to access the Web interface.

➤ **To access the Web interface:**

1. Open a standard Web browser (see "Computer Requirements" on page 29).
2. In the Web browser, specify the IP address of the device (e.g., <http://10.1.10.10>); the Web interface's Login window appears, as shown below:

Figure 6-1: Web Login Screen



The image shows a web login interface titled "Web Login". It contains two input fields: "Username" with the text "Admin" entered, and "Password" which is empty. Below the password field is a checkbox labeled "Remember Me" which is checked. To the right of the checkbox is a blue button labeled "Login".

3. In the 'Username' and 'Password' fields, enter the case-sensitive, user name and password respectively.
4. Click **Login**; the Web interface is accessed, displaying the Home page. For a detailed description of the Home page, see "Viewing the Home Page" on page 44.



Notes:

- By default, Web access is only through the IP address of the OAMP interface. However, you can allow access from any of the device's IP network interfaces (i.e., OAMP, Control, or Media), by setting the EnableWebAccessFromAllInterfaces parameter to 1.
- The default username and password is "Admin". To change the login user name and password, see "Configuring the Web User Accounts" on page 46.
- If you want the Web browser to remember your password, select the 'Remember Me' check box and then agree to the browser's prompt (depending on your browser) to save the password for future logins. On your next login attempt, simply press the Tab or Enter keys to auto-fill the 'Username' and 'Password' fields, and then click **Login**.

6.1.3 Areas of the GUI

The areas of the Web interface's GUI are shown in the figure below and described in the subsequent table.

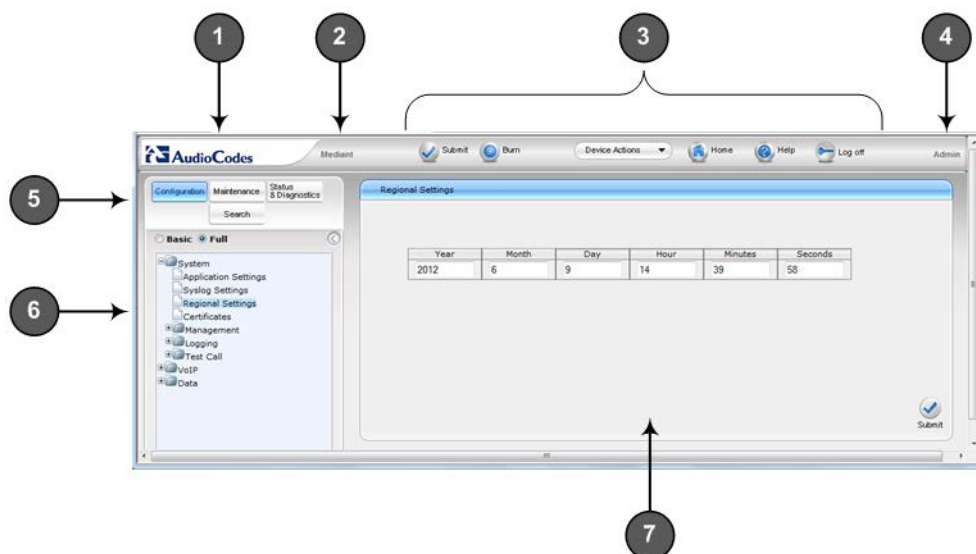








Table 6-1: Description of the Web GUI Areas

Item #	Description
1	Displays AudioCodes (corporate) logo image.
2	Displays the product name.
3	Toolbar, providing frequently required command buttons. For more information, see "Toolbar Description" on page 32.
4	Displays the username of the Web user that is currently logged in.
5	Navigation bar, providing the following tabs for accessing various functionalities in the Navigation tree: <ul style="list-style-type: none"> ▪ Configuration, Maintenance, and Status & Diagnostics tabs: Access the configuration menus (see "Working with Configuration Pages" on page 35) ▪ Search tab: Enables a search engine for searching configuration parameters (see "Searching for Configuration Parameters" on page 41)
6	Navigation tree, displaying a tree-like structure of elements (configuration menus or search engine) pertaining to the selected tab on the Navigation bar. For more information, see "Navigation Tree" on page 33.
7	Work pane, displaying the configuration page of the selected menu in the Navigation tree. This is where configuration is done. For more information, see "Working with Configuration Pages" on page 35.

6.1.4 Toolbar Description

The toolbar provides frequently required command buttons, described in the table below:

Table 6-2: Description of Toolbar Buttons

Icon	Button Name	Description
	Submit	Applies parameter settings to the device (see "Saving Configuration" on page 308). Note: This icon is grayed out when not applicable to the currently opened page.
	Burn	Saves parameter settings to flash memory (see "Saving Configuration" on page 308).
	Device Actions	Opens a drop-down list with frequently needed commands: <ul style="list-style-type: none"> ▪ Load Configuration File: Opens the Configuration File page for loading an <i>ini</i> file to the device (see "Backing Up and Loading Configuration File" on page 324). ▪ Save Configuration File: Opens the Configuration File page for saving the <i>ini</i> file to a folder on a computer (see "Backing Up and Loading Configuration File" on page 324). ▪ Reset: Opens the Maintenance Actions page for performing various maintenance procedures such as resetting the device (see "Resetting the Device" on page 305). ▪ Software Upgrade Wizard: starts the Software Upgrade wizard for upgrading the device's software (see "Software Upgrade Wizard" on page 320). ▪ Switch Over: Opens the High Availability Maintenance page for switching between Active and Redundant blades (see High Availability Maintenance on page 309). ▪ Reset Redundant: Opens the High Availability Maintenance page for resetting the Redundant blade (see High Availability Maintenance on page 309).
	Home	Opens the Home page (see "Viewing the Home Page" on page 44).
	Help	Opens the Online Help topic of the currently opened configuration page (see "Getting Help" on page 43).
	Log off	Logs off a session with the Web interface (see "Logging Off the Web Interface" on page 44).



Note: If you modify a parameter that takes effect only after a device reset, after you click the **Submit** button in the configuration page, the toolbar displays "Reset", as shown in the figure below. This is a reminder that you need to later save your settings to flash memory and reset the device.

Figure 6-2: "Reset" Displayed on Toolbar



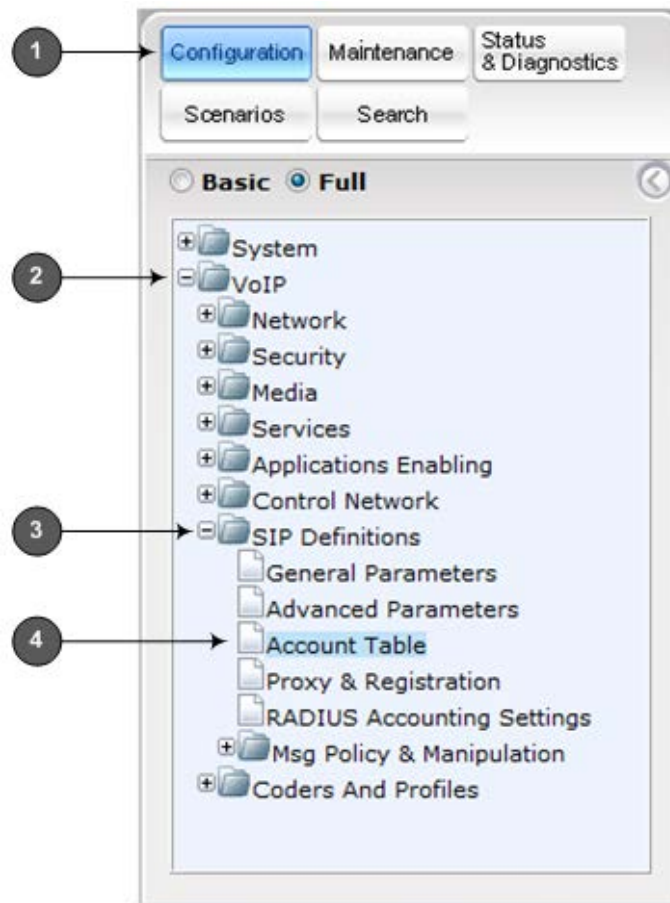
6.1.5 Navigation Tree

The Navigation tree is located in the Navigation pane and displays a tree-like structure of menus pertaining to the selected tab on the Navigation bar. You can drill-down to the required page item level to open its corresponding page in the Work pane.

The terminology used throughout this manual for referring to the hierarchical structure of the tree is as follows:

- *Menu*: first level (highest level)
- *Submenu*: second level - contained within a menu
- *Page item*: last level (lowest level in a menu) - contained within a menu or submenu

Figure 6-3: Navigating in Hierarchical Menu Tree (Example)



Note: The figure above is used only as an example. The displayed menus depend on supported features based on the Software License Key installed on your device.

6.1.5.1 Displaying Navigation Tree in Basic and Full View

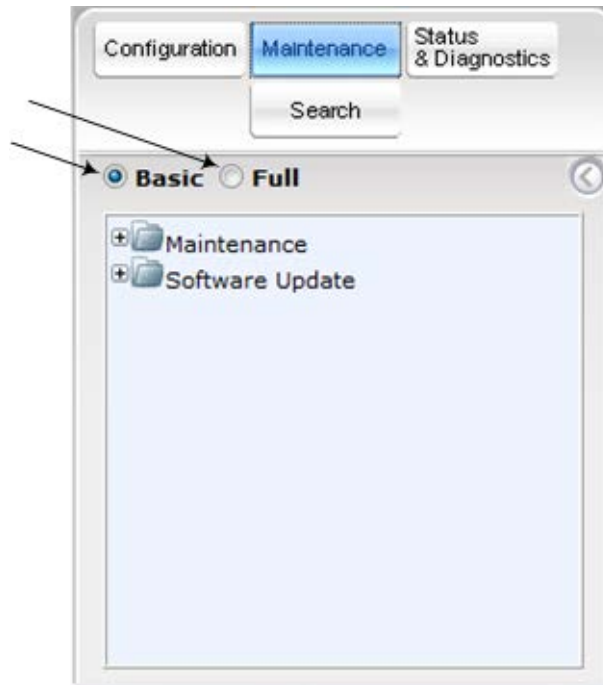
You can view an expanded or reduced display of the Navigation tree. This affects the number of displayed menus and submenus in the tree. The expanded (*Full*) view displays all the menus pertaining to the selected configuration tab; the reduced (*Basic*) view displays only commonly used menus. This is relevant when using the configuration tabs

(i.e., **Configuration**, **Maintenance**, and **Status & Diagnostics**) on the Navigation bar. The advantage of the Basic view is that it prevents "cluttering" of the Navigation tree with menus that may not be required.

➤ **To toggle between Full and Basic view:**

- To display a reduced menu tree, select the **Basic** option (default).
- To display all the menus and submenus in the Navigation tree, select the **Full** option.

Figure 6-4: Basic and Full View Options




Note: After you reset the device, the Web GUI is displayed in Basic view.

6.1.5.2 Showing / Hiding the Navigation Pane

You can hide the Navigation pane to provide more space for elements displayed in the Work pane. This is especially useful when the Work pane displays a wide table. The arrow button located below the Navigation bar is used to hide and show the pane.

➤ **To hide and show the Navigation pane:**

- **To hide the Navigation pane:** Click the left-pointing arrow ; the pane is hidden and the button is replaced by the right-pointing arrow button.


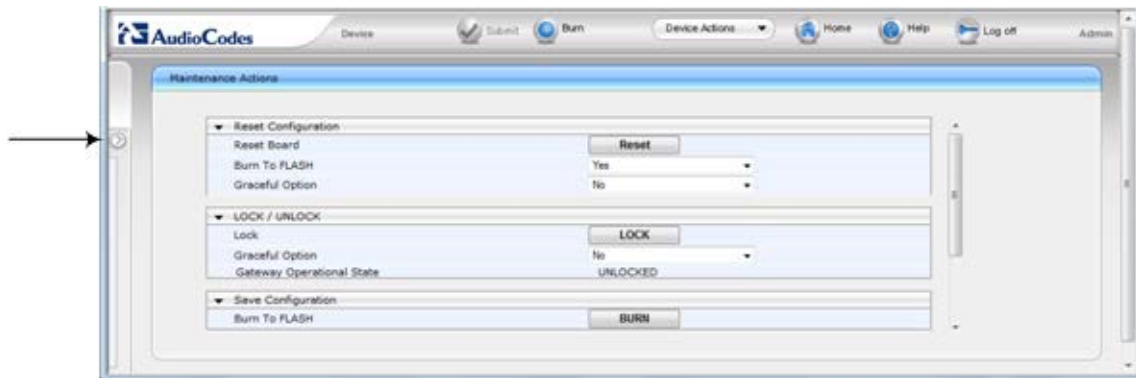
- **To show the Navigation pane:** Click the right-pointing arrow ; the pane is displayed and the button is replaced by the left-pointing arrow button.

Figure 6-5: Show and Hide Button (Navigation Pane in Hide View)





6.1.6 Working with Configuration Pages

The configuration pages contain the parameters for configuring the device and are displayed in the Work pane.

6.1.6.1 Accessing Pages

The configuration pages are accessed by clicking the required page item in the Navigation tree.

➤ To open a configuration page:

1. On the Navigation bar, click the required tab (**Configuration**, **Maintenance**, or **Status & Diagnostics**); the menus pertaining to the selected tab appear in the Navigation tree.
2. Navigate to the required page item, by performing the following:
 - Drill-down using the **plus**  sign to expand the menu and submenus.
 - Drill-up using the **minus**  sign to collapse the menu and submenus.
3. Click the required page item; the page opens in the Work pane.

You can also access previously opened pages by clicking the Web browser's **Back** button until you have reached the required page. This is useful if you want to view pages in which you have performed configurations in the current Web session.

Notes:

- You can also access certain pages from the **Device Actions** button located on the toolbar (see "Toolbar Description" on page 32).
- To view all the menus in the Navigation tree, ensure that the Navigation tree is in Full view (see "Displaying Navigation Tree in Basic and Full View" on page 33).
- To get Online Help for the currently displayed page, see "Getting Help" on page 43.
- Certain pages may not be accessible or may be read-only, depending on the access level of your Web user account (see "Configuring Web User Accounts" on page 46). If a page is read-only, "Read-Only Mode" is displayed at the bottom of the page.



6.1.6.2 Viewing Parameters

Some pages allow you to view a reduced or expanded display of parameters. The Web interface provides two methods for displaying page parameters:

- Displaying "basic" and "advanced" parameters - see "Displaying Basic and Advanced Parameters" on page 36
- Displaying parameter groups - see "Showing / Hiding Parameter Groups" on page 37

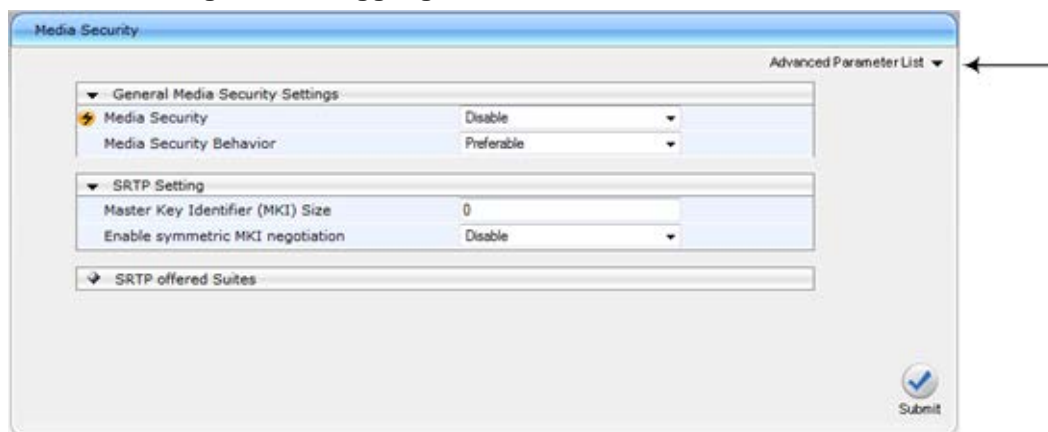
6.1.6.2.1 Displaying Basic and Advanced Parameters

Some pages provide a toggle button that allows you to show and hide parameters that typically are used only in certain deployments. This button is located on the top-right corner of the page and has two display states:

- **Advanced Parameter List** button with down-pointing arrow: click this button to display all parameters.
- **Basic Parameter List** button with up-pointing arrow: click this button to show only common (*basic*) parameters.

The figure below shows an example of a page displaying basic parameters only. If you click the **Advanced Parameter List** button (shown below), the page will also display the advanced parameters.

Figure 6-6: Toggling between Basic and Advanced View



Notes:

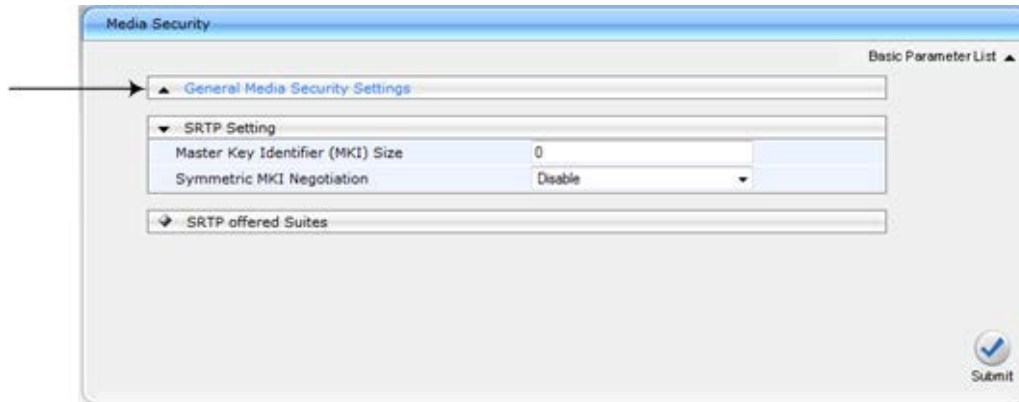
- When the Navigation tree is in Full mode (see "Navigation Tree" on page 33), configuration pages display all their parameters.
- If a page contains only basic parameters, the **Basic Parameter List** button is not displayed.
- If you reset the device, the Web pages display only the basic parameters.
- The basic parameters are displayed in a dark blue background.



6.1.6.2.2 Showing / Hiding Parameter Groups

Some pages provide groups of parameters, which can be hidden or shown. To toggle between hiding and showing a group, simply click the group title button that appears above each group. The button appears with a down-pointing or up-pointing arrow, indicating that it can be collapsed or expanded when clicked, respectively.

Figure 6-7: Expanding and Collapsing Parameter Groups



6.1.6.3 Modifying and Saving Parameters



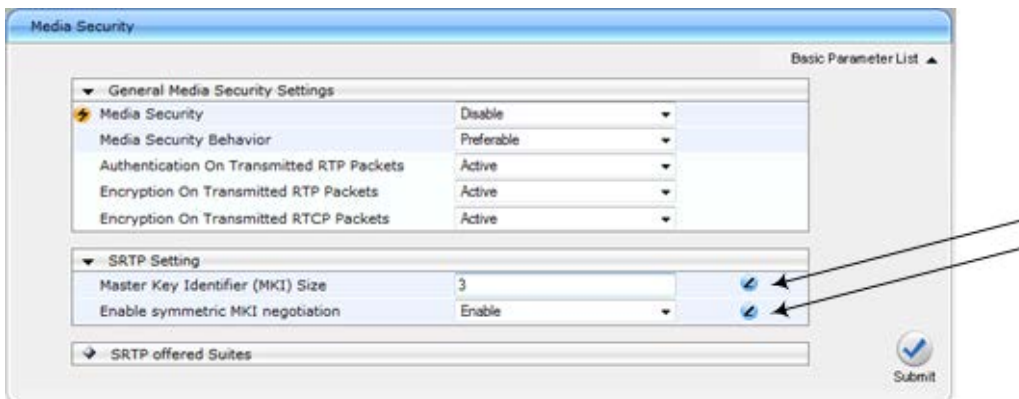



When you modify a parameter value on a page, the **Edit**  symbol appears to the right of the parameter. This indicates that the parameter has been modified, but has yet to be applied (submitted). After you apply your modifications, the  symbol disappears.

Figure 6-8: Edit Symbol after Modifying Parameter Value



- **To save configuration changes on a page to the device's volatile memory (RAM), do one of the following:**

- On the toolbar, click the **Submit**  button.
- At the bottom of the page, click the **Submit**  button.

When you click **Submit**, modifications to parameters with on-the-fly capabilities are immediately applied to the device and take effect. Parameters displayed on the page with the lightning bolt  symbol take effect only after a device reset. For resetting the device, see "Resetting the Device" on page 305.



Note: Parameters saved to the volatile memory (by clicking **Submit**), revert to their previous settings after a hardware or software reset, or if the device is powered down. Therefore, to ensure parameter changes (whether on-the-fly or not) are retained, save ('burn') them to the device's non-volatile memory, i.e., flash (see "Saving Configuration" on page 308).

If you enter an invalid parameter value (e.g., not in the range of permitted values) and then click **Submit**, a message box appears notifying you of the invalid value. In addition, the parameter value reverts to its previous value and is highlighted in red, as shown in the figure below:

Figure 6-9: Value Reverts to Previous Valid Value



6.1.6.4 Working with Tables

This section describes how to work with configuration tables, which are provided in basic or enhanced design, depending on the configuration page.

6.1.6.4.1 Basic Design Tables

A few of the tables in the Web interface are in basic design format. The figure below displays a typical table in the basic design format and the subsequent table describes its command buttons.

Figure 6-10: Adding an Index Entry to a Table

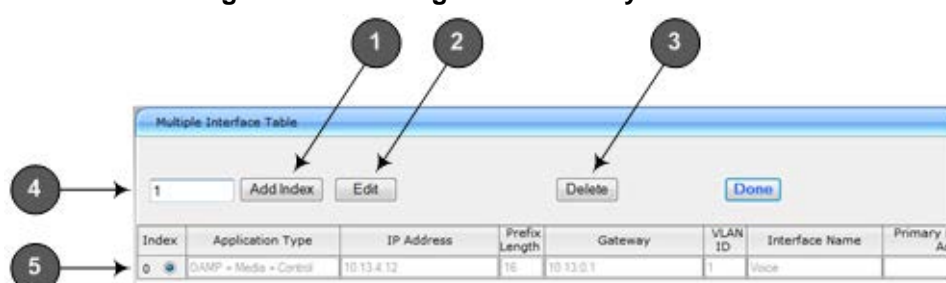


Table 6-3: Basic Table Design Description

Item #	Button / Field	
1	Add Index (or Add) button	Adds an index entry row to the table.
2	Edit	Edits the selected row.
3	Delete	Removes the selected row from the table.
4	'Add Index' field	Defines the index number. When adding a new row, enter the required index number in this field, and then click Add

Item #	Button / Field	
		Index.
5	Index radio button	Selects the row for editing and deleting.
-	Compact button	Organizes the index entries in ascending, consecutive order, starting from index 0. For example, assume you have three index entries, 0, 4 and 6. After you click Compact , index entry 4 is re-assigned to index 1 and index entry 6 is re-assigned to index 2.
-	Apply button	Saves the row configuration. Click this button after you add or edit each index entry.

6.1.6.4.2 Enhanced Design Tables

Most of the tables in the Web interface are designed in the enhanced table format. The figure below displays a typical table in the enhanced design format and the subsequent table describes its command buttons and areas.

Figure 6-11: Displayed Details Pane

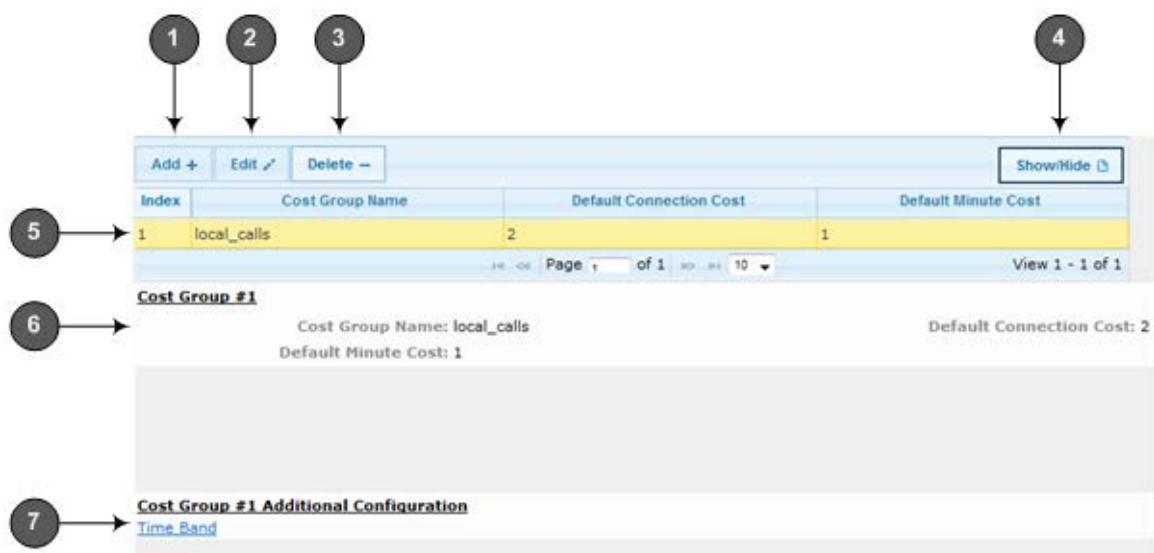
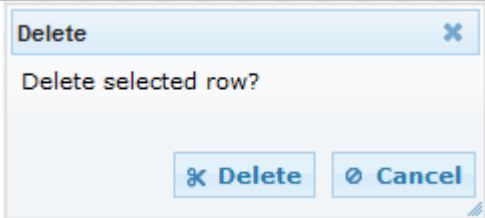


Table 6-4: Enhanced Table Design Description

Item #	Button	
1	Add	Adds a new index entry row to the table. When you click this button, a dialog box appears with parameters for configuring the new entry. When you have completed configuration, click the Submit button in the dialog box to add it to the table.
2	Edit	Edits the selected row.
3	Delete	Removes the selected row from the table. When you click this button, a confirmation box appears requesting you to confirm deletion. Click Delete to accept deletion.

Item #	Button	
		
4	Show/Hide	Toggles between displaying and hiding the full configuration of a selected row. This configuration is displayed below the table (see Item #6) and is useful for large tables that cannot display all its columns in the work pane.
5	-	Selected index row entry for editing, deleting and showing configuration.
6	-	Displays the full configuration of the selected row when you click the Show/Hide button.
7	-	Links to access additional configuration tables related to the current configuration.

If the configuration of an entry row is invalid, the index of the row is highlighted in red, as shown below:

Figure 6-12: Invalid Configuration with Index Highlighted in Red



The table also enables you to define the number of rows to display on the page and to navigate between pages displaying multiple rows. This is done using the page navigation area located below the table, as shown in the figure below:

Figure 6-13: Viewing Table Rows per Page

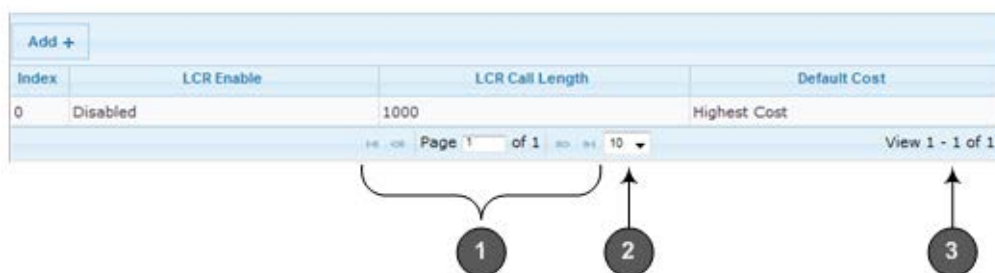


Table 6-5: Row Display and Page Navigation

Item #	Description
1	<p>Defines the page that you want to view. Enter the required page number or use the following page navigation buttons:</p> <ul style="list-style-type: none"> ➡ - Displays the next page ➡➡ - Displays the last page ⬅️ - Displays the previous page ⬅️⬅️ - Displays the first page
2	<p>Defines the number of rows to display per page. You can select 5 or 10, where the</p>

Item #	Description
	default is 10.
3	Displays the currently displayed page number.

6.1.7 Searching for Configuration Parameters

You can locate the exact Web page on which a specific parameter appears, by using the device's Search feature. The Web parameter's corresponding *ini* file parameter name is used as the search key. The search key can include the full parameter name (e.g., "EnableIPSec") or a substring of it (e.g., "sec"). If you search for a substring, all parameters containing the specified substring in their names are listed in the search result.



Note: If an *ini* file parameter is not configurable in the Web interface, the search fails.

➤ **To search for a parameter:**

1. On the Navigation bar, click the **Search** tab; the Search engine appears in the Navigation pane.
2. In the field alongside the **Search** button, enter the parameter name or a substring of the name for which you want to search. If you have done a previous search for such a parameter, instead of entering the required string, you can use the 'Search History' drop-down list to select the string saved from a previous search.
3. Click **Search**; a list of found parameters based on your search key appears in the Navigation pane. Each searched result displays the following:
 - *ini* file parameter name
 - Link (in green) to the Web page on which the parameter appears
 - Brief description of the parameter
 - Menu navigation path to the Web page on which the parameter appears
4. In the searched list, click the required parameter (green link) to open the page on which the parameter appears; the relevant page opens in the Work pane and the searched parameter is highlighted in the page for easy identification, as shown in the figure below:

Figure 6-14: Searched Result Screen

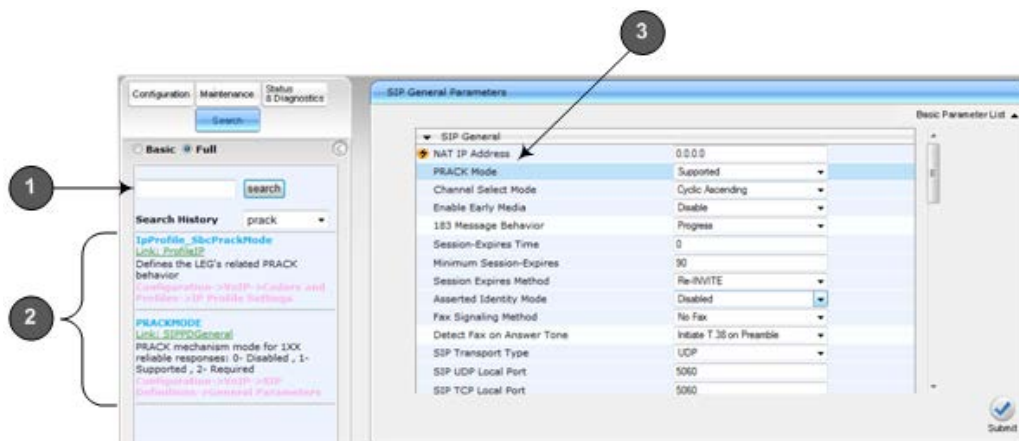
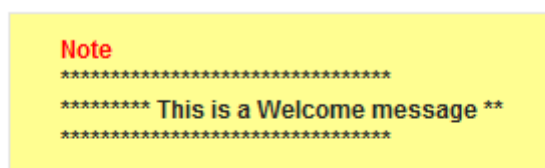
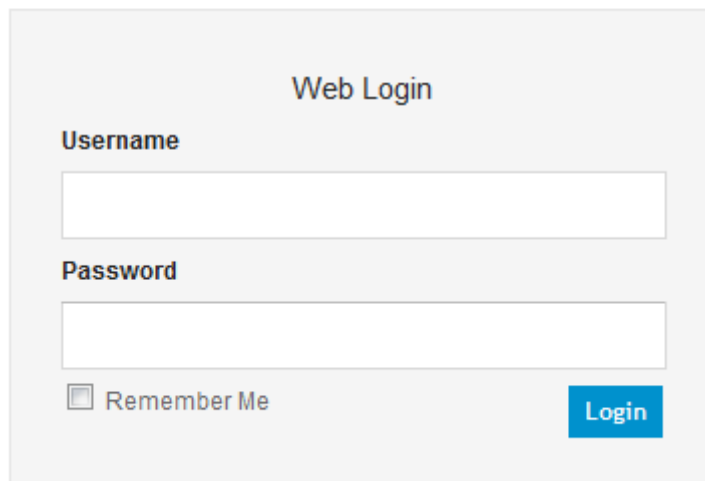


Table 6-6: Search Description

Item #	Description
1	Search field for entering search key and Search button for activating the search process.
2	Search results listed in Navigation pane.
3	Found parameter, highlighted on relevant Web page

6.1.8 Creating a Login Welcome Message

You can create a Welcome message box that is displayed on the Web Login page for logging in to the Web interface. The figure below displays an example of a Welcome message:

Figure 6-15: User-Defined Web Welcome Message after Login



To enable and create a Welcome message, use the WelcomeMessage table ini file parameter. If this parameter is not configured, no Welcome message is displayed.

Table 6-7: ini File Parameter for Welcome Login Message

Parameter	Description
[WelcomeMessage]	Enables and defines a Welcome message that appears on the Web Login page for logging in to the Web interface. The format of this parameter is as follows: [WelcomeMessage] FORMAT WelcomeMessage_Index = WelcomeMessage_Text; [WelcomeMessage]

Parameter	Description
	<p>For Example:</p> <pre>[WelcomeMessage] FORMAT WelcomeMessage_Index = WelcomeMessage_Text; WelcomeMessage 1 = "*****", WelcomeMessage 2 = "***** This is a Welcome message **", WelcomeMessage 3 = "*****", [WelcomeMessage]</pre> <p>Each index row represents a line of text in the Welcome message box. Up to 20 lines (or rows) of text can be defined.</p>

6.1.9 Getting Help

The Web interface provides you with context-sensitive Online Help. The Online Help provides brief descriptions of parameters pertaining to the currently opened page.

- To view the Help topic of a currently opened page:


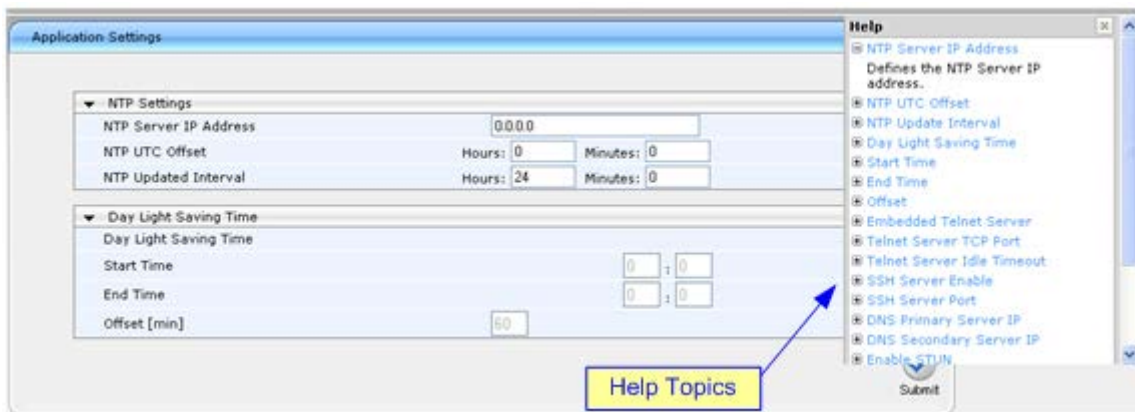




1. On the toolbar, click the **Help**  button; the Help topic pertaining to the opened page appears, as shown below:

Figure 6-16: Help Topic for Current Page



2. To view a description of a parameter, click the **plus**  sign to expand the parameter. To collapse the description, click the **minus**  sign.
3. To close the Help topic, click the **close**  button located on the top-right corner of the Help topic window or simply click the **Help**  button.



Note: Instead of clicking the **Help** button for each page you open, you can open it once for a page and then simply leave it open. Each time you open a different page, the Help topic pertaining to that page is automatically displayed.

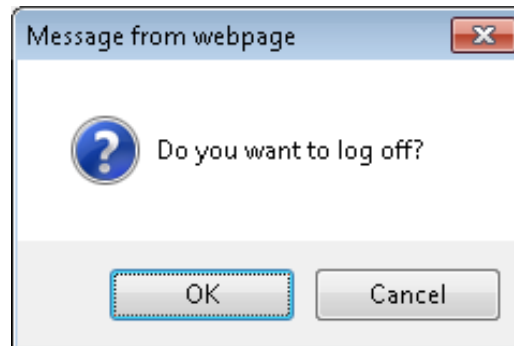
6.1.10 Logging Off the Web Interface

The procedure below describes how to log off the Web interface.

➤ To log off the Web interface:

1. On the toolbar, click the **Log Off**  icon; the following confirmation message box appears:

Figure 6-17: Log Off Confirmation Box




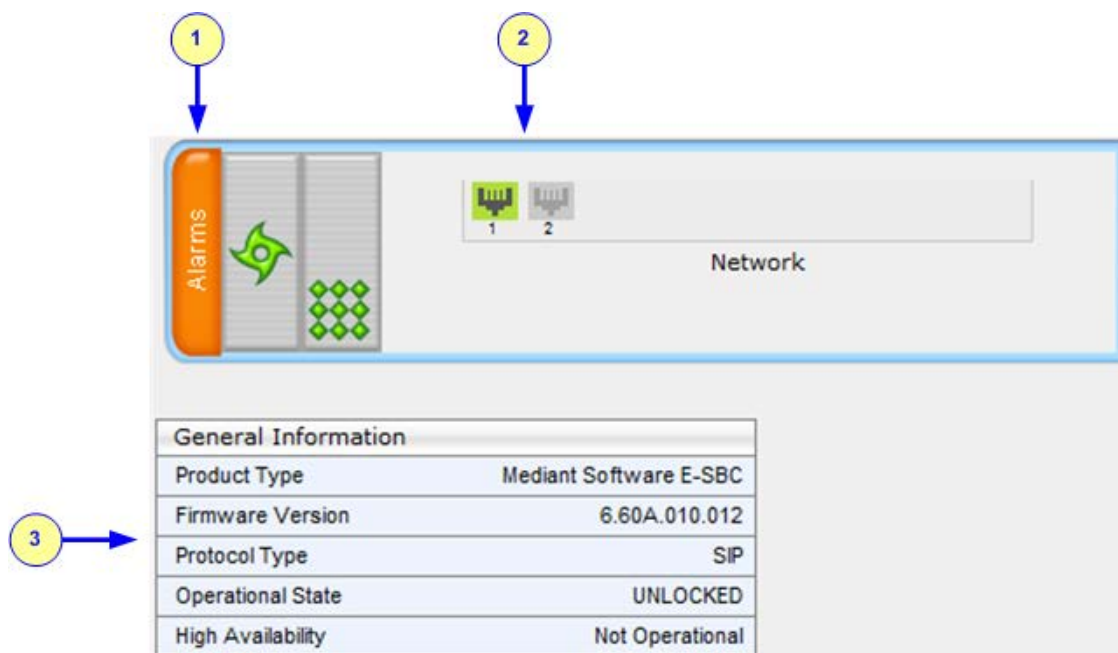
2. Click **OK**; you are logged off the Web session and the Web Login dialog box appears enabling you to re-login, if required.

6.2 Viewing the Home Page

The Home page is displayed when you access the device's Web interface. The Home page provides you with a graphical display of the device's front panel, showing color-coded status icons for various operations device.

➤ To access the Home page:

- On the toolbar, click the **Home**  icon.





In addition to the color-coded status information depicted on the graphical display of the device, the Home page displays various read-only information in the General Information pane:

- **IP Address:** IP address of the device
- **Subnet Mask:** Subnet mask address of the device
- **Default Gateway Address:** Default gateway used by the device
- **Firmware Version:** Software version running on the device
- **Protocol Type:** Signaling protocol currently used by the device (i.e. SIP)
- **Gateway Operational State:**
 - "LOCKED": device is locked (i.e. no new calls are accepted)
 - "UNLOCKED": device is not locked
 - "SHUTTING DOWN": device is currently shutting down

To perform these operations, see "Basic Maintenance" on page 305.

The table below describes the areas of the Home page.

Table 6-8: Home Page Description

Item #	Description
1	<p>Displays the highest severity of an active alarm raised (if any) by the device:</p> <ul style="list-style-type: none"> ■ Green = No alarms ■ Red = Critical alarm ■ Orange = Major alarm ■ Yellow = Minor alarm <p>To view active alarms, click this Alarms area to open the Active Alarms page (see Viewing Active Alarms on page 339).</p>
2	<p>Gigabit Ethernet port status icons:</p> <ul style="list-style-type: none"> ■  (green): Ethernet link is working ■  (gray): Ethernet link is not connected <p>To view detailed Ethernet port information, click these icons to open the Ethernet Port Information page (see Viewing Ethernet Port Information on page 338).</p>
3 & 4	Reserved for future use.
5	<p>General Information pane, displaying the following:</p> <ul style="list-style-type: none"> ■ Firmware Version: software version currently running on the device ■ Protocol Type: signaling protocol currently used by the device (i.e. SIP) ■ Gateway Operational State: operational state of the device: <ul style="list-style-type: none"> ✓ "LOCKED" - device is locked (i.e. no new calls are accepted) ✓ "UNLOCKED" - device is not locked ✓ "SHUTTING DOWN" - device is currently shutting down ■ High Availability: status of the device's HA mode: <ul style="list-style-type: none"> ✓ "Not Operational": HA is not configured or device not installed with HA Software License Key ✓ "Synchronizing": Redundant device synchronizing with Active device ✓ "Operational": Device is in HA mode ✓ "Stand Alone": HA is configured but Redundant device is missing and HA is currently unavailable ✓ "Not Available": HA is not configured correctly (error)

6.3 Configuring Web User Accounts

You can create up to 10 Web user accounts for the device. Up to five Web users can simultaneously be logged in to the device's Web interface. Web user accounts prevent unauthorized access to the Web interface, enabling login access only to users with correct credentials (i.e., username and password). Each Web user account is composed of the following attributes:

- **Username and password:** Credentials that enable authorized login access to the Web interface.
- **Access level (user type):** Access privileges specifying what the user can view in the Web interface and its read/write privileges. The table below describes the different types of Web user account access levels:

Table 6-9: Access Levels of Web User Accounts

User Access Level	Numeric Representation*	Privileges
Master	220	Read / write privileges for all pages. Can create all user types, including additional Master users and Security Administrators. It can delete all users except the last Security Administrator.
Security Administrator	200	Read / write privileges for all pages. It can create all user types and is the only one that can create the first Master user. Note: There must be at least one Security Administrator.
Administrator	100	Read / write privileges for all pages except security-related pages, which are read-only.
Monitor	50	No access to security-related and file-loading pages; read-only access to other pages.
No Access	0	No access to any page. Note: This access level is not applicable when using advanced Web user account configuration in the Web Users table.

* The numeric representation of the access level is used only to define accounts in a RADIUS server (the access level ranges from 1 to 255).

By default, the device is pre-configured with the following two Web user accounts:

Table 6-10: Pre-configured Web User Accounts

User Access Level	Username (Case-Sensitive)	Password (Case-Sensitive)
Security Administrator	Admin	Admin
Monitor	User	User

After you log in to the Web interface, the username is displayed on the toolbar.

If the Web session is idle (i.e., no actions are performed) for more than five minutes, the Web session expires and you are once again requested to login with your username and password. Users can be banned for a period of time upon a user-defined number of unsuccessful login attempts. Login information (such as how many login attempts were made and the last successful login time) can be presented to the user.

➤ **To prevent user access after a specific number of failed logins:**

1. From the 'Deny Access On Fail Count' drop-down list, select the number of failed logins after which the user is prevented access to the device for a user-defined time (see next step).
2. In the 'Deny Authentication Timer' field, enter the interval (in seconds) that the user needs to wait before a new login attempt from the same IP address can be done after reaching the number of failed login attempts (defined in the previous step).



Notes:

- For security, it's recommended that you change the default username and password.
- The Security Administrator user can change all attributes of all Web user accounts. Web users with access levels other than Security Administrator can change only their password and username.
- To restore the two Web user accounts to default settings (usernames and passwords), set the *ini* file parameter ResetWebPassword to 1.
- To log in to the Web interface with a different Web user, click the **Log off** button and then login with with a different username and password.
- You can set the entire Web interface to read-only (regardless of Web user access levels), by using the *ini* file parameter DisableWebConfig (see "Web and Telnet Parameters" on page 394).
- You can define additional Web user accounts using a RADIUS server.

6.3.1 Basic User Accounts Configuration

This section describes basic Web user account configuration. This is relevant only if the two default, pre-configured Web user accounts - Security Administrator ("Admin") and Monitor ("User") - are sufficient for your management scheme.

For the Security Administrator, you can change only the username and password; not its access level. For the Monitor user, you can change username and password as well as access level (Administrator, Monitor, or No Access).



Notes:

- The access level of the Security Administrator cannot be modified.
- The access level of the second user account can be modified only by the Security Administrator.
- The username and password can be a string of up to 19 characters. When you log in to the Web interface, the username and password string values are case-sensitive, according to your configuration.
- Up to two users can be logged in to the Web interface at the same time, and they can be of the same user.

➤ **To configure the two pre-configured Web user accounts:**

1. Open the Web User Accounts page (**Configuration** tab > **System** menu > **Web User Accounts**). If you are logged in as Security Administrator, both Web user accounts are displayed (as shown below). If you are logged in with the second user account, only the details of this user account are displayed.

Figure 6-18: WEB User Accounts Page (for Users with 'Security Administrator' Privileges)

Current Logged User: Admin		
▼ Account Data for User: Admin		
User Name	Admin	Change User Name
Access Level	Security Administrator	
▼ Fill in the following 3 fields to change the password		
Current Password		
New Password		
Confirm New Password		Change Password
▼ Account Data for User: User		
User Name	User	Change User Name
Access Level	User Monitor	Change Access Level
▼ Fill in the following 3 fields to change the password		
Current Password		
New Password		
Confirm New Password		Change Password
▼ Web Users Table		
Create Web Users Table	Create Table	

2. To change the username of an account:
 - a. In the 'User Name' field, enter the new user name.
 - b. Click **Change User Name**; if you are currently logged in to the Web interface with this account, the 'Web Login' dialog box appears.
 - c. Log in with your new user name.
3. To change the password of an account:
 - a. In the 'Current Password' field, enter the current password.
 - b. In the 'New Password' and 'Confirm New Password' fields, enter the new password.
 - c. Click **Change Password**; if you are currently logged in to the Web interface with this account, the 'Web Login' dialog box appears.
 - d. Log in with your new password.
4. To change the access level of the optional, second account:
 - a. Under the **Account Data for User: User** group, from the 'Access Level' drop-down list, select a new access level user.
 - b. Click **Change Access Level**; the new access level is applied immediately.

6.3.2 Advanced User Accounts Configuration

This section describes advanced Web user account configuration. This is relevant if you need the following management scheme:

- Enhanced security settings per Web user (e.g., limit session duration)
- More than two Web user accounts (up to 10 Web user accounts)
- Master users

This advanced Web user configuration is done in the Web Users table, which is initially accessed from the Web User Accounts page (see procedure below). Once this table is accessed, subsequent access immediately opens the Web Users table instead of the Web User Accounts page.



Notes:

- Only the Security Administrator user can **initially** access the Web Users table.
- Only Security Administrator and Master users can add, edit, or delete users.
- Admin users have read-only privileges in the Web Users table. Monitor users have no access to this page.
- If you delete a user who is currently in an active Web session, the user is immediately logged off by the device.
- All users can change their own passwords. This is done in the WEB Security Settings page (see "Configuring Web Security Settings" on page 53).
- To remove the Web Users table and revert to the Web User Accounts page with the pre-configured, default Web user accounts, set the ResetWebPassword *ini* file parameter to 1. This also deletes all other Web users.
- Once the Web Users table is accessed, Monitor users and Admin users can only change their passwords in the Web Security Settings page (see "Configuring Web Security Settings" on page 53). The new password must have at least four different characters than the previous password. (The Security Administrator users and Master users can change their passwords in the Web Users table and in the Web Security Settings page.)
- This table can only be configured using the Web interface.

➤ To add Web user accounts with advanced settings:

1. Open the Web Users Table page:
 - Upon initial access:
 - a. Open the Web User Accounts page (**Configuration** tab > **System** menu > **Web User Accounts**).
 - b. Under the **Web Users Table** group, click the **Create Table** button.
 - Subsequent access: **Configuration** tab > **System** menu > **Web User Accounts**.

The Web Users table appears, listing the two default, pre-configured Web use accounts - Security Administrator ("Admin") and Monitor ("User"):

Figure 6-19: Web Users Table Page

Index	Username	Password	Status	Password Age	Session Limit	Session Timeout	Block Duration	User Level
0	Admin	*	Valid	0	2	60	60	SecAdmin
1	User	*	Valid	0	2	60	60	Monitor

Page 1 of 1 View 1 - 2 of 2

- Click the **Add** button; the following dialog box is displayed:

Figure 6-20: Web Users Table - Add Record Dialog Box

Add Record

Index
0

Username

Password

Status
New

Password Age
90

Session Limit
2

Session Timeout
60

Block Duration
60

User Level
Monitor

Submit
Cancel

- Add a user as required. For a description of the parameters, see the table below.
- Click **Submit**.

Table 6-11: Web User Parameters Description

Parameter	Description
Web: Username	Defines the Web user's username. The valid value is a string of up to 40 alphanumeric characters, including the period ".", underscore "_", and hyphen "-" signs.
Web: Password	Defines the Web user's password. The valid value is a string of 8 to 40 ASCII characters, which must include the following: <ul style="list-style-type: none"> At least eight characters At least two letters that are upper case (e.g., "AA") At least two letters that are lower case (e.g., "aa") At least two numbers At least two signs (e.g., the dollar "\$" sign) No spaces in the string At least four characters different to the previous password

Parameter	Description
Web: Status	<p>Defines the status of the Web user.</p> <ul style="list-style-type: none"> ▪ New = (Default) User is required to change its password on the next login. When the user logs in to the Web interface, the user is immediately prompted to change the current password. ▪ Valid = User can log in to the Web interface as normal. ▪ Failed Access = This state is automatically set for users that exceed a user-defined number of failed login attempts, set by the 'Deny Access on Fail Count' parameter (see "Configuring Web Security Settings" on page 53). These users can log in only after a user-defined timeout configured by the 'Block Duration' parameter (see below) or if their status is changed (to New or Valid) by a System Administrator or Master. ▪ Old Account = This state is automatically set for users that have not accessed the Web interface for a user-defined number of days, set by the 'User Inactivity Timer' (see "Configuring Web Security Settings" on page 53). These users can only log in to the Web interface if their status is changed (to New or Valid) by a System Administrator or Master. <p>Notes:</p> <ul style="list-style-type: none"> ▪ The Old Account status is applicable only to Admin and Monitor users; System Administrator and Master users can be inactive indefinitely. ▪ For security, it is recommended to set the status of a newly added user to New in order to enforce password change.
Web: Password Age	<p>Defines the duration (in days) of the validity of the password. When this duration elapses, the user is prompted to change the password; otherwise, access to the Web interface is blocked.</p> <p>The valid value is 0 to 10000, where 0 means that the password is always valid. The default is 90.</p>
Web: Session Limit	<p>Defines the maximum number of Web interface sessions allowed for the user. In other words, this allows the same user account to log in to the device from different sources (i.e., IP addresses).</p> <p>The valid value is 0 to 5. The default is 2.</p> <p>Note: Up to 5 users can be logged in to the Web interface at any given.</p>
Web: Session Timeout	<p>Defines the duration (in minutes) of Web inactivity of a logged-in user, after which the user is automatically logged off the Web interface.</p> <p>The valid value is 0 to 100000. The default is according to the settings of the 'Session Timeout' global parameter (see "Configuring Web Security Settings" on page 53).</p>
Web: Block Duration	<p>Defines the duration (in seconds) for which the user is blocked when the user exceeds a user-defined number of failed login attempts. This is configured by the 'Deny Access On Fail Count' parameter (see "Configuring Web Security Settings" on page 53).</p> <p>The valid value is 0 to 100000, where 0 means that the user can do as many login failures without getting blocked. The default is according to the settings of the 'Deny Authentication Timer' parameter (see "Configuring Web Security Settings" on page 53).</p> <p>Note: The 'Deny Authentication Timer' parameter relates to failed Web logins from specific IP addresses.</p>

Parameter	Description
Web: User Level	<p>Defines the user's access level.</p> <ul style="list-style-type: none"> Monitor = (Default) Read-only user. This user can only view Web pages and access to security-related pages is denied. Admin = Read/write privileges for all pages, except security-related pages including the Web Users table where this user has only read-only privileges. SecAdmin = Read/write privileges for all pages. This user is the Security Administrator. Master-User = Read/write privileges for all pages. This user also functions as a security administrator. <p>Notes:</p> <ul style="list-style-type: none"> At least one Security Administrator must exist. The last remaining Security Administrator cannot be deleted. The first Master user can be added only by a Security Administrator user. Additional Master users can be added, edited and deleted only by Master users. If only one Master user exists, it can be deleted only by itself. Master users can add, edit, and delete Security Administrators (but cannot delete the last Security Administrator). Only Security Administrator and Master users can add, edit, and delete Admin and Monitor users.

6.4 Displaying Login Information upon Login

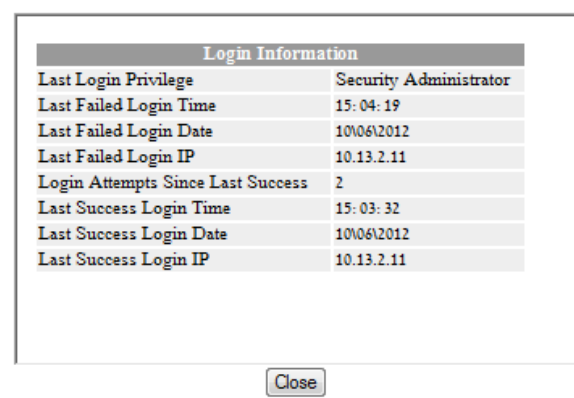
The device can display login information immediately upon Web login.

➤ **To enable display of user login information upon a successful login:**

1. Open the WEB Security Settings page (**Configuration** tab > **System** menu > **Management** submenu > **WEB Security Settings**).
2. From the 'Display Login Information' drop-down list, select **Yes**.
3. Click **Submit** to apply your changes.

Once enabled, the Login Information window is displayed upon a successful login, as shown in the example below:

Figure 6-21: Login Information Window



6.5 Configuring Web Security Settings

The WEB Security Settings page is used to define a secure Web access communication method. For a description of these parameters, see "Web and Telnet Parameters" on page 394.

➤ **To define Web access security:**

1. Open the WEB Security Settings page (**Configuration** tab > **System** menu > **Management** submenu > **WEB Security Settings**).

▼ General	
HTTP Authentication Mode	Web Based Authentication
Secured Web Connection (HTTPS)	HTTP and HTTPS
Requires Client Certificates for HTTPS connection	Disable
HTTPS Cipher String	RC4:EXP
▼ Session	
Session Timeout (minutes)	15
▼ Access Block Parameters	
Deny Authentication Timer	60
Deny Access On Fail Count	3
Display Login Information	No

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 308.

6.6 Web Login Authentication using Smart Cards

You can enable Web login authentication using certificates from a third-party, common access card (CAC) with user identification. When a user attempts to access the device through the Web browser (HTTPS), the device retrieves the Web user's login username (and other information, if required) from the CAC. The user attempting to access the device is only required to provide the login password. Typically, a TLS connection is established between the CAC and the device's Web interface, and a RADIUS server is implemented to authenticate the password with the username. Therefore, this feature implements a two-factor authentication - what the user has (i.e., the physical card) and what the user knows (i.e., the login password).

This feature is enabled using the EnableMgmtTwoFactorAuthentication parameter.



Note: For specific integration requirements for implementing a third-party smart card for Web login authentication, contact your AudioCodes representative.

➤ **To log in to the Web interface using CAC:**

1. Insert the Common Access Card into the card reader.
2. Access the device using the following URL: `https://<host name or IP address>`; the device prompts for a username and password.
3. Enter the password only. As some browsers require that the username be provided, it's recommended to enter the username with an arbitrary value.

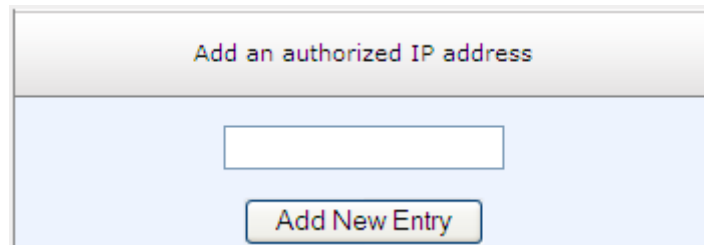
6.7 Configuring Web and Telnet Access List

The Web & Telnet Access List page is used to define IP addresses (up to ten) that are permitted to access the device's Web, Telnet, and SSH interfaces. Access from an undefined IP address is denied. If no IP addresses are defined, this security feature is inactive and the device can be accessed from any IP address. The Web and Telnet Access List can also be defined using the *ini* file parameter `WebAccessList_x` (see "Web and Telnet Parameters" on page 394).

➤ **To add authorized IP addresses for Web, Telnet, and SSH interfaces access:**

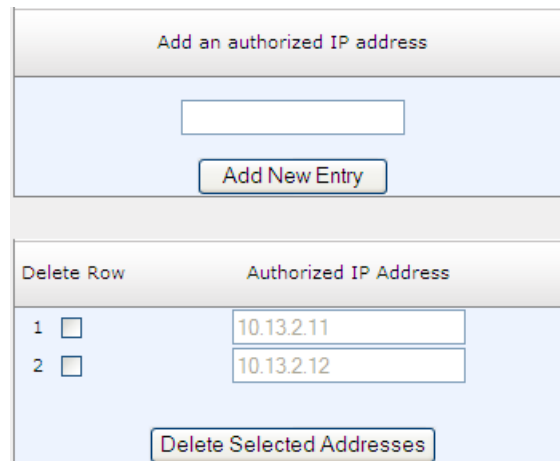
1. Open the Web & Telnet Access List page (**Configuration** tab > **System** menu > **Management** submenu > **Web & Telnet Access List**).

Figure 6-22: Web & Telnet Access List Page - Add New Entry



2. To add an authorized IP address, in the 'Add an authorized IP address' field, enter the required IP address, and then click **Add New Entry**; the IP address you entered is added as a new entry to the Web & Telnet Access List table.

Figure 6-23: Web & Telnet Access List Table



Delete Row	Authorized IP Address
1 <input type="checkbox"/>	10.13.2.11
2 <input type="checkbox"/>	10.13.2.12

3. To delete authorized IP addresses, select the Delete Row check boxes corresponding to the IP addresses that you want to delete, and then click **Delete Selected Addresses**; the IP addresses are removed from the table and these IP addresses can no longer access the Web and Telnet interfaces.
4. To save the changes to flash memory, see "Saving Configuration" on page 308.



Notes:

- The first authorized IP address in the list must be your PC's (terminal) IP address; otherwise, access from your PC is denied.
- Delete your PC's IP address last from the 'Web & Telnet Access List' page. If it is deleted before the last, subsequent access to the device from your PC is denied.

6.8 Configuring RADIUS Settings

The RADIUS Settings page is used for configuring the Remote Authentication Dial In User Service (RADIUS) accounting parameters. For a description of these parameters, see "Configuration Parameters Reference" on page 387.

➤ **To configure RADIUS:**

1. Open the RADIUS Settings page (**Configuration** tab > **System** menu > **Management** submenu > **RADIUS Settings**).

Figure 6-24: RADIUS Parameters Page

▼ General RADIUS Setting		
⚡ Enable RADIUS Access Control	Disable	▼
Use RADIUS for Web/Telnet Login	Disable	▼
⚡ RADIUS Authentication Server IP Address	0.0.0.0	
⚡ RADIUS Authentication Server Port	1645	
⚡ RADIUS Shared Secret	●●●●●●●●	
▼ General RADIUS Authentication		
Default Access Level	200	
⚡ Device Behavior Upon RADIUS Timeout	Verify Access Locally	▼
⚡ Local RADIUS Password Cache Mode	Reset Timer Upon Access	▼
Local RADIUS Password Cache Timeout [sec]	300	
RADIUS VSA Vendor ID	5003	
RADIUS VSA Access Level Attribute	35	

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 308.

Reader's Notes

7 CLI-Based Management

This section provides an overview of the CLI-based management and configuration relating to CLI management. The device's CLI-based management interface can be accessed using the RS-232 serial port or by using Secure SHell (SSH) or Telnet through the Ethernet interface.



Notes:

- For security, CLI is disabled by default.
- CLI is used only for debugging and mainly allows you to view various information regarding device configuration and performance.

7.1 Enabling CLI using Telnet

The device's CLI can be accessed using Telnet. Secure Telnet using Secure Socket Layer (SSL) can be configured whereby information is not transmitted in the clear. If SSL is used, a special Telnet client is required on your PC to connect to the Telnet interface over a secured connection; examples include C-Kermit for UNIX and Kermit-95 for Windows.

For security, some organizations require the display of a proprietary notice upon starting a Telnet session. You can use the configuration ini file parameter, WelcomeMessage to configure such a message (see Creating a Login Welcome Message on page 42).

➤ To enable Telnet:

1. Open the Telnet/SSH Settings page (**Configuration** tab > **System** menu > **Management** > **Telnet/SSH Settings**).

Figure 7-1: Telnet Settings on Telnet/SSH Settings Page

▼ Telnet Settings	
Embedded Telnet Server	Enable Unsecured ▼
Telnet Server TCP Port	23
⚡ Telnet Server Idle Timeout	0

2. Set the 'Embedded Telnet Server' parameter to **Enable Unsecured** or **Enable Secured** (i.e, SSL).
3. Configure the other Tenet parameters as required. For a description of these parameters, see Telnet Parameters on page 397.
4. Click **Submit**.
5. Save the changes to flash memory with a device reset.

7.2 Enabling CLI using SSH and RSA Public Key

The device's CLI can be accessed using Telnet. However, unless configured for TLS, Telnet is not secure as it requires passwords to be transmitted in clear text. To overcome this, Secure SHell (SSH) is used, which is the de-facto standard for secure CLI. SSH 2.0 is a protocol built above TCP, providing methods for key exchange, authentication, encryption, and authorization.

SSH requires appropriate client software for the management PC. Most Linux distributions have OpenSSH pre-installed; Windows-based PCs require an SSH client software such as PuTTY, which can be downloaded from <http://www.chiark.greenend.org.uk/~sgtatham/putty/>.

By default, SSH uses the same username and password as the Telnet and Web server. SSH supports 1024/2048-bit RSA public keys, providing carrier-grade security. Follow the instructions below to configure the device with an administrator RSA key as a means of strong authentication.

➤ **To enable SSH and configure RSA public keys for Windows (using PuTTY SSH):**

1. Start the PuTTY Key Generator program, and then do the following:
 - a. Under the 'Parameters' group, do the following:
 - ◆ Select the **SSH-2 RSA** option.
 - ◆ In the 'Number of bits in a generated key' field, enter "1024" bits.
 - b. Under the 'Actions' group, click **Generate** and then follow the on-screen instructions.
 - c. Under the 'Actions' group, click **Save private key** to save the new private key to a file (*.ppk) on your PC.
 - d. Under the 'Key' group, select the displayed encoded text between "ssh-rsa" and "rsa-key-....", as shown in the example below:

Figure 7-2: Selecting Public RSA Key in PuTTY



2. Open the Telnet/SSH Settings page (**Configuration** tab > **System** menu > **Management** > **Telnet/SSH Settings**), and then do the following:
 - a. Set the 'Enable SSH Server' parameter to **Enable**.
 - b. Paste the public key that you copied in Step 1.d into the 'Admin Key' field, as shown below:

Figure 7-3: SSH Settings - Pasting Public RSA Key in 'Admin Key' Field

SSH Settings	
Enable SSH Server	Enable
Server Port	22
Admin Key	AAAAB3NzaC1yc2EAAAABJQAAAIBh4d5kzHckyRm/3awrb2b/Cscd/d2FDolycGW/b qjDy3LI889hCtu/GE5ADw8u/6FPxm/7ehhUcMptE2NzqZnz7S2VrE3xEV/ch451nve n77J3kUclH3GdoTeb4G2UpP82ag+y0pnu4wluK/D6jk+m1ALMdmQNEyH5k6cww==
Require Public Key	Enable
Max Payload Size	32768
Max Binary Packet Size	35000
Enable Last Login Message	Enable
Max Login Attempts	3

- c. For additional security, you can set the 'Require Public Key' to **Enable**. This ensures that SSH access is only possible by using the RSA key and not by using user name and password.
 - d. Configure the other SSH parameters as required. For a description of these parameters, see SSH Parameters on page 413.
 - e. Click **Submit**.
3. Start the PuTTY Configuration program, and then do the following:
 - a. In the 'Category' tree, drill down to **Connection**, then **SSH**, and then **Auth**; the 'Options controlling SSH authentication' pane appears.
 - b. Under the 'Authentication parameters' group, click **Browse** and then locate the private key file that you created and saved in Step 4.
 4. Connect to the device with SSH using the username "Admin"; RSA key negotiation occurs automatically and no password is required.
- **To configure RSA public keys for Linux (using OpenSSH 4.3):**
1. Run the following command to create a new key in the admin.key file and to save the public portion to the admin.key.pub file:


```
ssh-keygen -f admin.key -N "" -b 1024
```
 2. Open the admin.key.pub file, and then copy the encoded string from "ssh-rsa" to the white space.
 3. Open the Telnet/SSH Settings page (**Configuration** tab > **System** menu > **Management** > **Telnet/SSH Settings**), and then paste the value copied in Step 2 into the 'Admin Key' field.
 4. Click **Submit**.
 5. Connect to the device with SSH, using the following command:


```
ssh -i admin.key xx.xx.xx.xx
```

where xx.xx.xx.xx is the device's IP address. RSA-key negotiation occurs automatically and no password is required.

7.3 Establishing a CLI Session

The procedure below describes how to establish a CLI session with the device.



Notes:

- The default login username and password are both "Admin" (case-sensitive).
- Only the primary User Account, which has Security Administration access level (200) can access the device using Telnet. For configuring the username and password, see Configuring Web User Accounts on page 46.

- **To establish a CLI session with the device:**
1. Establish a Telnet or SSH session with the device using its OAMP IP address.
 2. Log in to the session using the username and password assigned to the Admin user of the Web interface:
 3. At the Username prompt, type the username, and then press Enter:


```
Username: Admin
```
 4. At the Password prompt, type the password, and then press Enter:


```
Password: Admin
```


5. At the prompt, type the following, and then press Enter:

```
enable
```

6. At the prompt, type the password again, and then press Enter:

```
Password: Admin
```

7.4 CLI Commands

The CLI commands are used mainly to display current configuration and performance. These commands are organized in subdirectories. When the CLI session starts, you are located in the 'root' directory.

To access a subdirectory, type its name, and then press Enter. The CLI commands can be entered in an abbreviated format by typing only the letters shown in upper case (i.e., capital letters). For example, the **CHangePassWord** command can be entered by typing **chpw**. If you know the full path to a command inside one of the subdirectories, the short format can be used to run it directly. For example, the **PERformance** command in the **MGmt** subdirectory may be run directly by typing **/mg/perf**.

The following table summarizes the basic CLI commands:

Table 12: Basic CLI Commands

Purpose	Commands	Description
Help	h	Displays the help for a specific command, action, or parameter.
Navigation	cd	Enters another directory.
	cd root	Navigates to the root directory (/).
	..	Goes up one level.
	exit	Terminates the CLI session.

7.4.1 Status Commands

The following table summarizes the Show commands and their corresponding options.

Table 13: Show CLI Commands

Command	Short Format	Arguments	Description
SHow	sh	info dsp ip log	Displays operational data. <ul style="list-style-type: none"> info: Displays general device information tdm: Displays PSTN-related information dsp: Displays DSP resource information ip: Displays information about IP interfaces
SHow INFO	sh info	-	Displays device hardware information, versions, uptime, temperature reading, and the last reset reason.
SHow DSP	sh dsp	status perf	Displays status and version for each DSP device, along with overall performance statistics.

Command	Short Format	Arguments	Description
SHoW IP	sh ip	conf perf route	Displays IP interface status and configuration, along with performance statistics. Note: The display format may change according to the configuration.
SHoW LOG	sh log	[stop]	Displays (or stops displaying) Syslog messages in the CLI session.

Example:

```

/>sh info
Board type: gateway SDH, firmware version 6.60.000.020
Uptime: 0 days, 0 hours, 3 minutes, 54 seconds
Memory usage: 63%
Temperature reading: 39 C
Last reset reason:
Board was restarted due to issuing of a reset from Web interface
Reset Time : 7.1.2012 21.51.13

/>sh dsp status
DSP firmware: 491096AE8 Version:0660.03 Used=0 Free=480 Total=480
DSP device 0: Active Used=16 Free= 0 Total=16
DSP device 1: Active Used=16 Free= 0 Total=16
DSP device 2: Active Used=16 Free= 0 Total=16
DSP device 3: Active Used=16 Free= 0 Total=16
DSP device 4: Active Used=16 Free= 0 Total=16
DSP device 5: Active Used=16 Free= 0 Total=16
DSP device 6: Inactive
DSP device 7: Inactive
DSP device 8: Inactive
DSP device 9: Inactive
DSP device 10: Inactive
DSP device 11: Inactive
DSP device 12: Active Used=16 Free= 0 Total=16
DSP device 13: Active Used=16 Free= 0 Total=16
DSP device 14: Active Used=16 Free= 0 Total=16
DSP device 15: Active Used=16 Free= 0 Total=16
DSP device 16: Active Used=16 Free= 0 Total=16
DSP device 17: Active Used=16 Free= 0 Total=16
DSP device 18: Inactive
PSEC - DSP firmware: AC491IPSEC Version: 0660.03
CONFERENCE - DSP firmware: AC491256C Version: 0660.03

/>sh dsp perf
DSP Statistics (statistics for 968 seconds):
Active DSP resources: 480
Total DSP resources: 480
DSP usage %: 100

/>sh ip perf
Networking Statistics (statistics for 979 seconds):
IP KBytes TX: 25
IP KBytes RX: 330
IP KBytes TX per second: 0
IP KBytes RX per second: 1
IP Packets TX: 1171
IP Packets RX: 5273
IP Packets TX per second: 3
IP Packets RX per second: 12

```



```

Peak KByte/s TX in this interval: 18
Peak KByte/s RX in this interval: 4
Discarded packets: 186
DHCP requests sent: 0
IPSec Security Associations: 0
/>/mg/perf reset
Done.

/>sh ip perf
Networking Statistics (statistics for 2 seconds):
IP KBytes TX: 2
IP KBytes RX: 4
IP KBytes TX per second: 0
IP KBytes RX per second: 1
IP Packets TX: 24
IP Packets RX: 71
IP Packets TX per second: 3
IP Packets RX per second: 12
Peak KByte/s TX in this interval: 18
Peak KByte/s RX in this interval: 4
Discarded packets: 0
DHCP requests sent: 0
IPSec Security Associations: 0

/>sh ip conf
Interface   IP Address          Subnet Mask          Default Gateway
-----
OAM         10.4.64.13          55.255.0.0           10.4.0.1
Media       10.4.64.13          255.255.0.0          10.4.0.1
Control     10.4.64.13          255.255.0.0          10.4.0.1
MAC address: 00-90-8f-04-5c-e9

/>sh ip route
Destination      Mask                Gateway              Intf  Flags
-----
0.0.0.0          0.0.0.0            10.4.0.1             OAM  A  S
10.4.0.0         255.255.0.0        10.4.64.13           OAM  A  L
127.0.0.0        255.0.0.0          127.0.0.1            AR   S
127.0.0.1        255.255.255.255    127.0.0.1            A   L  H
Flag legend: A=Active R=Reject L=Local S=Static E=rEDirect
M=Multicast
               B=Broadcast H=Host I=Invalid
End of routing table, 4 entries displayed.

```

7.4.2 Ping Command

The Ping command is described in the following table:

Table 14: Ping Command

Command	Short Format	Arguments	Description
PING	ping	[-n count] [-l size] [-w timeout] [-p cos] ip-address	Sends ICMP echo request packets to a specified IP address. <ul style="list-style-type: none"> count: number of packets to send. size: payload size in each packet. timeout: time (in seconds) to wait for a reply to each packet. cos: Class-of-Service (as per 802.1p) to use.

Example:

```

/>ping 10.31.2.10
Ping process started for address 10.31.2.10. Process ID - 27.
Reply from 10.31.2.10: bytes=0 time<0ms
Reply from 10.31.2.10: bytes=0 time<0ms
Reply from 10.31.2.10: bytes=0 time<0ms
Reply from 10.31.2.10: bytes=0 time<0ms
Ping statistics for 10.31.2.10:
Packets:Sent = 4, Received = 4, Lost 0 (0% loss),
Approximate round trip times in milli-seconds:
Minimum = 0ms, Maximum = 0ms, Average = 0ms

```

7.4.3 Management Commands

The commands under the **MGmt** directory, described in the table below, display current performance values.

Table 15: CLI Management Command

Command	Short Format	Arguments	Description
/MGmt/PERformance	/mg/perf	basic control dsp net ds1 reset	Displays performance statistics. The <i>reset</i> argument clears all statistics to zero.

7.4.4 Configuration Commands

The commands under the **CONfiguration** directory query and modify the current device configuration. The following commands are available:

Table 16: Configuration CLI Commands

Command	Short Format	Arguments	Description
SetConfigParam IP	/conf/scp ip	ip-addr subnet def-gw	Sets the IP address, subnet mask, and default gateway address of the device (on-the-fly). Note: This command may cause disruption of service. The CLI session may disconnect since the device changes its IP address.
RestoreFactorySettings	/conf/rfs		Restores all parameters to factory settings.
SaveAndRestart	/conf/sar		Saves all current configurations to the non-volatile memory and resets the device.
ConfigFile	/conf/cf	view get set	Retrieves the full <i>ini</i> file from the device and allows loading a new <i>ini</i> file directly in the CLI session. Note: The argument <i>view</i> displays the file, page by page. The argument <i>get</i> displays the file without breaks.

7.4.5 LDAP Commands

The commands under the **IPNetworking\OpenLdap** directory allow you to perform various Lightweight Directory Access Protocol (LDAP) actions.

Table 17: LDAP Commands

Sub-Command	Arguments	Description
LdapSTatus	-	Displays the LDAP connection status.
LdapSearch	<search key> <attribute1> [<attribute 2> ...<attribute 5>]	Searches an LDAP server. The parameters enclosed by [] are optional.
LDapOpen	-	Opens a connection to the LDAP server using parameters provided in the configuration file.
LDapSetDebugmode	<mode>	Sets the LdapDebugLevelMode parameter. Possible levels 0-3.
LDapGetDebugmode	-	Gets the LdapDebugLevelMode parameter value

8 SNMP-Based Management

The device provides an embedded SNMP Agent to operate with a third-party SNMP Manager (e.g., element management system or EMS) for operation, administration, maintenance, and provisioning (OAMP) of the device. The SNMP Agent supports standard Management Information Base (MIBs) and proprietary MIBs, enabling a deeper probe into the interworking of the device. The SNMP Agent can also send unsolicited events (SNMP traps) towards the SNMP Manager. All supported MIB files are supplied to customers as part of the release.

This section provides configuration relating to SNMP management.



Note: For more information on SNMP support such as SNMP traps, refer to the *SNMP User's Guide*.

8.1 Configuring SNMP Community Strings

The SNMP Community String page allows you to configure up to five read-only and up to five read-write SNMP community strings and to configure the community string that is used for sending traps.

For detailed descriptions of the SNMP parameters, see "SNMP Parameters" on page 398.

➤ **To configure the SNMP community strings:**

1. Open the SNMP Community String page (**Configuration** tab > **System** menu > **Management** submenu > **SNMP** submenu > **SNMP Community String**).

Delete	Community String	Access Level
<input type="checkbox"/>		Read Only
<input type="checkbox"/>		Read Only
<input type="checkbox"/>		Read Only
<input type="checkbox"/>		Read Only
<input type="checkbox"/>		Read Only
<input type="checkbox"/>		Read / Write
<input type="checkbox"/>		Read / Write
<input type="checkbox"/>		Read / Write
<input type="checkbox"/>		Read / Write
<input type="checkbox"/>		Read / Write

Disable SNMP

Trap Community String

Trap Manager Host Name

2. Configure the SNMP community strings parameters according to the table below.
3. Click **Submit** to apply your changes.

4. To save the changes to flash memory, see "Saving Configuration" on page 308.

To delete a community string, select the **Delete** check box corresponding to the community string that you want to delete, and then click **Submit**.

Table 8-1: SNMP Community String Parameters Description

Parameter	Description
Community String	<ul style="list-style-type: none"> ▪ Read Only [SNMPReadOnlyCommunityString_x]: Up to five read-only community strings (up to 19 characters each). The default string is 'public'. ▪ Read / Write [SNMPReadWriteCommunityString_x]: Up to five read / write community strings (up to 19 characters each). The default string is 'private'.
Trap Community String [SNMPTrapCommunityString]	Community string used in traps (up to 19 characters). The default string is 'trapuser'.

8.2 Configuring SNMP Trap Destinations

The SNMP Trap Destinations page allows you to configure up to five SNMP trap managers. You can associate a trap destination with SNMPv2 users and specific SNMPv3 users. Associating a trap destination with SNMPv3 users sends encrypted and authenticated traps to the SNMPv3 destination. By default, traps are sent unencrypted using SNMPv2.

➤ To configure SNMP trap destinations:

1. Open the SNMP Trap Destinations page (**Configuration** tab > **System** menu > **Management** submenu > **SNMP** > **SNMP Trap Destinations**).

Figure 8-1: SNMP Trap Destinations Page

		IP Address	Trap Port	Trap User	Trap Enable
<input checked="" type="checkbox"/>	SNMP Manager 1	0.0.0.0	162	v2cParams ▼	Enable ▼
<input checked="" type="checkbox"/>	SNMP Manager 2	0.0.0.0	162	hq-snmpv3 ▼	Enable ▼
<input type="checkbox"/>	SNMP Manager 3	0.0.0.0	162	v2cParams ▼	Enable ▼
<input type="checkbox"/>	SNMP Manager 4	0.0.0.0	162	v2cParams ▼	Enable ▼
<input type="checkbox"/>	SNMP Manager 5	0.0.0.0	18	v2cParams ▼	Enable ▼

2. Configure the SNMP trap manager parameters according to the table below.
3. Select the check box corresponding to the SNMP Manager that you wish to enable.
4. Click **Submit** to apply your changes.



Note: Only row entries whose corresponding check boxes are selected are applied when clicking **Submit**; otherwise, settings revert to their defaults.

Table 8-2: SNMP Trap Destinations Parameters Description

Parameter	Description
Web: SNMP Manager [SNMPManagerIsUsed_x]	Enables the SNMP Manager to receive traps and checks the validity of the configured destination (IP address and port number). <ul style="list-style-type: none"> ▪ [0] (check box cleared) = (Default) Disables SNMP Manager ▪ [1] (check box selected) = Enables SNMP Manager
Web: IP Address [SNMPManagerTableIP_x]	Defines the IP address (in dotted-decimal notation, e.g., 108.10.1.255) of the remote host used as the SNMP Manager. The device sends SNMP traps to this IP address.
Trap Port [SNMPManagerTrapPort_x]	Defines the port number of the remote SNMP Manager. The device sends SNMP traps to this port. The valid value range is 100 to 4000. The default is 162.
Web: Trap User [SNMPManagerTrapUser]	Associates a trap user with the trap destination. This determines the trap format, authentication level, and encryption level. <ul style="list-style-type: none"> ▪ v2cParams (default) = SNMPv2 user community string ▪ SNMPv3 user configured in "Configuring SNMP V3 Users" on page 68
Trap Enable [SNMPManagerTrapSendingEnable_x]	Activates the sending of traps to the SNMP Manager. <ul style="list-style-type: none"> ▪ [0] Disable ▪ [1] Enable (Default)

8.3 Configuring SNMP Trusted Managers

The SNMP Trusted Managers page allows you to configure up to five SNMP Trusted Managers, based on IP addresses. By default, the SNMP agent accepts SNMP Get and Set requests from any IP address, as long as the correct community string is used in the request. Security can be enhanced by using Trusted Managers, which is an IP address from which the SNMP agent accepts and processes SNMP requests.



Notes: The SNMP Trusted Managers table can also be configured using the table ini file parameter, SNMPTrustedMgr_x (see "SNMP Parameters" on page 398).

➤ **To configure SNMP Trusted Managers:**

1. Open the SNMP Trusted Managers page (**Configuration** tab > **System** menu > **Management** submenu > **SNMP** submenu > **SNMP Trusted Managers**).

Figure 8-2: SNMP Trusted Managers

Delete	Trusted Managers IP Address	
<input type="checkbox"/>	SNMP Trusted Manager 1	<input type="text" value="0.0.0.0"/>
<input type="checkbox"/>	SNMP Trusted Manager 2	<input type="text" value="0.0.0.0"/>
<input type="checkbox"/>	SNMP Trusted Manager 3	<input type="text" value="0.0.0.0"/>
<input type="checkbox"/>	SNMP Trusted Manager 4	<input type="text" value="0.0.0.0"/>
<input type="checkbox"/>	SNMP Trusted Manager 5	<input type="text" value="0.0.0.0"/>

2. Select the check box corresponding to the SNMP Trusted Manager that you want to enable and for whom you want to define an IP address.
3. Define an IP address in dotted-decimal notation.
4. Click **Submit** to apply your changes.
5. To save the changes, see "Saving Configuration" on page 308.

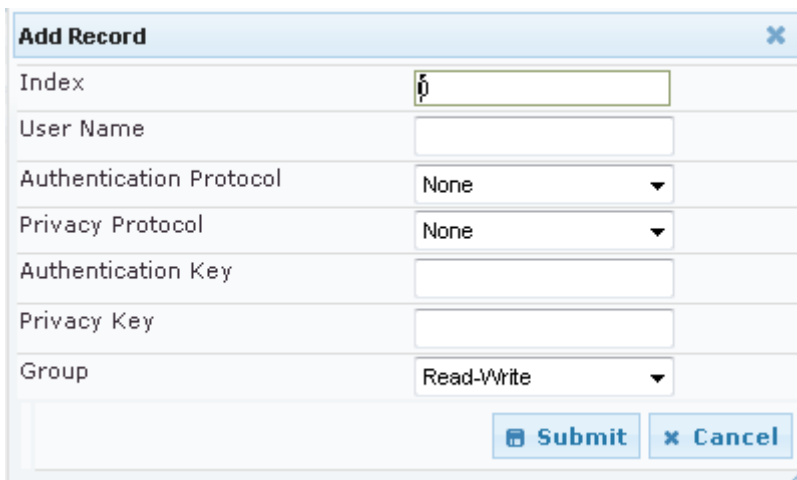
8.4 Configuring SNMP V3 Users

The SNMP v3 Users page allows you to configure authentication and privacy for up to 10 SNMP v3 users.

➤ **To configure SNMP v3 users:**

1. Open the SNMP v3 Users page (**Configuration** tab > **System** menu > **Management** submenu > **SNMP** submenu > **SNMP V3 Users**).
2. Click **Add**; the following dialog box appears:

Figure 8-3: SNMP V3 Setting Page - Add Record Dialog Box



The dialog box titled "Add Record" contains the following fields and controls:

- Index:** A text input field containing the value "5".
- User Name:** An empty text input field.
- Authentication Protocol:** A dropdown menu with "None" selected.
- Privacy Protocol:** A dropdown menu with "None" selected.
- Authentication Key:** An empty text input field.
- Privacy Key:** An empty text input field.
- Group:** A dropdown menu with "Read-Write" selected.
- Buttons:** "Submit" and "Cancel" buttons at the bottom right.

3. Configure the SNMP V3 Setting parameters according to the table below.
4. Click **Submit** to apply your settings.
5. To save the changes, see "Saving Configuration" on page 308.

**Notes:**

- If you delete a user that is associated with a trap destination (in "Configuring SNMP Trap Destinations" on page 66), the configured trap destination becomes disabled and the trap user reverts to default (i.e., SNMPv2).
- The SNMP v3 Users table can also be configured using the table ini file parameter, SNMPUsers (see "SNMP Parameters" on page 398).

Table 8-3: SNMP V3 Users Parameters

Parameter	Description
Index [SNMPUsers_Index]	The table index. The valid range is 0 to 9.
User Name [SNMPUsers_Username]	Name of the SNMP v3 user. This name must be unique.
Authentication Protocol [SNMPUsers_AuthProtocol]	Authentication protocol of the SNMP v3 user. <ul style="list-style-type: none"> ▪ [0] None (default) ▪ [1] MD5 ▪ [2] SHA-1
Privacy Protocol [SNMPUsers_PrivProtocol]	Privacy protocol of the SNMP v3 user. <ul style="list-style-type: none"> ▪ [0] None (default) ▪ [1] DES ▪ [2] 3DES ▪ [3] AES-128 ▪ [4] AES-192 ▪ [5] AES-256
Authentication Key [SNMPUsers_AuthKey]	Authentication key. Keys can be entered in the form of a text password or long hex string. Keys are always persisted as long hex strings and keys are localized.
Privacy Key [SNMPUsers_PrivKey]	Privacy key. Keys can be entered in the form of a text password or long hex string. Keys are always persisted as long hex strings and keys are localized.
Group [SNMPUsers_Group]	The group with which the SNMP v3 user is associated. <ul style="list-style-type: none"> ▪ [0] Read-Only (default) ▪ [1] Read-Write ▪ [2] Trap Note: All groups can be used to send traps.

Reader's Notes

9 INI File-Based Management

The device can be configured using an ini file, which is a text-based file with an *ini* file extension name that can be created using any standard text-based editor such as Notepad. Each configuration element of the device has a corresponding ini file parameter that you can use in the ini file for configuring the device. When you have created the ini file with your ini file parameter settings, you apply these settings to the device by installing (loading) the ini file to the device.

**Notes:**

- For a list and description of the *ini* file parameters, see "Configuration Parameters Reference" on page 387.
- To restore the device to default settings using the *ini* file, see "Restoring Factory Defaults" on page 327.

9.1 INI File Format

The *ini* file can be configured with any number of parameters. These *ini* file parameters can be one of the following types:

- Individual parameters - see "Configuring Individual ini File Parameters" on page 71
- Table parameters - see "Configuring Table ini File Parameters" on page 71

9.1.1 Configuring Individual ini File Parameters

The syntax for configuring individual *ini* file parameters in the ini file is as follows:

- An optional, subsection name (or group name) enclosed in square brackets "[...]". This is used to conveniently group similar parameters by their functionality.
- Parameter name, followed by an equal "=" sign and then its value.
- Comments must be preceded by a semicolon ";".

```
[subsection name]
parameter name = value
parameter name = value
; this is a comment line
; for example:
[System Parameters]
SyslogServerIP = 10.13.2.69
EnableSyslog = 1
```

For general *ini* file formatting rules, see "General ini File Formatting Rules" on page 73.

9.1.2 Configuring Table ini File Parameters

The table ini file parameters allow you to configure tables, which include multiple parameters (*columns*) and row entries (*indices*). When loading an *ini* file to the device, it's recommended to include only tables that belong to applications that are to be configured (dynamic tables of other applications are empty, but static tables are not).

The table ini file parameter is composed of the following elements:

- **Title of the table:** The name of the table in square brackets, e.g., [MY_TABLE_NAME].
- **Format line:** Specifies the columns of the table (by their string names) that are to be

configured.

- The first word of the Format line must be "FORMAT", followed by the Index field name and then an equal "=" sign. After the equal sign, the names of the columns are listed.
- Columns must be separated by a comma ",".
- The Format line must only include columns that can be modified (i.e., parameters that are not specified as read-only). An exception is Index fields, which are mandatory.
- The Format line must end with a semicolon ";".
- **Data line(s):** Contain the actual values of the columns (parameters). The values are interpreted according to the Format line.
 - The first word of the Data line must be the table's string name followed by the Index field.
 - Columns must be separated by a comma ",".
 - A Data line must end with a semicolon ";".
- **End-of-Table Mark:** Indicates the end of the table. The same string used for the table's title, preceded by a backslash "\", e.g., [MY_TABLE_NAME].

The following displays an example of the structure of a table ini file parameter.

```
[Table_Title]
; This is the title of the table.
FORMAT Index = Column_Name1, Column_Name2, Column_Name3;
; This is the Format line.
Index 0 = value1, value2, value3;
Index 1 = value1, $$, value3;
; These are the Data lines.
[\\Table_Title]
; This is the end-of-the-table-mark.
```

The table ini file parameter formatting rules are listed below:

- Indices (in both the Format and the Data lines) must appear in the same order. The Index field must never be omitted.
- The Format line can include a subset of the configurable fields in a table. In this case, all other fields are assigned with the pre-defined default values for each configured line.
- The order of the fields in the Format line isn't significant (as opposed to the Index fields). The fields in the Data lines are interpreted according to the order specified in the Format line.
- The double dollar sign (\$\$) in a Data line indicates the default value for the parameter.
- The order of the Data lines is insignificant.
- Data lines must match the Format line, i.e., it must contain exactly the same number of Indices and Data fields and must be in exactly the same order.
- A row in a table is identified by its table name and Index field. Each such row may appear only once in the *ini* file.
- Table dependencies: Certain tables may depend on other tables. For example, one table may include a field that specifies an entry in another table. This method is used to specify additional attributes of an entity, or to specify that a given entity is part of a larger entity. The tables must appear in the order of their dependency (i.e., if Table X is referred to by Table Y, Table X must appear in the *ini* file before Table Y).

For general *ini* file formatting rules, see "General ini File Formatting Rules" on page 73.

The table below displays an example of a table ini file parameter:

```
[ CodersGroup0 ]
FORMAT CodersGroup0_Index = CodersGroup0_Name, CodersGroup0_pTime,
CodersGroup0_rate, CodersGroup0_PayloadType, CodersGroup0_Sce;
```



```
CodersGroup0 0 = g711Alaw64k, 20, 0, 255, 0;  
CodersGroup0 1 = eg711Ulaw, 10, 0, 71, 0;  
[ \CodersGroup0 ]
```



Note: Do not include read-only parameters in the table ini file parameter as this can cause an error when attempting to load the file to the device.

9.1.3 General ini File Formatting Rules

The *ini* file must adhere to the following formatting rules:

- The *ini* file name must not include hyphens "-" or spaces; if necessary, use an underscore "_" instead.
- Lines beginning with a semi-colon ";" are ignored. These can be used for adding remarks in the *ini* file.
- A carriage return (i.e., Enter) must be done at the end of each line.
- The number of spaces before and after the equals sign "=" is irrelevant.
- Subsection names for grouping parameters are optional.
- If there is a syntax error in the parameter name, the value is ignored.
- Syntax errors in the parameter's value can cause unexpected errors (parameters may be set to the incorrect values).
- Parameter string values that denote file names (e.g., CallProgressTonesFileName) must be enclosed with inverted commas, e.g., CallProgressTonesFileName = 'cpt_usa.dat'.
- The parameter name is not case-sensitive.
- The parameter value is not case-sensitive, except for coder names.
- The *ini* file must end with at least one carriage return.

9.2 Loading an ini File

You can load an *ini* file to the device using the following methods:

- Web interface, using any of the following pages:
 - Configuration File - see "Backing Up and Loading Configuration File" on page [324](#)
 - Load Auxiliary Files - see "Loading Auxiliary Files" on page [311](#)

When loaded to the device, the configuration settings of the *ini* file are saved to the device's non-volatile memory. If a parameter is not included in the loaded *ini* file, the following occurs:

- Using the Load Auxiliary Files page: Current settings for parameters that were not included in the loaded ini file are retained.
- All other methods: The default is assigned to the parameters that were not included in the loaded ini file and thereby, overriding values previously configured for these parameters.


Notes:

- For a list and description of the *ini* file parameters, see "Configuration Parameters Reference" on page 387.
- Some parameters are configurable only through the *ini* file (and not the Web interface).
- To restore the device to default settings using the *ini* file, see "Restoring Factory Defaults" on page 327.

9.3 Modifying an ini File

You can modify an *ini* file currently used by the device. Modifying an *ini* file instead of loading an entirely new *ini* file preserves the device's current configuration.

➤ **To modify an *ini* file:**

1. Save the device's configuration as an *ini* file on your computer, using the Web interface (see "Loading an ini File" on page 73).
2. Open the *ini* file using a text file editor such as Notepad, and then modify the *ini* file parameters as required.
3. Save the modified *ini* file, and then close the file.
4. Load the modified *ini* file to the device (see "Loading an ini File" on page 73).



Tip: Before loading the *ini* file to the device, verify that the file extension of the file is *.ini*.

9.4 Secured Encoded ini File

The *ini* file contains sensitive information that is required for the functioning of the device. The file may be loaded to the device using HTTP. These protocols are not secure and are vulnerable to potential hackers. To overcome this security threat, the AudioCodes DConvert utility allows you to binary-encode (encrypt) the *ini* file before loading it to the device. For more information, refer to *DConvert Utility User's Guide*.


Notes:

- The procedure for loading an encoded *ini* file is identical to the procedure for loading an unencoded *ini* file (see "Loading an ini File" on page 73).
- If you download from the device (to a folder on your computer) an *ini* file that was loaded encoded to the device, the file is saved as a regular *ini* file (i.e., unencoded).

Part III

General System Settings

10 Configuring Certificates

The Certificates page allows you to configure X.509 certificates, which are used for secure management of the device, secure SIP transactions, and other security applications.



Note: The device is shipped with an active TLS setup. Thus, configure certificates only if required.

10.1 Replacing the Device's Certificate

The device is supplied with a working TLS configuration consisting of a unique self-signed server certificate. If an organizational Public Key Infrastructure (PKI) is used, you may wish to replace this certificate with one provided by your security administrator.

➤ **To replace the device's certificate:**

1. Your network administrator should allocate a unique DNS name for the device (e.g., dns_name.corp.customer.com). This DNS name is used to access the device and therefore, must be listed in the server certificate.
2. If the device is operating in HTTPS mode, then set the 'Secured Web Connection (HTTPS)' parameter (HTTPSOnly) to **HTTP and HTTPS** (see "Configuring Web Security Settings" on page 53). This ensures that you have a method for accessing the device in case the new certificate does not work. Restore the previous setting after testing the configuration.
3. Open the Certificates page (**Configuration** tab > **System** menu > **Certificates**).
4. Under the **Certificate Signing Request** group, do the following:
 - a. In the 'Subject Name [CN]' field, enter the DNS name.
 - b. Fill in the rest of the request fields according to your security provider's instructions.
 - c. Click the **Create CSR** button; a textual certificate signing request is displayed in the area below the button:

Figure 10-1: Certificate Signing Request Group

▼ Certificate Signing Request

Subject Name [CN]	audio.com
Organizational Unit [OU] (optional)	Headquarters
Company name [O] (optional)	Corporate
Locality or city name [L] (optional)	Poughkeepsie
State [ST] (optional)	New York
Country code [C] (optional)	US

Create CSR

After creating the CSR, copy the text below (including the BEGIN/END lines) and send it to your Certification Authority for signing.

```

-----BEGIN CERTIFICATE REQUEST-----
MIIBtjCCAR8CAQAwZjESMBAGA1UEAxMJVXVkaW8uY29tMRUwEwYDVQQLEwxiZWZk
cXVhcnRlcnMxZjAQBGNVBAOTCUNVcnEvcnF0ZTEVMBMGA1UEBxMMUG91Z2hrZWVw
c2llMREwDwYDVQQIEWhozXcgWW9yazELMAkGA1UEBhMCVVMwZ8wDQYJKoZIhvcN
AQEBBQADgY0AMIGJAoGBAPhpF2t4OLy3FRk5Bw7FLZFWCXQ7nvuocHtu7Nns071M
xL7Of8YoL63eeIK2eDo8nm6rJ0677z/AHWJmF65pAK1CboIPgoZNS0g6+5JAmJAA
1LNUnoqjEsK7CF32uvolH//gFkhy5z1eNvObI+25Fn38aJzEXc8DkGw219rROQRZ
AgMBAAGgADANBgkqhkiG9w0BAQQFAAOBgQDihdqbclzkHdLFr+5BRuScKyguXBM6
q7FGjFXAfzK1MngnBMc/Myf8GTbawrQF7p6dNj60DivmuCPf6Gzz5m2uqc6Lqoi
nLnQpVCmbdva/B1QyEpPbqh2qpULJ8CSeSrrY3ru23AZeDuByyho90IKrbAp//+3
ZvnZze5M5CBSLg==
-----END CERTIFICATE REQUEST-----
  
```


- Copy the text and send it to your security provider. The security provider, also known as Certification Authority or CA, signs this request and then sends you a server certificate for the device.
- Save the certificate to a file (e.g., cert.txt). Ensure that the file is a plain-text file containing the "BEGIN CERTIFICATE" header, as shown in the example of a Base64-Encoded X.509 Certificate below:

-----BEGIN CERTIFICATE-----

MIIDkzCCAnugAwIBAgIEAgAAADANBgkqhkiG9w0BAQQFADA/MQswCQYDVQQGEwJGUJETMBEGA1UEChMKQ2VydG1wb3N0ZTEbMBkGA1UEAxMSQ2VydG1wb3N0ZSBTZXJ2ZXV5MB4XDTEkMDYyNDA4MDAwMFoXDTEkMDYyNDA4MDAwMFowPzELMAkGA1UEBhMCRCR1IxEzARBgNVBAoTckN1cnRpcG9zdGUxGzAZBgNVBAMTEkN1cnRpcG9zdGUgU2VydMVLcjcCASEwDQYJKoZIhvcNAQEBBQADggEoADCCAQkCggEAPqd4Mzir4spWldGRx8bQrhZkonWnNm`+Yhb7+4Q67ecf1janH7GcN/SXsfx7jJpreWULf7v7Cvpr4R7qIJcmdHIntmf7JPM5n6cDBv17uSW63er7NkVnMFHwK1QaGFLMybFkzaeGrvFm4k3lRefiXDmuOe+FhJgHYezYHf44LvPRPwhSrzi9+Aq3o8pWDguJuzDIUP1F1jMa+LPwvREXfFcUW+w==

-----END CERTIFICATE-----

7. Scroll down to the **Upload certificates files from your computer** group, click the **Browse** button corresponding to the 'Send Device Certificate...' field, navigate to the cert.txt file, and then click **Send File**.
8. After the certificate successfully loads to the device, save the configuration with a device reset (see "Saving Configuration" on page 308); the Web interface uses the provided certificate.
9. Open the Certificates page again and verify that under the **Certificate information** group (at the top of the page), the 'Private key' read-only field displays "OK"; otherwise, consult your security administrator:

Figure 10-2: Private key "OK" in Certificate Information Group

▼ Certificate information	
Certificate subject:	/CN=ACL_3845462
Certificate issuer:	/CN=ACL_3845462
Time to expiration:	7261 days
Key size:	1024 bits
Private key:	OK

10. If the device was originally operating in HTTPS mode and you disabled it in Step 2, then return it to HTTPS by setting the 'Secured Web Connection (HTTPS)' parameter to **HTTPS Only**, and then reset the device with a flash burn.



Notes:

- The certificate replacement process can be repeated when necessary (e.g., the new certificate expires).
- It is possible to use the IP address of the device (e.g., 10.3.3.1) instead of a qualified DNS name in the Subject Name. This is not recommended since the IP address is subject to change and may not uniquely identify the device.
- The device certificate can also be loaded via the Automatic Update Facility by using the HTTPSCertFileName *ini* file parameter.

10.2 Loading a Private Key

The device is shipped with a self-generated random private key, which cannot be extracted from the device. However, some security administrators require that the private key be generated externally at a secure facility and then loaded to the device through configuration. Since private keys are sensitive security parameters, take precautions to load them over a physically-secure connection such as a back-to-back Ethernet cable connected directly to the managing computer.

➤ **To replace the device's private key:**

1. Your security administrator should provide you with a private key in either textual PEM (PKCS #7) or PFX (PKCS #12) format. The file may be encrypted with a short pass-phrase, which should be provided by your security administrator.
2. If the device is operating in HTTPS mode, then set the 'Secured Web Connection (HTTPS)' field (HTTPSONly) to **HTTP and HTTPS** (see "Configuring Web Security Settings" on page 53). This ensures that you have a method for accessing the device in case the new configuration does not work. Restore the previous setting after testing the configuration.
3. Open the Certificates page (**Configuration** tab > **System** menu > **Certificates**) and scroll down to the **Upload certificate files from your computer** group.

Figure 10-3: Upload Certificate Files from your Computer Group

4. Fill in the 'Private key pass-phrase' field, if required.
5. Click the **Browse** button corresponding to the 'Send Private Key' field, navigate to the key file, and then click **Send File**.
6. If the security administrator has provided you with a device certificate file, load it using the 'Send Device Certificate' field.
7. After the files successfully load to the device, save the configuration with a device reset (see "Saving Configuration" on page 308); the Web interface uses the new configuration.
8. Open the Certificates page again, and verify that under the **Certificate information** group (at the top of the page) the 'Private key' read-only field displays "OK"; otherwise, consult your security administrator.
9. If the device was originally operating in HTTPS mode and you disabled it in Step 2, then enable it by setting the 'Secured Web Connection (HTTPS)' field to **HTTPS Only**.

10.3 Mutual TLS Authentication

By default, servers using TLS provide one-way authentication. The client is certain that the identity of the server is authentic. When an organizational PKI is used, two-way authentication may be desired - both client and server should be authenticated using X.509 certificates. This is achieved by installing a client certificate on the managing PC and loading the root CA's certificate to the device's Trusted Root Certificate Store. The Trusted Root Certificate file may contain more than one CA certificate combined, using a text editor.

Since X.509 certificates have an expiration date and time, the device must be configured to use NTP (see "Simple Network Time Protocol Support" on page 83) to obtain the current date and time. Without the correct date and time, client certificates cannot work.

➤ To enable mutual TLS authentication for HTTPS:

1. Set the 'Secured Web Connection (HTTPS)' field to **HTTPS Only** (see "Configuring Web Security Settings" on page 53) to ensure you have a method for accessing the device in case the client certificate does not work. Restore the previous setting after testing the configuration.
2. Open the Certificates page (see "Replacing the Device's Certificate" on page 77).
3. In the **Upload certificate files from your computer** group, click the **Browse** button corresponding to the 'Send Trusted Root Certificate Store ...' field, navigate to the file, and then click **Send File**.
4. When the operation is complete, set the 'Requires Client Certificates for HTTPS connection' field to **Enable** (see "Configuring Web Security Settings" on page 53).
5. Save the configuration with a device reset (see "Saving Configuration" on page 308).

When a user connects to the secured Web interface of the device:

- If the user has a client certificate from a CA that is listed in the Trusted Root Certificate file, the connection is accepted and the user is prompted for the system password.
- If both the CA certificate and the client certificate appear in the Trusted Root Certificate file, the user is not prompted for a password (thus, providing a single-sign-on experience - the authentication is performed using the X.509 digital signature).
- If the user does not have a client certificate from a listed CA or does not have a client certificate, the connection is rejected.



Notes:

- The process of installing a client certificate on your PC is beyond the scope of this document. For more information, refer to your operating system documentation, and/or consult your security administrator.
- The root certificate can also be loaded via the Automatic Update facility, using the HTTPSRootFileName *ini* file parameter.
- You can enable the device to check whether a peer's certificate has been revoked by an Online Certificate Status Protocol (OCSP) server (see Configuring Certificate Revocation Checking (OCSP) on page 81).

10.4 Configuring Certificate Revocation Checking (OCSP)

Some Public-Key Infrastructures (PKI) can revoke a certificate after it has been issued. You can configure the device to check whether a peer's certificate has been revoked, using the Online Certificate Status Protocol (OCSP). When OCSP is enabled, the device queries the OCSP server for revocation information whenever a peer certificate is received (IPSec, TLS client mode, or TLS server mode with mutual authentication).

➤ **To configure OCSP:**

1. Open the General Security Settings page (**Configuration** tab > **VoIP** menu > **Security** > **General Security Settings**).

Figure 10-4: OCSP Parameters

OCSP Settings	
Enable OCSP Server	Enable
Primary Server IP	212.10.5.6
Secondary Server IP	0.0.0.0
Server Port	2560
Default Response When Server Unreachable	Reject

2. Configure the OCSP parameters as required. For a description of these parameters, see OCSP Parameters on page 414.
3. Click **Submit**.



Notes:

- The device does not query OCSP for its own certificate.
- Some PKIs do not support OCSP but generate Certificate Revocation Lists (CRLs). For such cases, set up an OCSP server such as OCSPD.

10.5 Self-Signed Certificates

The device is shipped with an operational, self-signed server certificate. The subject name for this default certificate is 'ACL_nnnnnnn', where *nnnnnnn* denotes the serial number of the device. However, this subject name may not be appropriate for production and can be changed while still using self-signed certificates.

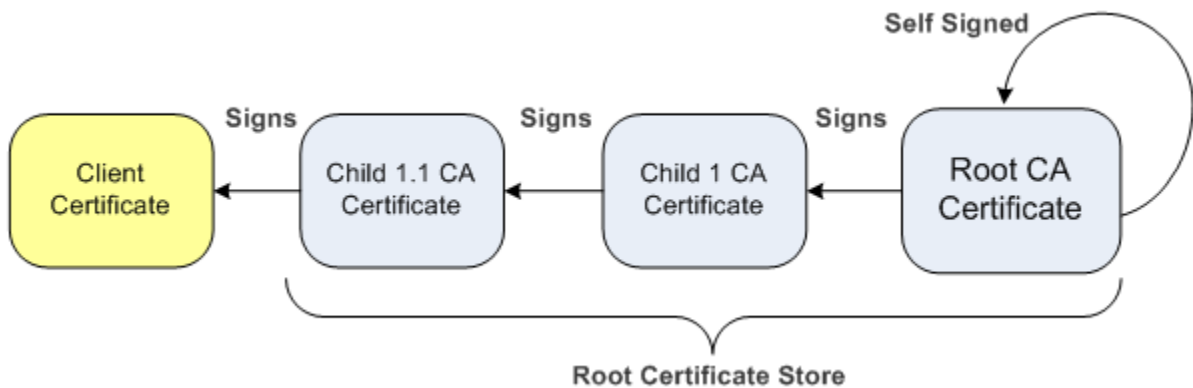
➤ **To change the subject name and regenerate the self-signed certificate:**

1. Before you begin, ensure the following:
 - You have a unique DNS name for the device (e.g., dns_name.corp.customer.com). This name is used to access the device and should therefore, be listed in the server certificate.
 - No traffic is running on the device. The certificate generation process is disruptive to traffic and should be executed during maintenance time.
2. Open the Certificates page (see "Replacing the Device's Certificate" on page 77).
3. In the 'Subject Name [CN]' field, enter the fully-qualified DNS name (FQDN) as the certificate subject, select the desired private key size (in bits), and then click **Generate self-signed**; after a few seconds, a message appears displaying the new subject name.
4. Save the configuration with a device reset (see "Saving Configuration" on page 308) for the new certificate to take effect.

10.6 Loading Certificate Chain for Trusted Root

A certificate chain is a sequence of certificates where each certificate in the chain is signed by the subsequent certificate. The last certificate in the list of certificates is the Root CA certificate, which is self-signed. The purpose of a certificate chain is to establish a chain of trust from a child certificate to the trusted root CA certificate. The CA vouches for the identity of the child certificate by signing it. A client certificate is considered trusted if one of the CA certificates up the certificate chain is found in the server certificate directory.

Figure 10-5: Certificate Chain Hierarchy



For the device to trust a whole chain of certificates, you need to combine the certificates into one text file (using a text editor). Once done, upload the file using the 'Trusted Root Certificate Store' field in the Certificates page.



Note: The maximum supported size of the combined file of trusted chain of certificates is 100,000 bytes (including the certificate's headers).

11 Date and Time

The date and time of the device can be configured manually or it can be obtained automatically from a Simple Network Time Protocol (SNTP) server.

11.1 Configuring Date and Time Manually

The date and time of the device can be configured manually.

➤ **To manually configure the device's date and time, using the Web interface:**

1. Open the Regional Settings page (**Configuration** tab > **System** menu > **Regional Settings**).

Figure 11-1: Regional Settings Page

Year	Month	Day	Hour	Minutes	Seconds
2010	2	4	10	21	46

2. Enter the current date and time of the geographical location in which the device is installed.
3. Click the **Submit** button.



Notes:

- If the device is configured to obtain the date and time from an SNTP server, the fields on this page are read-only, displaying the received date and time.
- After performing a hardware reset, the date and time are returned to their defaults and thus, should be updated.

11.2 Automatic Date and Time through SNTP Server

The Simple Network Time Protocol (SNTP) client functionality generates requests and reacts to the resulting responses using the NTP version 3 protocol definitions (according to RFC 1305). Through these requests and responses, the NTP client synchronizes the system time to a time source within the network, thereby eliminating any potential issues should the local system clock 'drift' during operation. By synchronizing time to a network time source, traffic handling, maintenance, and debugging become simplified for the network administrator.

The NTP client follows a simple process in managing system time: the NTP client requests an NTP update, receives an NTP response, and then updates the local system clock based on a configured NTP server within the network.

The client requests a time update from a specified NTP server at a specified update interval. In most situations, this update interval is every 24 hours based on when the system was restarted. The NTP server identity (as an IP address or FQDN) and the update interval are user-defined, or an SNMP MIB object.

When the client receives a response to its request from the identified NTP server, it must be interpreted based on time zone or location offset that the system is to a standard point of reference called the Universal Time Coordinate (UTC). The time offset that the NTP client uses is configurable.

If required, the clock update is performed by the client as the final step of the update process. The update is performed in such a way as to be transparent to the end users. For instance, the response of the server may indicate that the clock is running too fast on the client. The client slowly robs bits from the clock counter to update the clock to the correct

time. If the clock is running too slow, then in an effort to catch the clock up, bits are added to the counter, causing the clock to update quicker and catch up to the correct time. The advantage of this method is that it does not introduce any disparity in the system time that is noticeable to an end user or that could corrupt call timeouts and timestamps.

The procedure below describes how to configure SNTP.

➤ **To configure SNTP using the Web interface:**

1. Open the Application Settings page (**Configuration** tab > **System** menu > **Application Settings**).

Figure 11-2: SNTP Configuration in Application Settings Page

NTP Settings			
NTP Server DN/IP	212.13.4.5		
NTP UTC Offset	Hours: 0	Minutes: 0	
NTP Updated Interval	Hours: 24	Minutes: 0	
NTP Secondary Server IP			

Day Light Saving Time			
Day Light Saving Time	Enable		
DST Mode	Day of month		
Start Time	Sep	02	0 : 0
End Time	Apr	07	0 : 0
Offset [min]	60		
Day of Month Start	Sep	Sunday	First 0 : 0
Day of Month End	Apr	Sunday	First 0 : 0

2. Configure the NTP parameters:
 - 'NTP Server DN/IP' (NTPServerIP) - defines the IP address or FQDN of the NTP server.
 - 'NTP UTC Offset' (NTPServerUTCOffset) - defines the time offset in relation to the UTC. For example, if your region is 2 hours ahead of the UTC, enter "2".
 - 'NTP Updated Interval' (NTPUpdateInterval) - defines the period after which the date and time of the device is updated.
 - 'NTP Secondary Server IP' (NTPSecondaryServerIP) - defines the secondary NTP server.
3. Configure daylight saving, if required:
 - 'Day Light Saving Time' (DayLightSavingTimeEnable) - enables daylight saving time.
 - 'DST Mode' - Determines the range type for configuring the start and end date for daylight saving:
 - ◆ **Day of Year:** The range is configured by date of month, for example, from January 4 to August 31.
 - ◆ **Day of month:** The range is configured by day of month, for example, from the second Sunday of May January to the last Sunday of August.
 - 'Start Time' (DayLightSavingTimeStart) and 'End Time' (DayLightSavingTimeEnd) - defines the period for which daylight saving time is relevant.
 - 'Offset' (DayLightSavingTimeOffset) - defines the offset in minutes to add to the time for daylight saving. For example, if your region has daylight saving of one hour, the time received from the NTP server is 11:00, and the UTC offset for your region is +2 (i.e., 13:00), you need to enter "60" to change the local time to 14:00.
4. Verify that the device is set to the correct date and time. You can do this by viewing the date and time in the Regional Settings page, as described in "Configuring Date and Time Manually" on page 83.

Part IV

General VoIP Configuration

12 Network

This section describes the network-related configuration.

12.1 Configuring Physical Ethernet Ports

The device's physical Ethernet ports are grouped into pairs (termed *Group Members*), where each group consists of an active port and a standby port. This provides Ethernet port redundancy within a group, whereby if an active port is disconnected the device switches over to the standby port. These port groups can be assigned to IP network interfaces in the Multiple Interface table (see "Configuring IP Network Interfaces" on page 90). This enables physical separation of network interfaces, providing a higher level of segregation of sub-networks. Equipment connected to different physical ports is not accessible to one another. The only connection between them can be established by cross connecting them with media streams (a VoIP calls).

For each Ethernet port, you can configure the speed, duplex mode, native VLAN (PVID), and provide a brief description. Up to two port-pair redundancy groups are supported or up to four port groups where each group is assigned only one port is supported (a combination of port-pair redundancy groups and single-port groups can be configured).



Notes:

- To configure the transmit (Tx) and receive (Rx) settings of each port group and to assign ports to port groups, see "Configuring Tx/Rx for Ethernet Port-Pair Groups" on page 88.
- The Ethernet ports can also be configured using the table ini file parameter, PhysicalPortsTable.

➤ **To configure the physical Ethernet ports:**

1. Open the Physical Ports Settings page (**Configuration** tab > **VoIP** menu > **Network** submenu > **Physical Ports Settings**).

Index	Port	Mode	Native Vlan	Speed&Duplex	Description	Group Member	Group Status
1	GE_1	Enable	1	Auto Negotiation	User Port #0	GROUP_1	Active
2	GE_2	Enable	1	Auto Negotiation	User Port #1	GROUP_2	Active

2. Select the 'Index' radio button corresponding to the port that you want to configure.
3. Click the **Edit** button.
4. Configure the ports (see the table below for a description of the parameters).
5. Click **Apply**.

Table 12-1: Physical Port Settings Parameters Description

Parameter	Description
Port [PhysicalPortsTable_Port]	(Read-only) Displays the port number. The string values displayed on the Web page represent the physical ports, as shown below:
Mode [PhysicalPortsTable_Mode]	(Read-only field) Displays the mode of the port: <ul style="list-style-type: none"> ▪ [0] Disable ▪ [1] Enable (default)

Parameter	Description
Native Vlan [PhysicalPortsTable_NativeVlan]	Defines the Native VLAN or PVID of the port. Incoming packets without a VLAN ID are tagged with this VLAN. For outgoing packets, if the VLAN ID as defined in the Multiple Interface table is the same as the Native VLAN ID, the device sends the packet without a VLAN; otherwise, the VLAN ID as defined in the Multiple Interface table takes precedence. The valid value range is 1 to 4096. The default is 1.
Speed & Duplex [PhysicalPortsTable_SpeedDuplex]	Defines the speed and duplex mode of the port. <ul style="list-style-type: none"> [0] 10BaseT Half Duplex [1] 10BaseT Full Duplex [2] 100BaseT Half Duplex [3] 100BaseT Full Duplex [4] Auto Negotiation (default) [6] 1000BaseT Half Duplex [7] 1000BaseT Full Duplex
Description [PhysicalPortsTable_PortDescription]	Defines an arbitrary description of the port.
Group Member [PhysicalPortsTable_GroupMember]	(Read-only field) Displays the group to which the port belongs.
Group Status [PhysicalPortsTable_GroupStatus]	(Read-only) Displays the status of the port: <ul style="list-style-type: none"> "Active" - the active port "Redundant" - the standby (redundant) port

12.2 Configuring Tx/Rx for Ethernet Port-Pair Groups

The Ethernet Group Settings table allows you to configure the transmit (Tx) and receive (Rx) settings for the physical ports belonging to a port-pair group for 1+1 physical port redundancy. You can also assign ports to each port group, where the group can be assigned a single port or two ports for 1+1 redundancy. If an Ethernet Group has a single port, it will operate as a single port (i.e., without 1+1 redundancy). You can setup the device with a combination of Ethernet Groups, where one group has only one physical port (i.e., no redundancy) and another group has two ports for port-pair redundancy.

To view the mapping of physical ports to logical ports (strings) used in the device's management tools (e.g., Web interface), use the CLI command, show voip ports. This displays the MAC address and port status (up or down) of the physical port, and its corresponding logical port. Below shows an example of the mapping results from running this command:

```
Mediant SW# show voip ports
```

Port Num	Port Name	MAC Address	Link Status
1	GE_1	00:1e:67:11:7c:28	UP
2	GE_2	00:1e:67:11:7c:29	DOWN
3	GE_3	68:05:ca:03:6b:4e	DOWN
4	GE_4	68:05:ca:03:6b:98	DOWN



Note: The Ethernet Group Settings table can also be configured using the table ini file parameter, EtherGroupTable.

➤ **To configure the Ethernet port-pair groups:**

1. Open the Ethernet Group Settings page (**Configuration** tab > **VoIP** menu > **Network** submenu > **Ethernet Group Settings**).

Index	Group	Mode	Member 1	Member 2
1	<input checked="" type="radio"/> GROUP_1	2RX 1TX ▼	GE_1 ▼	None ▼
2	<input type="radio"/> GROUP_2	2RX 1TX	GE_2	None

2. Select the 'Index' radio button corresponding to the port group that you want to configure.
3. Click the **Edit** button.
4. Configure the ports as required. For a description of the parameters, see the table below.
5. Click **Apply**.
6. Save your settings to flash memory with a device reset (see "Saving Configuration" on page 308).

Table 12-2: Ethernet Group Settings Parameters Description

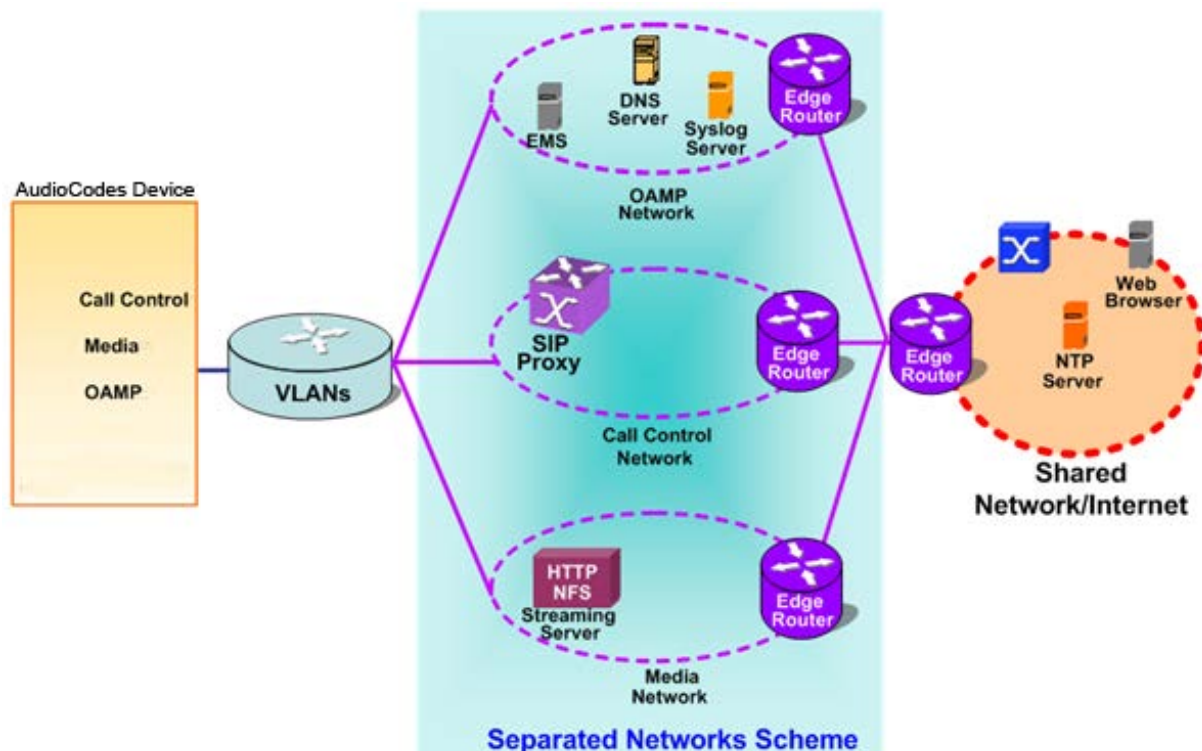
Parameter	Description
Group [EtherGroupTable_Group]	(Read-only) Displays the Ethernet port-pair group number.
Mode [EtherGroupTable_Mode]	<p>Defines the mode of operation of the ports in the group:</p> <ul style="list-style-type: none"> ▪ [3] 2RX/1TX = Both ports in the group can receive packets, but only one port can transmit. The transmitting port is determined arbitrarily by the device. If the selected port fails at a later stage, a switchover to the redundant port is done, which begins to transmit as well as receive. ▪ [4] 2RX/2TX = Both ports in the group can receive and transmit packets. <p>Notes:</p> <ul style="list-style-type: none"> ▪ It is recommended to use the 2RX/1TX option when implementing 1+1 Ethernet redundancy. In such a setup, the ports can be connected to the same LAN switch or each to a different switch where both are in the same subnet. If connecting each port to a different switch, the 2RX/2TX option can be used but only if the port group is associated with OAMP and/or Control application types, not media. ▪ For Ethernet port settings and connections of the Maintenance interface when implementing High Availability, see Initial HA Configuration on page 293.
Member 1 [EtherGroupTable_Member1]	Defines the first port in the Ethernet Group.
Member 2 [EtherGroupTable_Member2]	Defines the second port in the Ethernet Group.

12.3 Configuring IP Network Interfaces

You can configure a single VoIP network interface for all applications, which includes OAMP (management traffic), call control (SIP messages), and media (RTP traffic), or you can configure multiple logical, IP network interfaces for these applications. A need often arises to have logically separated network segments for these applications for administration and security. This can be achieved by employing Layer-2 VLANs and Layer-3 subnets.

The figure below illustrates a typical network architecture where the device is configured with three network interfaces for the OAMP, call control, and media applications. The device is connected to a VLAN-aware switch for directing traffic from and to the device to the three separated Layer-3 broadcast domains according to VLAN tags (middle pane).

Figure 12-1: Multiple Network Interfaces



The Multiple Interface Table page allows you to configure these network interfaces. Each row of the table defines a logical IP interface with the following attributes:

- Application type allowed on the interface:
 - Control - call control signaling traffic (i.e., SIP)
 - Media - RTP traffic
 - Operations, Administration, Maintenance and Provisioning (OAMP) - management (such as Web- and SNMP-based management)
 - Maintenance - Maintenance interface used in High Availability (HA) mode when two devices are deployed together for redundancy - this interface represents one of the Ethernet interfaces or Ethernet groups on each device used for the Ethernet connectivity between the two devices
- IP address and subnet mask represented by prefix length (IPv4 and IPv6 Internet Layer protocols)
- VLAN ID
- Default Gateway - traffic from this interface destined to a subnet that does not meet any of the routing rules, local or static routes, are forwarded to this gateway
- Primary and secondary DNS IP address (optional)

- Associated physical Ethernet port group (Underlying Device) used for the interface - useful for setting trusted and un-trusted networks on different physical ports

You can configure up to 48 interfaces, consisting of up to 47 Control and Media interfaces, including a Maintenance interface if implementing an HA system, and 1 OAMP interface.

The default VoIP interface is as follows:

- Application type: OAMP + Media + Control
- IP address: 192.168.0.1 with prefix length 24 (i.e., subnet mask 255.255.255.0)
- Name: "Voice"
- VLAN ID: 1

For configuring Quality of Service (QoS), see "Configuring the QoS Settings" on page 102.

Complementing the Multiple Interface table is the IP Routing table, which allows you to define static routing rules for non-local hosts/subnets. For more information, see "Configuring the IP Routing Table" on page 99.



Notes:

- For more information on HA and configuring the Maintenance interface, see Configuring High Availability on page 287.
- To configure firewall rules (access list) for allowing or blocking packets received from specific IP network interfaces, see "Configuring Firewall Settings" on page 115.
- The Multiple Interface table can also be configured using the table ini file parameter, InterfaceTable (see "Networking Parameters" on page 387).

➤ To configure IP network interfaces:

1. Open the Multiple Interface Table page (**Configuration** tab > **VoIP** menu > **Network** submenu > **IP Settings**).

Index	Application Type	Interface Mode	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name	Primary DNS Server IP Address	Secondary DNS Server IP Address	Underlying
0	OAMP + Media + Control	IPv4 Manual	10.8.244.80	16	10.8.0.1	1	Voice	0.0.0.0	0.0.0.0	GROUP_1
1	MAINTENANCE	IPv4 Manual	10.3.0.51	16	10.3.0.1	2	Unknown	0.0.0.0	0.0.0.0	GROUP_2

▼

IP Interface Status Table

2. In the 'Add Index' field, enter the desired index number for the new interface, and then click **Add Index**; the index row is added to the table.
3. Configure the interface according to the table below.
4. Click the **Apply** button; the interface is added to the table and the **Done** button appears.
5. Click **Done** to validate the interface. If the interface is not valid (e.g., if it overlaps with another interface in the table or if it does not adhere to the other rules as summarized in "Multiple Interface Table Configuration Summary and Guidelines" on page 94), a warning message is displayed.
6. Save the changes to flash memory and reset the device (see "Saving Configuration" on page 308).

To view configured network interfaces that are currently active, click the IP Interface Status Table button. For more information, see Viewing Active IP Interfaces on page 345.

Table 12-3: Multiple Interface Table Parameters Description

Parameter	Description
-----------	-------------

Parameter	Description
Table parameters	
Index [InterfaceTable_Index]	Table index row of the interface. The range is 0 to 47.
Web: Application Type [InterfaceTable_ApplicationTypes]	<p>Defines the applications allowed on the interface.</p> <ul style="list-style-type: none"> ▪ [0] OAMP = Operations, Administration, Maintenance and Provisioning (OAMP) applications (e.g., Web, Telnet, SSH, and SNMP). ▪ [1] Media = Media (i.e., RTP streams of voice). ▪ [2] Control = Call Control applications (e.g., SIP). ▪ [3] OAMP + Media = OAMP and Media applications. ▪ [4] OAMP + Control = OAMP and Call Control applications. ▪ [5] Media + Control = Media and Call Control applications. ▪ [6] OAMP + Media + Control = All application types are allowed on the interface. ▪ [99] MAINTENANCE = Only the Maintenance application for HA is allowed on this interface. <p>Note: For valid configuration, see Multiple Interface Table Configuration Rules on page 94.</p>
Web: Interface Mode [InterfaceTable_InterfaceMode]	<p>Defines the method that the interface uses to acquire its IP address.</p> <ul style="list-style-type: none"> ▪ [3] IPv6 Manual Prefix = IPv6 manual prefix IP address assignment. The IPv6 prefix (higher 64 bits) is set manually while the interface ID (the lower 64 bits) is derived from the device's MAC address. ▪ [4] IPv6 Manual = IPv6 manual IP address (128 bits) assignment. ▪ [10] IPv4 Manual = IPv4 manual IP address (32 bits) assignment. <p>Note: For valid configuration, see Multiple Interface Table Configuration Rules on page 94.</p>
Web: IP Address [InterfaceTable_IPAddress]	<p>Defines the IPv4/IPv6 IP address in dotted-decimal notation.</p> <p>Note: You can configure overlapping IP addresses for multiple control and media interfaces.</p>
Web: Prefix Length [InterfaceTable_PrefixLength]	<p>Defines the prefix length of the related IP address. This is a Classless Inter-Domain Routing (CIDR)-style representation of a dotted-decimal subnet notation. The CIDR-style representation uses a suffix indicating the number of bits which are set in the dotted-decimal format. For example, 192.168.0.0/16 is synonymous with 192.168.0.0 and subnet 255.255.0.0. This CIDR lists the number of '1' bits in the subnet mask (i.e., replaces the standard dotted-decimal representation of the subnet mask for IPv4 interfaces). For example, a subnet mask of 255.0.0.0 is represented by a prefix length of 8 (i.e., 11111111 00000000 00000000 00000000) and a subnet mask of 255.255.255.252 is represented by a prefix length of 30 (i.e., 11111111 11111111 11111111 11111100).</p> <p>The prefix length is a Classless Inter-Domain Routing (CIDR) style presentation of a dotted-decimal subnet notation. The CIDR-style presentation is the latest method for interpretation of IP addresses. Specifically, instead of using eight-bit address</p>

Parameter	Description
	<p>blocks, it uses the variable-length subnet masking technique to allow allocation on arbitrary-length prefixes.</p> <p>The prefix length for IPv4 can range from 0 to 30 and for IPv6 it must be set to 64.</p> <p>Note: For valid configuration, see Multiple Interface Table Configuration Rules on page 94.</p>
Web: Gateway [InterfaceTable_Gateway]	<p>Defines the IP address of the default gateway for the interface. When traffic is sent from this interface to an unknown destination (i.e., not in the same subnet and not defined for any static routing rule), it is forwarded to this default gateway.</p> <p>Note: For valid configuration, see Multiple Interface Table Configuration Rules on page 94.</p>
Web: VLAN ID [InterfaceTable_VlanID]	<p>Defines a VLAN ID for the interface.</p> <p>Note: For valid configuration, see Multiple Interface Table Configuration Rules on page 94.</p>
Web: Interface Name [InterfaceTable_InterfaceName]	<p>Defines a name for this interface. This name is used in various configuration tables to associate this network interface with other configuration entities such as Media Realms. It is also displayed in management interfaces (Web, CLI, and SNMP) for clarity where it has no functional use.</p> <p>The valid value is a string of up to 16 characters.</p> <p>Note: For valid configuration, see Multiple Interface Table Configuration Rules on page 94.</p>
Web: Primary DNS Server IP address [InterfaceTable_PrimaryDNSServerIPAddress]	<p>(Optional) Defines the primary DNS server's IP address (in dotted-decimal notation), which is used for translating domain names into IP addresses for the interface.</p> <p>By default, no IP address is defined.</p>
Web: Secondary DNS Server IP address [InterfaceTable_SecondaryDNSServerIPAddress]	<p>(Optional) Defines the secondary DNS server's IP address (in dotted-decimal notation), which is used for translating domain names into IP addresses for the interface.</p> <p>By default, no IP address is defined.</p>
Underlying Interface [InterfaceTable_UnderlyingInterface]	<p>Assigns a physical Ethernet port-pair (Group Member) to this IP interface. This is useful for separating trusted networks from untrusted networks, by assigning each to different physical ports. To view the port groups and configure port settings, see Configuring Physical Ethernet Ports on page 87.</p>

12.3.1 Assigning NTP Services to Application Types

You can associate the Network Time Protocol (NTP) application with the OAMP or Control application type. This is done using the EnableNTPasOAM ini file parameter.

12.3.2 Multiple Interface Table Configuration Rules

The Multiple Interface table configuration must adhere to the following rules:

- Multiple Control and Media interfaces can be configured with overlapping IP addresses and subnets.
- The prefix length replaces the dotted-decimal subnet mask presentation and must have a value of 0-30 for IPv4 addresses and a value of 64 for IPv6 addresses.
- Only one OAMP interface must be configured and this must be an IPv4 address. This OAMP interface can be combined with Media and Control.
- At least one Control interface must be configured with an IPv4 address.
- At least one Media interface must be configured with an IPv4 address.
- One or more Media and/or Control interfaces can be configured with an IPv6 address.
- The network interface types can be combined:
 - Example 1:
 - ◆ One combined OAMP-Media-Control interface with an IPv4 address
 - ◆ One combined Media-Control interface with an IPv6 address
 - Example 2:
 - ◆ One OAMP interface with an IPv4 address
 - ◆ One or more Control interfaces with IPv4 addresses
 - ◆ One or more Media interfaces with IPv4 interfaces (with VLANs)
 - Example 3:
 - ◆ One combined OAMP-Media interface with an IPv4 address
 - ◆ One or more combined Media-Control interfaces with IPv4 addresses
 - ◆ None or additional combined Media-Control interfaces with IPv6 addresses
- Each network interface can be configured with a Default Gateway. The address of the Default Gateway must be in the same subnet as the associated interface. Additional static routing rules can be configured in the IP Routing table.
- The interface name must be configured (mandatory) and unique for each interface, and can include up to 16 characters.
- For IPv4 addresses, the 'Interface Mode' column must be set to IPv4 Manual (numeric value 10). For IPv6 addresses, the 'Interface Mode' can be set to either IPv6 Manual (numeric value 4) or IPv6 Manual Prefix (numeric value 3).
- The same VLAN ID may be shared between two interfaces where one has an IPv6 address and the other an IPv4 address. But the same VLAN ID cannot be shared between two interfaces having IPv4 addresses, or two interfaces having IPv6 addresses.
- For network configuration to take effect, you must save the configuration to the device's flash memory (burn) with a device reset..

**Notes:**

- When configuring the network interfaces and VLANs in the Multiple Interface table using the Web interface, it is recommended to check that your configuration is valid, by clicking the **Done** button in the Multiple Interface Table page.
- Upon device start up, the Multiple Interface table is parsed and passes comprehensive validation tests. If any errors occur during this validation phase, the device sends an error message to the Syslog server and falls back to a "safe mode", using a single interface and no VLANs. Ensure that you view the Syslog messages that the device sends in system startup to see if any errors occurred.

12.3.3 Troubleshooting the Multiple Interface Table

If any of the Multiple Interface table guidelines are violated, the device falls back to a "safe mode" configuration, working temporarily with IP address 192.168.0.1. For more information on validation failures, consult the Syslog messages.

Validation failures may be caused by one of the following:

- One of the Application Types (OAMP, Control, or Media) are missing in the IPv4 interfaces.
- An IPv6 interface was defined with a prefix length other than 64.
- There are too many interfaces for Application Type, OAMP. There is only one interface defined, but the 'Application Types' column is not set to **OAMP + Media + Control** (numeric value 6).
- An IPv4 interface was defined with 'Interface Type' other than **IPv4 Manual** (10).
- An IPv6 interface was defined with 'Interface Type' other than IPv6 Manual (4) or IPv6 Manual Prefix (3).
- An IPv6 interface was defined with an IPv4 address in the 'Gateway' column (including "0.0.0.0").
- Two interfaces of the same address family have the same VLAN ID value.
- Two interfaces have the same name.

Apart from these validation errors, connectivity problems may be caused by one of the following:

- Trying to access the device with untagged traffic when VLANs are on and Native VLAN is not configured properly.
- The IP Routing table is not configured properly.

12.3.4 Networking Configuration Examples

This section provides configuration examples of networking interfaces.

12.3.4.1 One VoIP Interface for All Applications

This example describes the configuration of a single VoIP interface for all applications:

1. **Multiple Interface table:** Configured with a single interface for OAMP, Media and Control:

Table 12-4: Example of Single VoIP Interface in Multiple Interface Table

Index	Application Type	Interface Mode	IP Address	Prefix Length	Default	VLAN ID	Interface Name
0	OAMP, Media & Control	IPv4	192.168.0.2	16	192.168.0.1	1	myInterface

2. **IP Routing table:** Two routes are configured for directing traffic for subnet 201.201.0.0/16 to 192.168.11.10, and all traffic for subnet 202.202.0.0/16 to 192.168.11.1:

Table 12-5: Example of IP Routing Table

Destination IP Address	Prefix Length	Gateway IP Address	Metric
201.201.0.0	16	192.168.11.10	1
202.202.0.0	16	192.168.11.1	1

3. The **NTP** applications remain with their default application types.

12.3.4.2 VoIP Interface per Application Type

This example describes the configuration of three VoIP interfaces; one for each application type:

1. **Multiple Interface table:** Configured with three interfaces, each for a different application type, i.e., one for OAMP, one for Call Control, and one for RTP Media, and each with a different VLAN ID and default gateway:

Table 12-6: Example of VoIP Interfaces per Application Type in Multiple Interface Table

Index	Application Type	Interface Mode	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name
0	OAMP	IPv4 Manual	192.168.0.2	16	192.168.0.1	1	ManagementIF
1	Control	IPv4 Manual	200.200.85.14	24	200.200.85.1	200	myControlIF
2	Media	IPv4 Manual	211.211.85.14	24	211.211.85.1	211	myMediaIF

2. **IP Routing table:** A routing rule is required to allow remote management from a host in 176.85.49.0 / 24:

Table 12-7: Example IP Routing Table

Destination IP Address	Prefix Length	Gateway IP Address	Metric	Interface Name
176.85.49.0	24	192.168.11.1	1	-

3. All other parameters are set to their respective default values. The NTP application remains with its default application types.

12.3.4.3 VoIP Interfaces for Combined Application Types

This example describes the configuration of multiple interfaces for the following applications:

- One interface for the OAMP application.
- Interfaces for Call Control and Media applications, where two of them are IPv4 interfaces and one is an IPv6 interface.

1. **Multiple Interface table:**

Table 12-8: Example of VoIP Interfaces of Combined Application Types in Multiple Interface Table

Index	Application Type	Interface Mode	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name
0	OAMP	IPv4 Manual	192.168.0.2	16	192.168.0.1	1	Mgmt
1	Media & Control	IPv4 Manual	200.200.85.14	24	200.200.85.1	201	MediaCntrl1
2	Media & Control	IPv4 Manual	200.200.86.14	24	200.200.86.1	202	MediaCntrl2
3	Media & Control	IPv6 Manual	2000::1:200:200:86:14	64	::	202	V6CntrlMedia2

2. **IP Routing table:** A routing rule is required to allow remote management from a host in 176.85.49.0/24:

Table 12-9: Example of IP Routing Table

Destination IP Address	Prefix Length	Gateway IP Address	Metric	Interface Name
176.85.49.0	24	192.168.0.10	1	-

3. The NTP application is configured (using the ini file) to serve as OAMP applications:
- ```
EnableNTPasOAM = 1
```



#### 4. DiffServ table:

- Layer-2 QoS values are assigned:
  - ◆ For packets sent with DiffServ value of 46, set VLAN priority to 6
  - ◆ For packets sent with DiffServ value of 40, set VLAN priority to 6
  - ◆ For packets sent with DiffServ value of 26, set VLAN priority to 4
  - ◆ For packets sent with DiffServ value of 10, set VLAN priority to 2
- Layer-3 QoS values are assigned:
  - ◆ For Media Service class, the default DiffServ value is set to 46
  - ◆ For Control Service class, the default DiffServ value is set to 40
  - ◆ For Gold Service class, the default DiffServ value is set to 26
  - ◆ For Bronze Service class, the default DiffServ value is set to 10

**Figure 12-2: Example of Layer-2 QoS in DiffServ Table**

| Index | Differentiated Services | VLAN Priority |
|-------|-------------------------|---------------|
| 1     | 0                       | 7             |
| 2     | 46                      | 6             |
| 3     | 40                      | 6             |
| 4     | 26                      | 4             |
| 5     | 10                      | 2             |

| Differentiated Services |    |
|-------------------------|----|
| Media Premium QoS       | 46 |
| Control Premium QoS     | 40 |
| Gold QoS                | 26 |
| Bronze QoS              | 10 |

#### 12.3.4.4 VoIP Interfaces with Multiple Default Gateways

Below is a configuration example using default gateways per IP network interface. In this example, the default gateway for OAMP is 192.168.0.1 and for Media and Control it is 200.200.85.1.

**Table 12-10: Configured Default Gateway Example**

| Index | Application Type | Interface Mode | IP Address    | Prefix Length | Gateway      | VLAN ID | Interface Name |
|-------|------------------|----------------|---------------|---------------|--------------|---------|----------------|
| 0     | OAMP             | IPv4 Manual    | 192.168.0.2   | 16            | 192.168.0.1  | 100     | Mgmt           |
| 1     | Media & Control  | IPv4 Manual    | 200.200.85.14 | 24            | 200.200.85.1 | 200     | CntrlMedia     |

A separate IP routing table enables you to configure static routing rules. Configuring the following static routing rules enables OAMP applications to access peers on subnet 17.17.0.0 through the gateway 192.168.10.1 (which is not the default gateway of the interface), and Media & Control applications to access peers on subnet 171.79.39.0 through the gateway 200.200.85.10 (which is not the default gateway of the interface).



Table 12-11: Separate Routing Table Example

| Destination IP Address | Prefix Length | Gateway IP Address | Metric | Interface Name | Status |
|------------------------|---------------|--------------------|--------|----------------|--------|
| 17.17.0.0              | 16            | 192.168.10.1       | 1      | 0              | Active |
| 171.79.39.0            | 24            | 200.200.85.10      | 1      | 1              | Active |

## 12.4 Configuring the IP Routing Table

The IP Routing Table page allows you to define up to 30 static IP routing rules for the device. These rules can be associated with a network interface (defined in the Multiple Interface table) and therefore, the routing decision is based on the source subnet/VLAN. If not associated with an IP interface, the static IP rule is based on destination IP address. Traffic destined to the subnet specified in the routing rule is re-directed to the defined gateway, reachable through the specified interface. Before sending an IP packet, the device searches this table for an entry that matches the requested destination host/network. If such an entry is found, the device sends the packet to the indicated router. If no explicit entry is found, the packet is sent to the default gateway.

➤ **To configure static IP routing:**

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

Figure 12-3: IP Routing Table Page

The screenshot displays the 'IP Routing Table' configuration interface. It features a main table with the following data:

| # | Delete Row               | Destination IP Address | Prefix Length | Gateway IP Address | Metric | Interface Name | Status |
|---|--------------------------|------------------------|---------------|--------------------|--------|----------------|--------|
| 1 | <input type="checkbox"/> | 169.254.254.252        | 30            | 0.0.0.0            | 0      | InternalIF     | Active |
| 2 | <input type="checkbox"/> | 10.9.0.0               | 16            | 0.0.0.0            | 0      | Voice          | Active |
| 3 | <input type="checkbox"/> | 0.0.0.0                | 0             | 10.9.0.1           | 1      | Voice          | Active |
| 4 | <input type="checkbox"/> | 0.0.0.0                | 0             | 169.254.254.253    | 2      | InternalIF     | Active |

Below the table is a 'Delete Selected Entries' button. At the bottom, the 'Add a new table entry' section contains a table with the following data:

| Destination IP Address | Prefix Length | Gateway IP Address | Metric | Interface Name |
|------------------------|---------------|--------------------|--------|----------------|
|                        | 16            |                    | 1      |                |

An 'Add New Entry' button is located at the bottom of the 'Add a new table entry' section.

2. In the Add a new table entry table, add a new static routing rule according to the parameters described in the table below.
3. Click **Add New Entry**; the new routing rule is added to the IP routing table.

To delete a routing rule from the table, select the 'Delete Row' check box corresponding to the required routing rule, and then click **Delete Selected Entries**.



**Notes:**

- You can delete only inactive routing rules.
- The IP Routing table can also be configured using the table ini file parameter, StaticRouteTable.



Table 12-12: IP Routing Table Description

| Parameter                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      | Description                                                                                                                                                                                                                                                                                                                                                                                     |
|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Destination IP Address<br>[StaticRouteTable_Destination]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       | Defines the IP address of the destination host/network. The destination can be a single host or a whole subnet, depending on the Prefix Length configured for this routing rule.                                                                                                                                                                                                                |
| Prefix Length<br>[StaticRouteTable_PrefixLength]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Defines the Classless Inter-Domain Routing (CIDR)-style representation of a dotted-decimal subnet notation, of the destination host/network. The CIDR-style representation uses a suffix indicating the number of bits that are set in the dotted-decimal format. For example, 16 is synonymous with subnet 255.255.0.0.                                                                        |
| The address of the host/network you want to reach is determined by an AND operation that is applied to the fields 'Destination IP Address' and 'Prefix Length'. For example, to reach the network 10.8.x.x, enter 10.8.0.0 in the 'Destination IP Address' field and 16 in the 'Prefix Length'. As a result of the AND operation, the value of the last two octets in the 'Destination IP Address' field is ignored. To reach a specific host, enter its IP address in the 'Destination IP Address' field and 32 in the 'Prefix Length' field. |                                                                                                                                                                                                                                                                                                                                                                                                 |
| Gateway IP Address<br>[StaticRouteTable_Gateway]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               | Defines the IP address of the router (next hop) used for traffic destined to the subnet/host as defined in the 'Destination IP Address' / 'Prefix Length' field.<br><b>Note:</b> The Gateway address must be in the same subnet as the IP address of the interface over which you configure this static routing rule.                                                                           |
| Metric                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Defines the number of hops needed to reach the specified destination.<br><b>Note:</b> The recommended value for this parameter is 1. This parameter must be set to a number greater than 0 for the routing rule to be valid. Routing entries with Hop Count equals 0 are local routes set automatically by the device.                                                                          |
| Interface Name<br>[StaticRouteTable_InterfaceName]                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             | Assigns a network interface through which the 'Gateway IP Address' is reached. This is the string value as configured for the network interface in the 'Interface Name' field of the Multiple Interface table (see "Configuring IP Network Interfaces" on page 90).<br><b>Note:</b> The IP address of the 'Gateway IP Address' field must be in the same subnet as this interface's IP address. |
| Status                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         | Read-only field displaying the status of the static IP route: <ul style="list-style-type: none"> <li>"Active" - routing rule is used by the device.</li> <li>"Inactive" - routing rule is not applied. When the destination IP address is not on the same segment with the next hop or the interface does not exist, the route state changes to "Inactive".</li> </ul>                          |



## 12.4.1 Interface Column

This example describes the configuration of static IP routing rules.



**Note:** The Interface Address family must be coherent with the Routing Rule Address family. IPv4 interfaces cannot be selected in an IPv6 routing rule, and vice versa.

1. Configure network interfaces in the Multiple Interface table, as shown below:

**Table 12-13: Configured Network Interfaces in Multiple Interface Table**

| Index | Application Type | Interface Mode | IP Address   | Prefix Length | Gateway     | VLAN ID | Interface Name |
|-------|------------------|----------------|--------------|---------------|-------------|---------|----------------|
| 0     | OAMP             | IPv4 Manual    | 192.168.0.2  | 16            | 192.168.0.1 | 501     | Mng            |
| 1     | Media & Control  | IPv4 Manual    | 10.32.174.50 | 24            | 10.32.174.1 | 2012    | MediaCntrl     |
| 2     | Media            | IPv4 Manual    | 10.33.174.50 | 24            | 10.33.174.1 | 2013    | Media1         |
| 3     | Control          | IPv4 Manual    | 10.34.174.50 | 24            | 10.34.174.1 | 2014    | Cntrl1         |

2. Configure static IP Routing rules in the IP Routing table, as shown below:

**Table 12-14: Configured Static IP Routing Rules in IP Routing Table**

| Destination IP Address | Prefix Length | Gateway IP Address | Metric | Interface Name |
|------------------------|---------------|--------------------|--------|----------------|
| 10.31.174.0            | 24            | 192.168.11.1       | 1      | Mng            |
| 174.96.151.15          | 24            | 10.32.174.12       | 1      | MediaCntrl     |
| 10.35.174.0            | 24            | 10.34.174.240      | 1      | Cntrl1         |

Note that the IP address configured in the 'Gateway IP Address' field (i.e., next hop) must reside on the same subnet as the IP address of the associated network interface that is specified in the 'Interface Name' field.

## 12.4.2 Routing Table Configuration Summary and Guidelines

The Routing table configurations must adhere to the following rules:

- Up to 30 different static routing rules can be configured.
- The 'Prefix Length' replaces the dotted-decimal subnet mask presentation. This column must have a value of 0-31 for IPv4 interfaces and a value of 64 for IPv6 interfaces.
- The 'Gateway IP Address' field must be on the same subnet as the IP address of the associated interface specified in the 'Interface Name' field.
- The 'Interface Name' selected for the routing rule must be of the same address family as the rule defined.
- The 'Metric' field must be set to 1.
- For the configuration settings to take effect, you must reset the device with a "burn" to flash memory.



### 12.4.3 Troubleshooting the Routing Table

When adding a new static routing rule, the added rule passes a validation test. If errors are found, the routing rule is rejected and is not added to the IP Routing table. Failed routing validations may result in limited connectivity (or no connectivity) to the destinations specified in the incorrect routing rule. For any error found in the Routing table or failure to configure a routing rule, the device sends a notification message to the Syslog server reporting the problem.

Common routing rule configuration errors may include the following:

- The IP address specified in the 'Gateway IP Address' field is unreachable from the interface specified in the 'Interface Name' field.
- The same destination is configured in two different routing rules.
- More than 30 routing rules have been configured.



**Note:** If an IP routing rule is required to access OAMP applications (for remote management, for example) and the route is not configured correctly, the route is not added and the device is not accessible remotely. To restore connectivity, the device must be accessed locally from the OAMP subnet and the required routes be configured.

## 12.5 Configuring Quality of Service

The Diff Serv Table page is used for configuring the Layer-2 and Layer-3 Quality of Service (QoS) parameters. Differentiated Services (DiffServ) is an architecture providing different types or levels of service for IP traffic. DiffServ (according to RFC 2474), prioritizes certain traffic types based on their priority, thereby, accomplishing a higher-level QoS at the expense of other traffic types. By prioritizing packets, DiffServ routers can minimize transmission delays for time-sensitive packets such as VoIP packets.

You can assign DiffServ to four classes of traffic and assign VLAN priorities (IEEE 802.1p) to various values of DiffServ:

- Premium Media service class – used for RTP media traffic
- Premium Control service class – used for call control (i.e., SIP) traffic
- Gold service class – used for streaming applications
- Bronze service class – used for OAMP applications

The Layer-3 QoS parameters define the values of the DiffServ field in the IP header of the frames related to a specific service class. The Layer-2 QoS parameters define the values for the 3 priority bits in the VLAN tag (according to the IEEE 802.1p standard) according to the value of the DiffServ field found in the packet IP header.

The DiffServ Table (DiffServToVlanPriority) allows you to configure up to 64 DiffServ-to-VLAN Priority mapping (Layer 2 class of service). For each packet sent to the LAN, the VLAN Priority of the packet is set according to the DiffServ value in the IP header of the packet.

The mapping of an application to its CoS and traffic type is shown in the table below:

**Table 12-15: Traffic/Network Types and Priority**

| Application         | Traffic / Network Types | Class-of-Service (Priority) |
|---------------------|-------------------------|-----------------------------|
| Debugging interface | Management              | Bronze                      |
| Telnet              | Management              | Bronze                      |
| DHCP                | Management              | Network                     |



| Application         | Traffic / Network Types                                                                                                                                                                            | Class-of-Service (Priority)                                                                                                     |
|---------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------|
| Web server (HTTP)   | Management                                                                                                                                                                                         | Bronze                                                                                                                          |
| SNMP GET/SET        | Management                                                                                                                                                                                         | Bronze                                                                                                                          |
| Web server (HTTPS)  | Management                                                                                                                                                                                         | Bronze                                                                                                                          |
| RTP traffic         | Media                                                                                                                                                                                              | Premium media                                                                                                                   |
| RTCP traffic        | Media                                                                                                                                                                                              | Premium media                                                                                                                   |
| T.38 traffic        | Media                                                                                                                                                                                              | Premium media                                                                                                                   |
| SIP                 | Control                                                                                                                                                                                            | Premium control                                                                                                                 |
| SIP over TLS (SIPS) | Control                                                                                                                                                                                            | Premium control                                                                                                                 |
| Syslog              | Management                                                                                                                                                                                         | Bronze                                                                                                                          |
| SNMP Traps          | Management                                                                                                                                                                                         | Bronze                                                                                                                          |
| DNS client          | Varies according to DNS settings: <ul style="list-style-type: none"> <li>OAMP</li> <li>Control</li> </ul>                                                                                          | Depends on traffic type: <ul style="list-style-type: none"> <li>Control: Premium Control</li> <li>Management: Bronze</li> </ul> |
| NTP                 | Varies according to the interface type associated with NTP (see "Assigning NTP Services to Application Types" on page 94): <ul style="list-style-type: none"> <li>OAMP</li> <li>Control</li> </ul> | Depends on traffic type: <ul style="list-style-type: none"> <li>Control: Premium control</li> <li>Management: Bronze</li> </ul> |

**Notes:**

- For the QoS settings to take effect, a device reset is required.
- You can also configure the DiffServ table using the table ini file parameter DiffServToVlanPriority.

➤ **To configure QoS:**

- Open the Diff Serv Table page (**Configuration** tab > **VoIP** menu > **Network** submenu > **QoS Settings**).

**Figure 12-4: DiffServ Table Page**

| Index | Differentiated Services        | VLAN Priority                  |
|-------|--------------------------------|--------------------------------|
| 1     | <input type="text" value="6"/> | <input type="text" value="1"/> |

| Differentiated Services |                                 |
|-------------------------|---------------------------------|
| Media Premium QoS       | <input type="text" value="46"/> |
| Control Premium QoS     | <input type="text" value="40"/> |
| Gold QoS                | <input type="text" value="26"/> |
| Bronze QoS              | <input type="text" value="10"/> |

- Configure DiffServ to VLAN priority mapping (Layer-2 QoS):
  - Enter an index entry, and then click Add.



- b. In the 'Differentiated Services' field, enter the DiffServ value (0-63) and its corresponding VLAN priority level (0-7).
  - c. Click Submit.
3. Configure the desired DiffServ (Layer-3 QoS) values for the following traffic classes:
  - Media Premium QoS: this affects Media RTP packets sent by the VoIP towards the LAN.
  - Control Premium QoS: this affects Control Protocol (SIP) packets sent by the VoIP towards the LAN.
  - Gold QoS: this affects HTTP Streaming packets sent by the VoIP towards the LAN.
  - Bronze QoS: this affects OAMP packets sent by the VoIP towards the LAN.
4. Click **Submit** to apply your changes.
5. Save the changes to flash memory and reset the device (see "Saving Configuration" on page 308).

## 12.6 Disabling ICMP Redirect Messages

You can configure the device's handling of ICMP Redirect messages. These messages can either be rejected (ignored) or permitted.

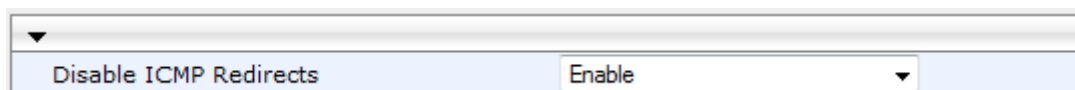


**Note:** You can also configure this feature using the ini file parameter DisableICMPRedirects (see "Routing Parameters" on page 388).

### ➤ To configure the handling of ICMP Redirect messages:

1. Open the Network Settings page (**Configuration** tab > **VoIP** menu > **Network** submenu > **Network Settings**).

**Figure 12-5: Disabling ICMP Redirect in Network Settings Page**



The screenshot shows a web interface with a dropdown menu labeled 'Disable ICMP Redirects'. The dropdown is open, showing the option 'Enable' selected.

2. From the 'Disable ICMP Redirects' drop-down list, select the required option.
3. Click **Submit** to apply your changes.

## 12.7 DNS

You can use the device's embedded domain name server (DNS) or an external, third-party DNS to translate domain names into IP addresses. This is useful if domain names are used as the destination in call routing. The device supports the configuration of the following DNS types:

- Internal DNS table - see "Configuring the Internal DNS Table" on page 104
- Internal SRV table - see "Configuring the Internal SRV Table" on page 106

### 12.7.1 Configuring the Internal DNS Table

The Internal DNS Table page, similar to a DNS resolution, translates up to 20 host (domain) names into IP addresses. This functionality can be used when a domain name (FQDN) is configured as an IP destination for IP-to-IP routing in the SBC IP-to-IP Routing



table. Up to four different IP addresses can be assigned to the same host name. This is typically needed for alternative Tel-to-IP call routing.



**Notes:**

- The device initially attempts to resolve a domain name using the Internal DNS table. If the domain name isn't listed in the table, the device performs a DNS resolution using an external DNS server for the related IP network interface, configured in the Multiple Interface table (see "Configuring IP Network Interfaces" on page 90).
- You can also configure the DNS table using the table ini file parameter, DNS2IP (see "DNS Parameters" on page 391).

➤ **To configure the internal DNS table:**

1. Open the Internal DNS Table page (**Configuration** tab > **VoIP** menu > **Network** submenu > **DNS** submenu > **Internal DNS Table**).
2. Click **Add**; the following dialog box appears:

**Figure 12-6: Internal DNS Table - Add Record Dialog Box**

3. Configure the DNS rule, as required. For a description of the parameters, see the table below.
4. Click **Submit**; the DNS rule is added to the table.

**Table 12-16: Internal DNS Table Parameter Description**

| Parameter                                     | Description                                                                                             |
|-----------------------------------------------|---------------------------------------------------------------------------------------------------------|
| Domain Name<br>[Dns2Ip_DomainName]            | Defines the host name to be translated.<br>The valid value is a string of up to 31 characters.          |
| First IP Address<br>[Dns2Ip_FirstIpAddress]   | Defines the first IP address (in dotted-decimal format notation) to which the host name is translated.  |
| Second IP Address<br>[Dns2Ip_SecondIpAddress] | Defines the second IP address (in dotted-decimal format notation) to which the host name is translated. |
| Third IP Address<br>[Dns2Ip_ThirdIpAddress]   | Defines the third IP address (in dotted-decimal format notation) to which the host name is translated.  |
| Fourth IP Address<br>[Dns2Ip_FourthIpAddress] | Defines the fourth IP address (in dotted-decimal format notation) to which the host name is translated. |



## 12.7.2 Configuring the Internal SRV Table

The Internal SRV Table page resolves host names to DNS A-Records. Three different A-Records can be assigned to each host name, where each A-Record contains the host name, priority, weight, and port.



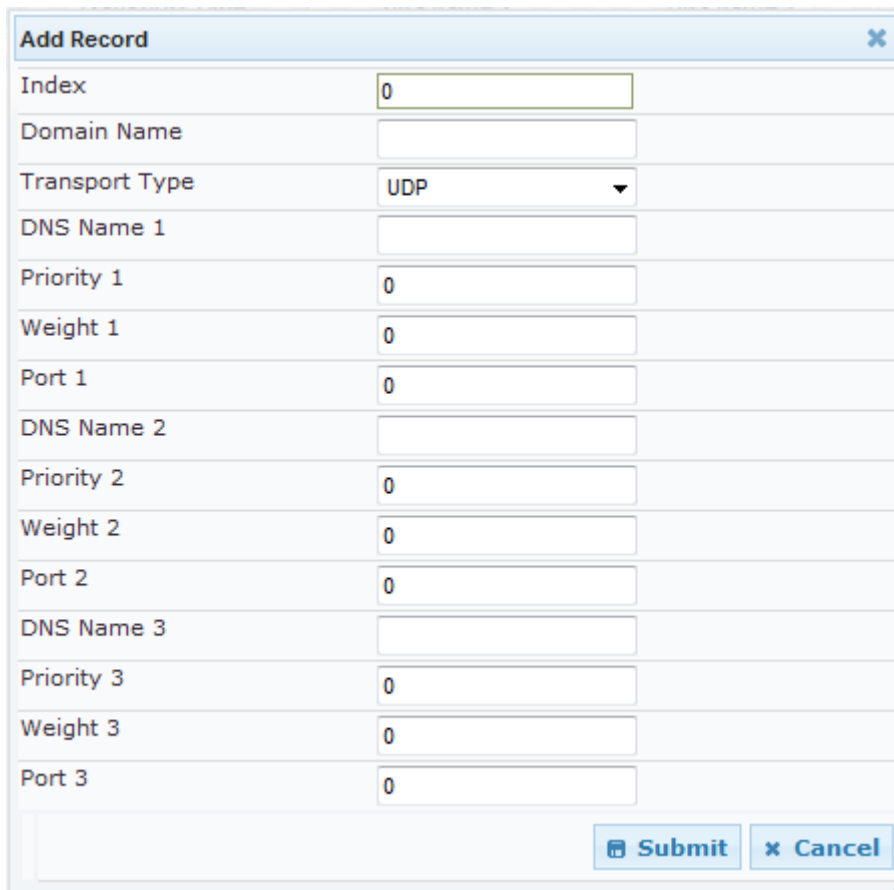
### Notes:

- If the Internal SRV table is configured, the device initially attempts to resolve a domain name using this table. If the domain name isn't found, the device performs a Service Record (SRV) resolution using an external DNS server configured in the Multiple Interface table (see "Configuring IP Network Interfaces" on page 90).
- The Internal SRV table can also be configured using the table ini file parameter, SRV2IP (see "DNS Parameters" on page 391).

### ➤ To configure the Internal SRV table:

1. Open the Internal SRV Table page (**Configuration** tab > **VoIP** menu > **Network** submenu > **DNS** submenu > **Internal SRV Table**).
2. Click **Add**; the following dialog box appears:

Figure 12-7: Internal SRV Table Page



|                |     |
|----------------|-----|
| Index          | 0   |
| Domain Name    |     |
| Transport Type | UDP |
| DNS Name 1     |     |
| Priority 1     | 0   |
| Weight 1       | 0   |
| Port 1         | 0   |
| DNS Name 2     |     |
| Priority 2     | 0   |
| Weight 2       | 0   |
| Port 2         | 0   |
| DNS Name 3     |     |
| Priority 3     | 0   |
| Weight 3       | 0   |
| Port 3         | 0   |

3. Configure the SRV rule, as required. For a description of the parameters, see the table below.
4. Click **Submit**; the SRV rule is added to the table.



Table 12-17: Internal SRV Table Parameter Description

| Parameter                                | Description                                                                                                                             |
|------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------|
| Domain Name<br>[Srv2lp_InternalDomain]   | Defines the host name to be translated.<br>The valid value is a string of up to 31 characters.                                          |
| Transport Type<br>[Srv2lp_TransportType] | Defines the transport type. <ul style="list-style-type: none"> <li>▪ [0] UDP (default)</li> <li>▪ [1] TCP</li> <li>▪ [2] TLS</li> </ul> |
| DNS Name (1-3)<br>[Srv2lp_Dns1/2/3]      | Defines the first, second or third DNS A-Record to which the host name is translated.                                                   |
| Priority (1-3)<br>[Srv2lp_Priority1/2/3] | Defines the priority of the target host. A lower value means that it is more preferred.                                                 |
| Weight (1-3)<br>[Srv2lp_Weight1/2/3]     | Defines a relative weight for records with the same priority.                                                                           |
| Port (1-3)<br>[Srv2lp_Port1/2/3]         | Defines the TCP or UDP port on which the service is to be found.                                                                        |

## 12.8 Configuring NFS Settings

Network File System (NFS) enables the device to access a remote server's shared files and directories and to handle them as if they're located locally. The device can use NFS to load *cmp*, *ini*, and auxiliary files through the Automatic Update mechanism (see 'Automatic Update' on page 327).

You can configure up to 16 different NFS file systems. As a file system, the NFS is independent of machine types, operating systems and network architectures. Note that an NFS file server can share multiple file systems. There must be a separate row for each remote file system shared by the NFS file server that needs to be accessed by the device.

### ➤ To add remote NFS file systems:


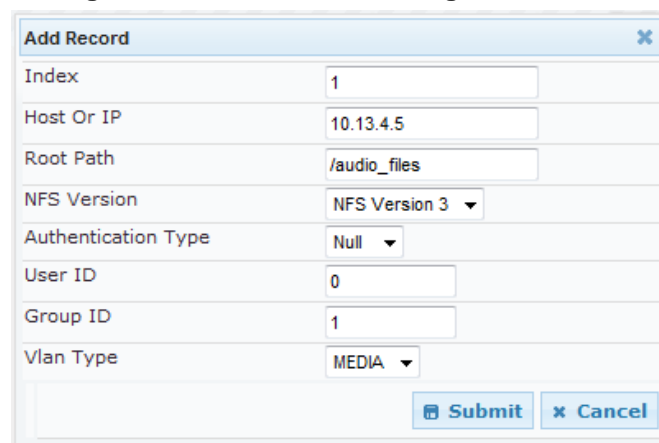
1. Open the Application Settings page (**Configuration** tab > **System** menu > **Application Settings**).
2. Under the 'NFS Settings' group, click the **NFS Table**  button; the NFS Table page appears.
3. Click the **Add** button; the Add Record dialog box appears:

Figure 12-8: Add Record Dialog Box for NFS



The 'Add Record' dialog box for NFS configuration contains the following fields and options:

- Index:** Text input field with value '1'.
- Host Or IP:** Text input field with value '10.13.4.5'.
- Root Path:** Text input field with value '/audio\_files'.
- NFS Version:** Dropdown menu with 'NFS Version 3' selected.
- Authentication Type:** Dropdown menu with 'Null' selected.
- User ID:** Text input field with value '0'.
- Group ID:** Text input field with value '1'.
- Vlan Type:** Dropdown menu with 'MEDIA' selected.

At the bottom right, there are two buttons: **Submit** and **Cancel**.



4. Configure the NFS parameters according to the table below.
5. Click the **Submit** button; the remote NFS file system is immediately applied, which can be verified by the appearance of the 'NFS mount was successful' message in the Syslog server.
6. To save the changes to flash memory, see "Saving Configuration" on page 308.


**Notes:**

- To avoid terminating current calls, a row must not be deleted or modified while the device is currently accessing files on that remote NFS file system.
- The combination of 'Host Or IP' and 'Root Path' must be unique for each row in the table. For example, the table must include only one row with a Host/IP of 192.168.1.1 and Root Path of /audio.
- The NFS table can also be configured using the table ini file parameter NFSServers (see "NFS Parameters" on page 390)

**Table 12-18: NFS Settings Parameters**

| Parameter                                    | Description                                                                                                                                                                                                                                                                                                |
|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Index                                        | The row index of the remote file system.<br>The valid range is 1 to 16.                                                                                                                                                                                                                                    |
| Host Or IP<br>[NFSServers_HostOrIP]          | The domain name or IP address of the NFS server. If a domain name is provided, a DNS server must be configured.                                                                                                                                                                                            |
| Root Path<br>[NFSServers_RootPath]           | Path to the root of the remote file system in the format: /[path]. For example, '/audio'.                                                                                                                                                                                                                  |
| NFS Version<br>[NFSServers_NfsVersion]       | NFS version used to access the remote file system. <ul style="list-style-type: none"> <li>▪ [2] NFS Version 2</li> <li>▪ [3] NFS Version 3 (default)</li> </ul>                                                                                                                                            |
| Authentication Type<br>[NFSServers_AuthType] | Authentication method used for accessing the remote file system. <ul style="list-style-type: none"> <li>▪ [0] Null</li> <li>▪ [1] Unix (default)</li> </ul>                                                                                                                                                |
| User ID<br>[NFSServers_UID]                  | User ID used in authentication when using Unix.<br>The valid range is 0 to 65537. The default is 0.                                                                                                                                                                                                        |
| Group ID<br>[NFSServers_GID]                 | Group ID used in authentication when using Unix.<br>The valid range is 0 to 65537. The default is 1.                                                                                                                                                                                                       |
| VLAN Type<br>[NFSServers_VlanType]           | The VLAN type for accessing the remote file system. <ul style="list-style-type: none"> <li>▪ [0] OAM</li> <li>▪ [1] MEDIA (default)</li> </ul> <p><b>Note:</b> This parameter applies only if VLANs are enabled or if Multiple IPs is configured (see "Configuring IP Network Interfaces" on page 90).</p> |

## 12.9 Network Address Translation Support

Network Address Translation (NAT) is a mechanism that maps internal IP addresses (and ports) used within a private network to global IP addresses and vice versa, providing transparent routing to end hosts. The primary advantages of NAT include (1) reduction in



the number of global IP addresses required in a private network (global IP addresses are only used to connect to the Internet) and (2) better network security by hiding the internal architecture.

The design of SIP creates a problem for VoIP traffic to pass through NAT. SIP uses IP addresses and port numbers in its message body. However, the NAT server is unable to modify the SIP messages and thus, can't change local addresses to global addresses.

This section discusses the device's solutions for overcoming NAT traversal issues.

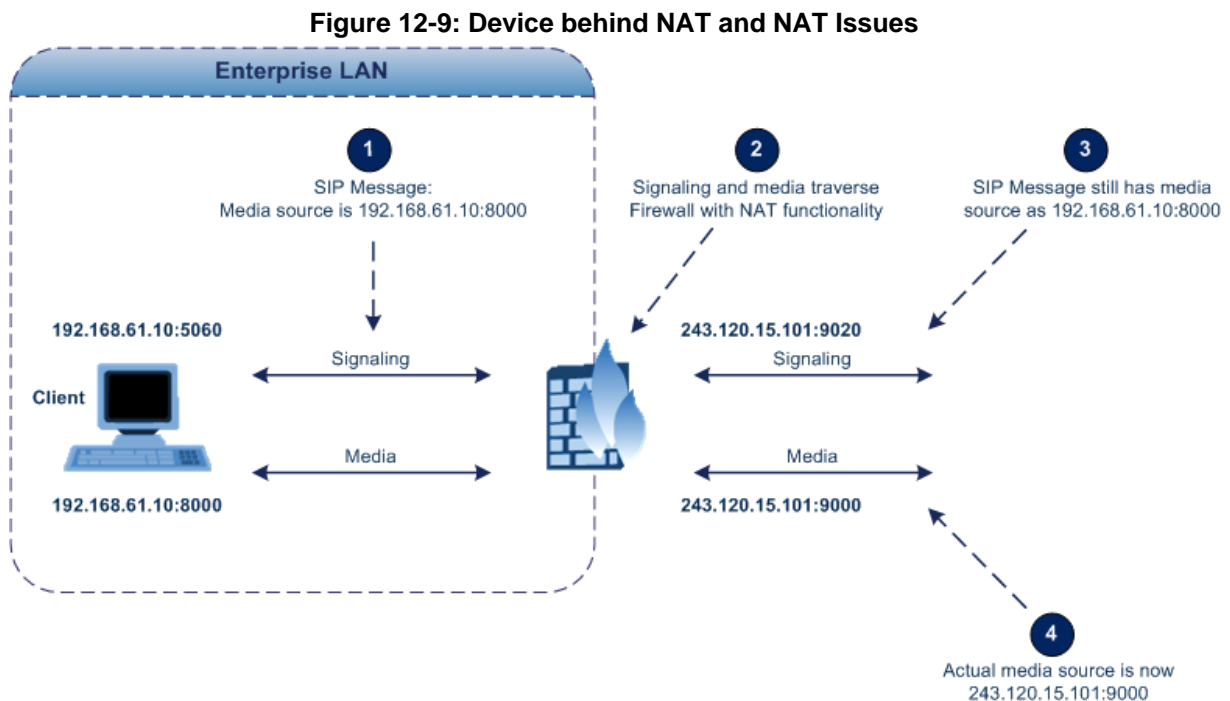
### 12.9.1 Device Located behind NAT

Two different streams traverse through NAT - signaling and media. A device located behind a NAT, that initiates a signaling path has problems receiving incoming signaling responses as they are blocked by the NAT server. Therefore, the initiating device must inform the receiving device where to send the media. To resolve this NAT problem, the following solutions are provided by the device, listed in priority of the selected method used by the device:

- a. If configured, uses the single Static NAT IP address for all interfaces - see "Configuring a Static NAT IP Address for All Interfaces" on page 110.
- b. If configured, uses the NAT Translation table which configures NAT per interface - see Configuring NAT Translation per IP Interface on page 110.

If NAT is not configured by any of the above-mentioned methods, the device sends the packet according to its IP address configured in the Multiple Interface table.

The figure below illustrates the NAT problem faced by the SIP networks where the device is located behind a NAT:





### 12.9.1.1 Configuring a Static NAT IP Address for All Interfaces

You can configure a global (public) IP address of the router to enable static NAT between the device and the Internet for all network interfaces. Thus, the device replaces the source IP address for media of all outgoing SIP messages sent on any of its network interfaces to this public IP address.

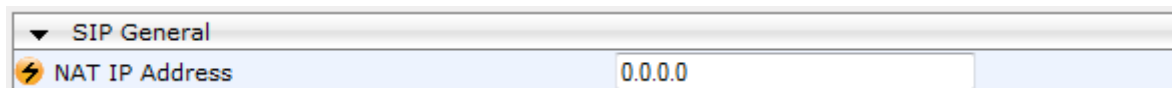


**Note:** The NAT IP address can also be configured using the ini file parameter, StaticNATIP.

➤ To configure a single static NAT IP address for all interfaces:

1. Open the SIP General Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** submenu > **General Parameters**).

**Figure 12-10: Configuring Static NAT IP Address in SIP General Parameters Page**



The screenshot shows a web interface for 'SIP General' parameters. Under the 'SIP General' tab, there is a section for 'NAT IP Address' with a text input field containing '0.0.0.0'.

2. In the 'NAT IP Address' field, enter the NAT IP address in dotted-decimal notation.
3. Click **Submit**.
4. Save the setting to the device's flash memory with a device reset (see "Saving Configuration" on page 308).

### 12.9.1.2 Configuring NAT Translation per IP Interface

The NAT Translation table defines network address translation (NAT) rules for translating source IP addresses per VoIP interface (SIP control and RTP media traffic) into NAT IP addresses (*global* or *public*), when the device is located behind NAT. This allows, for example, the separation of VoIP traffic between different ITSP's, and topology hiding of internal IP addresses to the "public" network. Each IP interface (configured in the Multiple Interface table) can be associated with a NAT rule in this table, translating the source IP address and port of the outgoing packet into the NAT address (IP address and port range). The device's NAT traversal mechanism replaces the source IP address of SIP messages sent from a specified VoIP interface to a public IP address.



**Note:** The NAT Translation table can also be configured using the table ini file parameter, NATTranslation.



➤ **To configure NAT translation rules:**

1. Open the NAT Translation Table page (**Configuration** tab > **VoIP** menu > **Control Network** submenu > **NAT Translation Table**).
2. Click the **Add** button; the following dialog box appears:

**Figure 12-11: NAT Translation Table Page**

| Add Record                                                                  |                |
|-----------------------------------------------------------------------------|----------------|
| Index                                                                       | 0              |
| Source Interface Name                                                       | Voice          |
| Target IP Address                                                           | 212.199.200.90 |
| Source Start Port                                                           | 5070           |
| Source End Port                                                             | 5070           |
| Target Start Port                                                           | 5070           |
| Target End Port                                                             | 5070           |
| <input type="button" value="Submit"/> <input type="button" value="Cancel"/> |                |

3. Configure the parameters as required. For a description of the parameters, see the table below:
4. Click **Submit** to apply your changes.
5. To save the changes to flash memory, see "Saving Configuration" on page 308.

**Table 12-19: NAT Translation Table Parameters**

| Parameter                                                       | Description                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Index<br>[NATTranslation_Index]                                 | Defines the table index entry. This table can include up to 32 entries.                                                                                                                                                                                                             |
| Source Interface Name<br>[NATTranslation_SourceIPInterfaceName] | Defines the name of the IP interface, as appears in the Multiple Interface table.                                                                                                                                                                                                   |
| Target IP Address<br>[NATTranslation_TargetIPAddress]           | Defines the global IP address. This address is set in the SIP Via and Contact headers as well as in the o= and c= SDP fields.                                                                                                                                                       |
| Source Start Port<br>[NATTranslation_SourceStartPort]           | Defines the optional starting port range (1-65536) of the IP interface, used as matching criteria for this NAT rule. If not configured, the match is done on the entire port range. Only IP addresses and ports of matched source ports will be replaced.                           |
| Source End Port<br>[NATTranslation_SourceEndPort]               | Defines the optional ending port range (1-65536) of the IP interface, used as matching criteria for this NAT rule. If not configured, the match is done on the entire port range. Only IP addresses and ports of matched source ports will be replaced.                             |
| Target Start Port<br>[NATTranslation_TargetStartPort]           | Defines the optional, starting port range (1-65536) of the global address. If not configured, the ports are not replaced. Matching source ports are replaced with the target ports. This address is set in the SIP Via and Contact headers, as well as in the o= and c= SDP fields. |



| Parameter                                          | Description                                                                                                                                                                                                                                                                       |
|----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Target End Port<br>[NATTranslation_TargetEndPoint] | Defines the optional, ending port range (1-65536) of the global address. If not configured, the ports are not replaced. Matching source ports are replaced with the target ports. This address is set in the SIP Via and Contact headers, as well as in the o= and c= SDP fields. |

## 12.9.2 Remote UA behind NAT

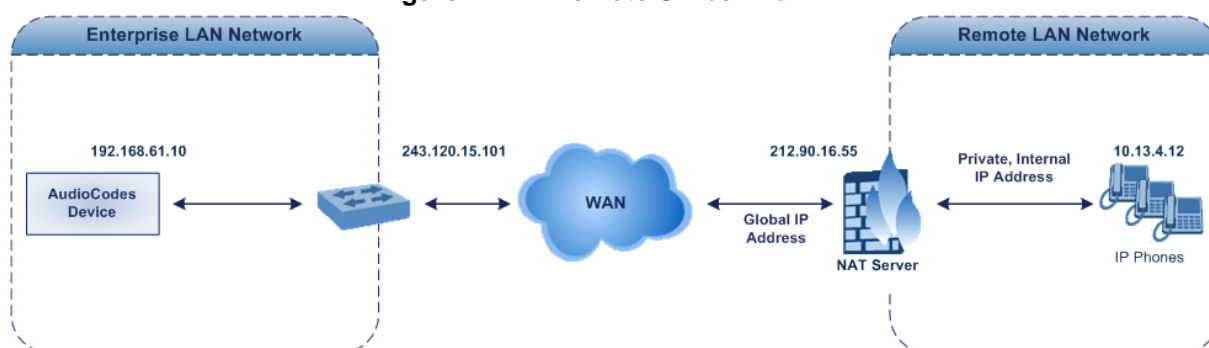
If the remote User Agent with which the device needs to communicate with is located behind NAT, the device can resolve the problem of activating the RTP/RTCP/T.38 streams to an invalid IP address / UDP port.

To resolve this NAT traversal issue, the device offers the following features:

- First Incoming Packet Mechanism - see "First Incoming Packet Mechanism" on page 112
- RTP No-Op packets according to the avt-rtp-noop draft - see "No-Op Packets" on page 113

The figure below illustrates a typical network architecture where the remote UA is located behind NAT:

Figure 12-12: Remote UA behind NAT



### 12.9.2.1 First Incoming Packet Mechanism

If the remote device resides behind a NAT device, it's possible that the device can activate the RTP/RTCP/T.38 streams to an invalid IP address / UDP port. To avoid such cases, the device automatically compares the source address of the first received incoming RTP/RTCP/T.38 stream with the IP address and UDP port of the remote device when the session was initially opened. If the two are not identical, then the destination IP address of the outgoing RTP packets is set to the source IP address of the first incoming packet. The RTP, RTCP and T.38 can thus have independent destination IP addresses and UDP ports.

➤ To enable NAT resolution using the First Incoming Packet mechanism:

1. Open the General Media Settings page (**Configuration** tab > **VoIP** menu > **Media** > **General Media Settings**).
2. Set the 'NAT Traversal' parameter to **Enable**.
3. Click **Submit**.



### 12.9.2.2 No-Op Packets

The device's No-Op packet support can be used to verify Real-Time Transport Protocol (RTP) and T.38 connectivity, and to keep NAT bindings and Firewall pinholes open. The No-Op packets are available for sending in RTP and T.38 formats.

You can control the activation of No-Op packets by using the *ini* file parameter NoOpEnable. If No-Op packet transmission is activated, you can control the time interval in which No-Op packets are sent in the case of silence (i.e., no RTP or T.38 traffic). This is done using the *ini* file parameter NoOpInterval. For a description of the RTP No-Op *ini* file parameters, see "Networking Parameters" on page 387.

- **RTP No-Op:** The RTP No-Op support complies with IETF Internet-Draft draft-wing-avt-rtp-noop-03 ("A No-Op Payload Format for RTP"). This IETF document defines a No-Op payload format for RTP. The draft defines the RTP payload type as dynamic. You can control the payload type with which the No-Op packets are sent. This is performed using the RTPNoOpPayloadType *ini* parameter (see "Networking Parameters" on page 387). The default payload type is 120.
- **T.38 No-Op:** T.38 No-Op packets are sent only while a T.38 session is activated. Sent packets are a duplication of the previously sent frame (including duplication of the sequence number).



**Note:** Receipt of No-Op packets is always supported.



## 12.10 Robust Receipt of Media Streams

The “robust-media” mechanism is an AudioCodes proprietary mechanism to filter out unwanted media (i.e., RTP, RTCP, and T.38) streams that are sent to the same port number on the device. In practice, the media RTP/RTCP ports may receive additional multiple unwanted media streams as result of traces of previous calls, call control errors, or deliberate attacks. When more than one media stream reaches the device on the same port number, the “robust-media” mechanism detects the valid media stream and ignores the rest.

## 12.11 Multiple Routers Support

Multiple routers support is designed to assist the device when it operates in a multiple routers network. The device learns the network topology by responding to Internet Control Message Protocol (ICMP) redirections and caches them as routing rules (with expiration time).

When a set of routers operating within the same subnet serve as devices to that network and intercommunicate using a dynamic routing protocol, the routers can determine the shortest path to a certain destination and signal the remote host the existence of the better route. Using multiple router support, the device can utilize these router messages to change its next hop and establish the best path.



**Note:** Multiple Routers support is an integral feature that doesn't require configuration.



# 13 Security

This section describes the VoIP security-related configuration.

## 13.1 Configuring Firewall Settings

The device provides an internal firewall that enables you to configure network traffic filtering rules (*access list*). You can add up to 50 firewall rules. The access list offers the following firewall possibilities:

- Block traffic from known malicious sources
- Allow traffic only from known "friendly" sources, and block all other traffic
- Mix allowed and blocked network sources
- Limit traffic to a user-defined rate (blocking the excess)
- Limit traffic to specific protocols, and specific port ranges on the device

For each packet received on the network interface, the table is scanned from top to bottom until the first matching rule is found. This rule can either permit (*allow*) or deny (*block*) the packet. Once a rule in the table is located, subsequent rules further down the table are ignored. If the end of the table is reached without a match, the packet is accepted.

### Notes:

- This firewall applies to a very low-level network layer and overrides your other security-related configuration. Thus, if you have configured higher-level security features (e.g., on the Application level), you must also configure firewall rules to permit this necessary traffic. For example, if you have configured IP addresses to access the Web and Telnet interfaces in the Web Access List (see 'Configuring Web and Telnet Access List' on page [Error! Bookmark not defined.](#)), you must configure a firewall rule that permits traffic from these IP addresses.
- Only Security Administrator users or Master users can configure firewall rules.
- Setting the 'Prefix Length' field to **0** means that the rule applies to **all** packets, regardless of the defined IP address in the 'Source IP' field. Therefore, it is highly recommended to set this parameter to a value other than 0.
- It is recommended to add a rule at the end of your table that blocks all traffic and to add firewall rules above it that allow required traffic (with bandwidth limitations). To block all traffic, use the following firewall rule:
  - Source IP: 0.0.0.0
  - Prefix Length: 0 (i.e., rule matches all IP addresses)
  - Start Port - End Port: 0-65535
  - Protocol: **Any**
  - Action Upon Match: **Block**
- If you are using the High Availability feature and you have configured "block" rules, then ensure that you also add "allow" rules for HA traffic. For more information, see Configuring Firewall Allowed Rules on page [299](#).
- You can also configure the firewall settings using the table ini file parameter, AccessList (see "Security Parameters" on page [407](#)).

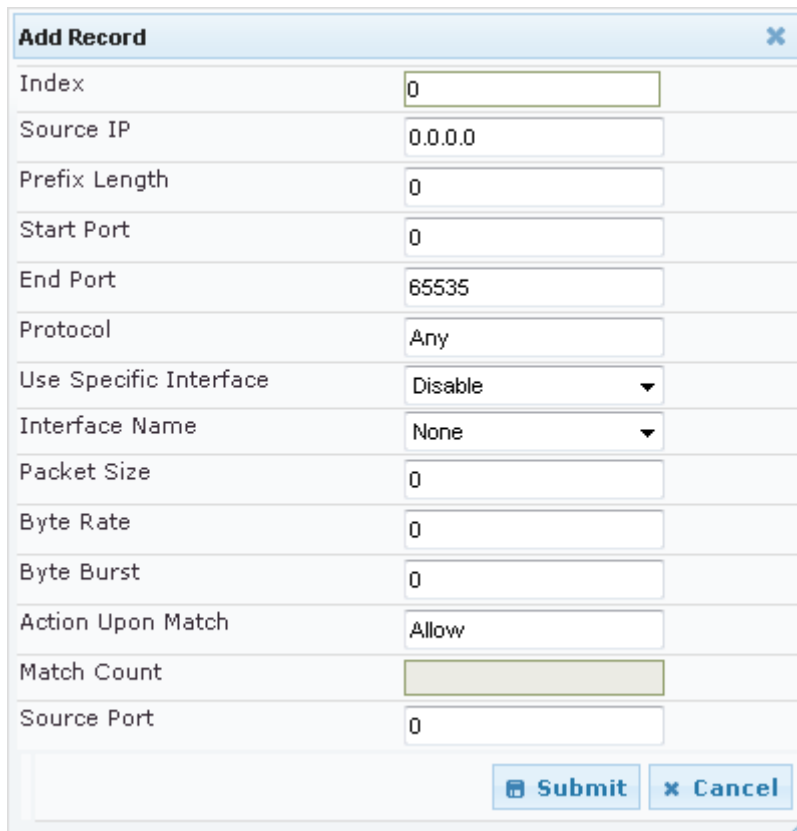




➤ **To add firewall rules:**

1. Open the Firewall Settings page (**Configuration** tab > **VoIP** menu > **Security** submenu > **Firewall Settings**).
2. Click the **Add** button; the following dialog box appears:

**Figure 13-1: Firewall Settings Page - Add Record**



| Add Record                                                                  |         |
|-----------------------------------------------------------------------------|---------|
| Index                                                                       | 0       |
| Source IP                                                                   | 0.0.0.0 |
| Prefix Length                                                               | 0       |
| Start Port                                                                  | 0       |
| End Port                                                                    | 65535   |
| Protocol                                                                    | Any     |
| Use Specific Interface                                                      | Disable |
| Interface Name                                                              | None    |
| Packet Size                                                                 | 0       |
| Byte Rate                                                                   | 0       |
| Byte Burst                                                                  | 0       |
| Action Upon Match                                                           | Allow   |
| Match Count                                                                 |         |
| Source Port                                                                 | 0       |
| <input type="button" value="Submit"/> <input type="button" value="Cancel"/> |         |

3. Configure the firewall parameters, as required. For a description of the parameters, see the table below.
4. Click **Submit** to add the new firewall rule to the table.
5. Reset the device to activate the rules.

The table below provides an example of configured firewall rules:

**Table 13-1: Firewall Rule Examples**

| Parameter                      | Value per Rule |              |         |           |         |
|--------------------------------|----------------|--------------|---------|-----------|---------|
|                                | 1              | 2            | 3       | 4         | 5       |
| <b>Source IP</b>               | 12.194.231.76  | 12.194.230.7 | 0.0.0.0 | 192.0.0.0 | 0.0.0.0 |
| <b>Prefix Length</b>           | 16             | 16           | 0       | 8         | 0       |
| <b>Start Port and End Port</b> | 0-65535        | 0-65535      | 0-65535 | 0-65535   | 0-65535 |
| <b>Protocol</b>                | Any            | Any          | icmp    | Any       | Any     |
| <b>Use Specific Interface</b>  | Enable         | Enable       | Disable | Enable    | Disable |
| <b>Interface Name</b>          | WAN            | WAN          | None    | Voice-Lan | None    |



| Parameter         | Value per Rule |       |       |       |       |
|-------------------|----------------|-------|-------|-------|-------|
|                   | 1              | 2     | 3     | 4     | 5     |
| Byte Rate         | 0              | 0     | 40000 | 40000 | 0     |
| Burst Bytes       | 0              | 0     | 50000 | 50000 | 0     |
| Action Upon Match | Allow          | Allow | Allow | Allow | Block |

The firewall rules in the above configuration example do the following:

- **Rules 1 and 2:** Typical firewall rules that allow packets ONLY from specified IP addresses (e.g., proxy servers). Note that the prefix length is configured.
- **Rule 3:** A more "advanced" firewall rule - bandwidth rule for ICMP, which allows a maximum bandwidth of 40,000 bytes/sec with an additional allowance of 50,000 bytes. If, for example, the actual traffic rate is 45,000 bytes/sec, then this allowance would be consumed within 10 seconds, after which all traffic exceeding the allocated 40,000 bytes/sec is dropped. If the actual traffic rate then slowed to 30,000 bytes/sec, the allowance would be replenished within 5 seconds.
- **Rule 4:** Allows traffic from the LAN voice interface and limits bandwidth.
- **Rule 5:** Blocks all other traffic.

**Table 13-2: Internal Firewall Parameters**

| Parameter                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|-----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Source IP<br>[AccessList_Source_IP]     | Defines the IP address (or DNS name) or a specific host name of the source network (i.e., from where the incoming packet is received).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Source Port<br>[AccessList_Source_Port] | Defines the source UDP/TCP ports (of the remote host) from where packets are sent to the device.<br>The valid range is 0 to 65535.<br><b>Note:</b> When set to 0, this field is ignored and any source port matches the rule.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Prefix Length<br>[AccessList_PrefixLen] | <b>(Mandatory)</b> Defines the IP network mask - 32 for a single host or the appropriate value for the source IP addresses. <ul style="list-style-type: none"> <li>■ A value of 8 corresponds to IPv4 subnet class A (network mask of 255.0.0.0).</li> <li>■ A value of 16 corresponds to IPv4 subnet class B (network mask of 255.255.0.0).</li> <li>■ A value of 24 corresponds to IPv4 subnet class C (network mask of 255.255.255.0).</li> </ul> The IP address of the sender of the incoming packet is trimmed in accordance with the prefix length (in bits) and then compared to the parameter 'Source IP'.<br>The default is 0 (i.e., applies to all packets). You <b>must</b> change this value to any of the above options.<br><b>Note:</b> A value of 0 applies to <b>all</b> packets, regardless of the defined IP address. Therefore, you must set this parameter to a value other than 0. |



| Parameter                                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Start Port<br>[AccessList_Start_Port]                         | <p>Defines the destination UDP/TCP start port (on this device) to where packets are sent.</p> <p>The valid range is 0 to 65535.</p> <p><b>Note:</b> When the protocol type isn't TCP or UDP, the entire range must be provided.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| End Port<br>[AccessList_End_Port]                             | <p>Defines the destination UDP/TCP end port (on this device) to where packets are sent.</p> <p>The valid range is 0 to 65535.</p> <p><b>Note:</b> When the protocol type isn't TCP or UDP, the entire range must be provided.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Protocol<br>[AccessList_Protocol]                             | <p>Defines the protocol type (e.g., UDP, TCP, ICMP, ESP or 'Any') or the IANA protocol number in the range of 0 (Any) to 255.</p> <p><b>Note:</b> This field also accepts the abbreviated strings 'SIP' and 'HTTP'. Specifying these strings implies selection of the TCP or UDP protocols, and the appropriate port numbers as defined on the device.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Use Specific Interface<br>[AccessList_Use_Specific_Interface] | <p>Determines whether you want to apply the rule to a specific network interface defined in the Multiple Interface table (i.e., packets received from that defined in the Source IP field and received on this network interface):</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ If enabled, then in the 'Interface Name' field (described below), select the interface to which the rule is applied.</li> <li>▪ If disabled, then the rule applies to all interfaces.</li> </ul>                                                                                                                                                                                     |
| Interface Name<br>[AccessList_Interface_ID]                   | <p>Defines the network interface to which you want to apply the rule. This is applicable if you enabled the 'Use Specific Interface' field. The list displays interface names as defined in the Multiple Interface table in "Configuring IP Network Interfaces" on page 90.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Packet Size<br>[AccessList_Packet_Size]                       | <p>Defines the maximum allowed packet size.</p> <p>The valid range is 0 to 65535.</p> <p><b>Note:</b> When filtering fragmented IP packets, this field relates to the overall (re-assembled) packet size, and not to the size of each fragment.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Byte Rate<br>[AccessList_Byte_Rate]                           | <p>Defines the expected traffic rate (bytes per second), i.e., the allowed bandwidth for the specified protocol. In addition to this field, the 'Burst Bytes' field provides additional allowance such that momentary bursts of data may utilize more than the defined byte rate, without being interrupted.</p> <p>For example, if 'Byte Rate' is set to 40000 and 'Burst Bytes' to 50000, then this implies the following: the allowed bandwidth is 40000 bytes/sec with extra allowance of 50000 bytes; if, for example, the actual traffic rate is 45000 bytes/sec, then this allowance would be consumed within 10 seconds, after which all traffic exceeding the allocated 40000 bytes/sec is dropped. If the actual traffic rate then slowed to 30000 bytes/sec, then the allowance would be</p> |



| Parameter                                    | Description                                                                                                                                                                                        |
|----------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                              | replenished within 5 seconds.                                                                                                                                                                      |
| Burst Bytes<br>[AccessList_Byte_Burst]       | Defines the tolerance of traffic rate limit (number of bytes).<br>The default is 0.                                                                                                                |
| Action Upon Match<br>[AccessList_Allow_Type] | Defines the firewall action to be performed upon rule match. <ul style="list-style-type: none"><li>▪ "Allow" = (Default) Permits these packets</li><li>▪ "Block" = Rejects these packets</li></ul> |
| Match Count<br>[AccessList_MatchCount]       | (Read-only) Displays the number of packets accepted or rejected by the rule.                                                                                                                       |



## 13.2 Configuring General Security Settings

The General Security Settings page is used to configure various security features. For a description of the parameters appearing on this page, refer "Configuration Parameters Reference" on page 387.

➤ **To configure the general security parameters:**

1. Open the General Security Settings page (**Configuration** tab > **VoIP** menu > **Security** submenu > **General Security Settings**).

|                                          |                         |   |
|------------------------------------------|-------------------------|---|
| ▼ IPsec Setting                          |                         |   |
| ⚡ Enable IP Security                     | Disable                 | ▼ |
| IKE Certificate Ext Validate             | Disable                 | ▼ |
| ▼ TLS Settings                           |                         |   |
| TLS Version                              | SSL 2.0-3.0 and TLS 1.0 | ▼ |
| Strict Certificate Extension Validation  | Disable                 | ▼ |
| ⚡ FIPS140 Mode                           | Disable                 | ▼ |
| Client Cipher String                     | ALL:!ADH                |   |
| ▼ SIP TLS Settings                       |                         |   |
| TLS Client Re-Handshake Interval         | 0                       |   |
| ⚡ TLS Mutual Authentication              | Disable                 | ▼ |
| Peer Host Name Verification Mode         | Disable                 | ▼ |
| TLS Client Verify Server Certificate     | Disable                 | ▼ |
| TLS Remote Subject Name                  |                         |   |
| ▼ OCSP Settings                          |                         |   |
| Enable OCSP Server                       | Disable                 | ▼ |
| Primary Server IP                        | 0.0.0.0                 |   |
| Secondary Server IP                      | 0.0.0.0                 |   |
| Server Port                              | 2560                    |   |
| Default Response When Server Unreachable | Reject                  | ▼ |

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, refer to "Saving Configuration" on page 308.



## 13.3 Intrusion Detection System

The device can be configured to detect malicious attacks on its system and send SNMP traps if malicious activity is identified. The Intrusion Detection System (IDS) is an important feature for Enterprises to ensure legitimate calls are not being adversely affected by attacks and to prevent Theft of Service and unauthorized access. If, for example, you identify the source (IP address) of the attack, you can add that source to your blacklist to prevent it from accessing your device.

There are many types of malicious attacks, the most common being:

- **Denial of service:** This can be Denial of Service (DoS) where an attacker wishing to prevent a server from functioning correctly directs a large amount of requests – sometimes meaningless and sometimes legitimate, or it can be Distributed Denial of Service (DDoS) where the attacker controls a large group of systems to coordinate a large scale DoS attack against a system:
  - Message payload tampering: Attacker may inject harmful content into a message, e.g., by entering meaningless or wrong information, with the goal of exploiting a buffer overflow at the target. Such messages can be used to probe for vulnerabilities at the target.
  - Message flow tampering: This is a special case of DoS attacks. These attacks disturb the ongoing communication between users. An attacker can then target the connection by injecting fake signaling messages into the communication channel (such as CANCEL messages).
  - Message Flooding: The most common DoS attack is where an attacker sends a huge amount of messages (e.g., INVITEs) to a target. The goal is to overwhelm the target's processing capabilities, thereby rendering the target inoperable.
- **SPAM over Internet Telephony (SPIT):** VoIP spam is unwanted, automatically dialed, pre-recorded phone calls using VoIP. It is similar to e-mail spam.
- **Theft of Service (ToS):** Service theft can be exemplified by phreaking, which is a type of hacking that steals service (i.e., free calls) from a service provider, or uses a service while passing the cost to another person.

The IDS configuration is based on IDS Policies, where each policy can be configured with a set of IDS rules. Each rule defines a type of malicious attack to detect and the number of attacks during an interval (threshold) before an SNMP trap is sent. Each policy is then applied to a target under attack (SIP interface) and/or source of attack (Proxy Set and/or subnet address).

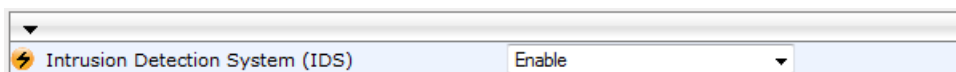
### 13.3.1 Enabling IDS

The procedure below describes how to enable IDS.

➤ **To enable IDS:**

1. Open the IDS Global Parameters page (**Configuration** tab > **VoIP** menu > **Security** > **Intrusion Detection and Prevention** > **Global Parameters**).

**Figure 13-2: Enabling IDS on IDS Global Parameters Page**



2. From the 'Intrusion Detection System' drop-down list, select **Enable**.
3. Reset the device with a burn-to-flash for the setting to take effect (see Saving Configuration).



## 13.3.2 Configuring IDS Policies

Configuring IDS policies is a two-stage process done in the following tables:

1. **IDS Policy table:** Defines a name and description for the policy. You can define up to 20 policies.
2. **IDS Rules table:** Defines the actual IDS rules per policy. Each policy can be configured with up to 20 rules.



**Note:** A maximum of 100 IDS rules can be configured (regardless of how many rules are assigned to each policy).

By default and for your convenience, the device provides three pre-configured IDS policies with rules that can be used in your deployment if they meet your requirements:

- "DEFAULT\_FEU": Policy for far-end users in the WAN
- "DEFAULT\_PROXY": Policy for proxy server
- "DEFAULT\_GLOBAL": Policy with global thresholds

These default policies are read-only.

### ➤ To configure IDS policies:

1. Open the IDS Policy Table page (**Configuration** tab > **VoIP** menu > **Security** > **Intrusion Detection and Prevention** > **Policy Table**).

**Figure 13-3: IDS Policy Table with Default Rules**

| Add + Edit ✎ Delete — Show/Hide ⌵                    |                |                                 |
|------------------------------------------------------|----------------|---------------------------------|
| Index                                                | Name           | Description                     |
| 0                                                    | DEFAULT_FEU    | Default policy for FEU          |
| 1                                                    | DEFAULT_PROXY  | Default policy for proxies      |
| 2                                                    | DEFAULT_GLOBAL | Default policy for global scope |
| Page 1 of 1 Show 10 records per page View 1 - 3 of 3 |                |                                 |
| IDS Policy Table #0 Additional Configuration         |                |                                 |
| <a href="#">IDS Rule Table</a>                       |                |                                 |

2. Add a Policy name:
  - a. Click **Add**.

**Figure 13-4: IDS Policy Table - Add Record**

Add Record ✕

Index

3

Name

SIP-Trunk

Description

for attacks from SIP Trunk

Submit

Cancel

- b. Configure the parameters as described in the following table, and then click **Submit**.



Table 13-3: IDS Policy Table Parameters

| Parameter                                    | Description                                                                                             |
|----------------------------------------------|---------------------------------------------------------------------------------------------------------|
| Index<br>CLI: policy<br>[IDSPolicy_Index]    | Defines the table row number for the policy.                                                            |
| Name<br>CLI: rule<br>[IDSPolicy_Description] | Defines a name for the policy.<br>The valid value is a string of up to 20 characters.                   |
| Description<br>[IDSPolicy_Name]              | Defines an arbitrary description of the policy.<br>The valid value is a string of up to 100 characters. |

3. Add rules to the policy:

- a. In the IDS Policy table, select the required policy and then click the **IDS Rule Table** link located below the table:

Figure 13-5: IDS Rule Table of Selected IDS Policy

The screenshot shows a web interface titled "IDS Rule Table". At the top, there are buttons for "Add +", "Edit", and "Delete", along with a "Show/Hide" button. Below these is a table with the following columns: Index, Reason, Threshold Scope, Threshold Window, Minor Alarm Threshold, Major Alarm Threshold, and Critical Alarm Threshold. The table contains five rows of data. Below the table, there is a "Selected Row #0" section that displays the details for the first row (Index 0): Reason: Connection abuse, Threshold Scope: IP, Threshold Window: 30, Minor Alarm Threshold: 5, Major Alarm Threshold: 0, and Critical Alarm Threshold: 0. The interface also includes pagination controls showing "Page 1 of 1" and "View 1 - 5 of 5".

| Index | Reason                   | Threshold Scope | Threshold Window | Minor Alarm Threshold | Major Alarm Threshold | Critical Alarm Threshold |
|-------|--------------------------|-----------------|------------------|-----------------------|-----------------------|--------------------------|
| 0     | Connection abuse         | IP              | 30               | 5                     | 0                     | 0                        |
| 1     | Malformed message        | IP              | 30               | 15                    | 0                     | 0                        |
| 2     | Authentication failure   | IP              | 600              | 20                    | 0                     | 0                        |
| 3     | Dialog establish failure | IP              | 300              | 30                    | 0                     | 0                        |
| 4     | Abnormal flow            | IP              | 30               | 15                    | 0                     | 0                        |

Selected Row #0

|                   |                  |                           |   |
|-------------------|------------------|---------------------------|---|
| Reason:           | Connection abuse | Minor-Alarm Threshold:    | 5 |
| Threshold Scope:  | IP               | Major-Alarm Threshold:    | 0 |
| Threshold Window: | 30               | Critical-Alarm Threshold: | 0 |

- b. Click **Add**.

Figure 13-6: IDS Rule Table - Add Record

The screenshot shows a "Add Record" form with the following fields and values: Index (0), Reason (Malformed message), Threshold Scope (IP), Threshold Window (30), Minor-Alarm Threshold (15), Major-Alarm Threshold (20), and Critical-Alarm Threshold (25). At the bottom right, there are "Submit" and "Cancel" buttons.

|                          |                   |
|--------------------------|-------------------|
| Index                    | 0                 |
| Reason                   | Malformed message |
| Threshold Scope          | IP                |
| Threshold Window         | 30                |
| Minor-Alarm Threshold    | 15                |
| Major-Alarm Threshold    | 20                |
| Critical-Alarm Threshold | 25                |

- c. Configure the parameters as required, and then click **Submit**. For a description of these parameters, see the table below. The figure above shows an example configuration where if 15 malformed SIP messages are received within a period of 30 seconds, a minor alarm is sent. Every 30 seconds, the rule's counters are cleared.
- d. To add more rules to the policy, repeat steps 1.b to 1.c.



Table 13-4: IDS Rule Table Parameters

| Parameter                                                                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|-------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Index<br>CLI: rule-id<br><b>[IDSRule_RuleID]</b>                                    | Defines the table row number for the rule.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Reason<br>CLI: reason<br><b>[IDSRule_Reason]</b>                                    | <p>Defines the type of intrusion attack (malicious event).</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Any = All events listed below are considered as attacks and are counted together.</li> <li>▪ <b>[1]</b> Connection abuse (default) = TLS authentication failure.</li> <li>▪ <b>[2]</b> Malformed message = <ul style="list-style-type: none"> <li>✓ Message exceeds a user-defined maximum message length (50K)</li> <li>✓ Any SIP parser error</li> <li>✓ Message Policy match (see Configuring SIP Message Policy Rules)</li> <li>✓ Basic headers not present</li> <li>✓ Content length header not present (for TCP)</li> <li>✓ Header overflow</li> </ul> </li> <li>▪ <b>[3]</b> Authentication failure = <ul style="list-style-type: none"> <li>✓ Local authentication ("Bad digest" errors)</li> <li>✓ Remote authentication (SIP 401/407 is sent if original message includes authentication)</li> </ul> </li> <li>▪ <b>[4]</b> Dialog establish failure = <ul style="list-style-type: none"> <li>✓ Classification failure (see Configuring Classification Rules)</li> <li>✓ Routing failure</li> <li>✓ Other local rejects (prior to SIP 180 response)</li> <li>✓ Remote rejects (prior to SIP 180 response)</li> </ul> </li> <li>▪ <b>[5]</b> Abnormal flow = <ul style="list-style-type: none"> <li>✓ Requests and responses without a matching transaction user (except ACK requests)</li> <li>✓ Requests and responses without a matching transaction (except ACK requests)</li> </ul> </li> </ul> |
| Threshold Scope<br>CLI: threshold-scope<br><b>[IDSRule_ThresholdScope]</b>          | <p>Defines the source of the attacker to consider in the device's detection count.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Global = All attacks regardless of source are counted together during the threshold window.</li> <li>▪ <b>[2]</b> IP = Attacks from each specific IP address are counted separately during the threshold window.</li> <li>▪ <b>[3]</b> IP+Port = Attacks from each specific IP address:port are counted separately during the threshold window. This option is useful for NAT servers, where numerous remote machines use the same IP address but different ports. However, it is not recommended to use this option as it may degrade detection capabilities.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Threshold Window<br>CLI: threshold-window<br><b>[IDSRule_ThresholdWindow]</b>       | <p>Defines the threshold interval (in seconds) during which the device counts the attacks to check if a threshold is crossed. The counter is automatically reset at the end of the interval.</p> <p>The valid range is 1 to 1,000,000. The default is 1.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Minor-Alarm Threshold<br>CLI: minor-alm-thr<br><b>[IDSRule_MinorAlarmThreshold]</b> | <p>Defines the threshold that if crossed a minor severity alarm is sent.</p> <p>The valid range is 1 to 1,000,000. A value of 0 or -1 means not defined.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |



| Parameter                                                                             | Description                                                                                                                                       |
|---------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------|
| Major-Alarm Threshold<br>CLI: major-alm-thr<br>[IDSRule_MajorAlarmThreshold]          | Defines the threshold that if crossed a major severity alarm is sent. The valid range is 1 to 1,000,000. A value of 0 or -1 means not defined.    |
| Critical-Alarm Threshold<br>CLI: critical-alm-thr<br>[IDSRule_CriticalAlarmThreshold] | Defines the threshold that if crossed a critical severity alarm is sent. The valid range is 1 to 1,000,000. A value of 0 or -1 means not defined. |

### 13.3.3 Assigning IDS Policies

The IDS Match table enables you to use your configured IDS policies. This is done by assigning them to any or a combination of the following entities:

- **SIP Interface:** Detects malicious attacks (according to specified IDS Policy) on specific SIP Interface(s)
- **Proxy Sets:** Detects malicious attacks (according to specified IDS Policy) from specified Proxy Set(s)
- **Subnet addresses:** Detects malicious attacks (according to specified IDS Policy) from specified subnet address

Up to 20 IDS policy-matching rules can be configured.

➤ **To assign an IDS policy:**

1. Open the IDS Match Table page (**Configuration** tab > **VoIP** menu > **Security** > **Intrusion Detection and Prevention** > **Match Table**).
2. Click **Add**.

**Figure 13-7: IDS Match Table - Add Record**

The figure above shows a configuration example where the IDS Policy, "SIP Trunk" is applied to SIP Interfaces 1 and 2, and all source IP addresses outside of subnet 10.1.0.0/16 and IP address 10.2.2.2.

3. Configure the IDS matching parameters. For a description of these parameters, see the following table.
4. Click **Submit**.

**Table 13-5: IDS Match Table Parameters**

| Parameter                 | Description                                |
|---------------------------|--------------------------------------------|
| Index<br>[IDSMATCH_Index] | Defines the table row number for the rule. |



| Parameter                                                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|-----------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SIP Interface<br>CLI: sip-interface<br><b>[IDSMatch_SIPInterface]</b> | <p>Defines the SIP Interface(s) to which you want to assign the IDS policy. This indicates the SIP Interfaces that are being attacked. The entered value must be the ID of the SIP Interface. The following syntax is supported:</p> <ul style="list-style-type: none"> <li>A comma-separated list of SIP Interface IDs (e.g., 1,3,4)</li> <li>A hyphen "-" indicates a range of SIP Interfaces (e.g., 3,4-7 means IDs 3, and 4 through 7)</li> <li>A prefix of an exclamation mark "!" means negation of the set (e.g., !3,4-7 means all indexes excluding 3, and excluding 4 through 7)</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| ProxySet<br>CLI: proxy-set<br><b>[IDSMatch_ProxySet]</b>              | <p>Defines the Proxy Set(s) to which the IDS policy is assigned. This indicates the Proxy Sets from where the attacks are coming from. The following syntax is supported:</p> <ul style="list-style-type: none"> <li>A comma-separated list of Proxy Set IDs (e.g., 1,3,4)</li> <li>A hyphen "-" indicates a range of Proxy Sets (e.g., 3,4-7 means IDs 3, and 4 through 7)</li> <li>A prefix of an exclamation mark "!" means negation of the set (e.g., !3,4-7 means all indexes excluding 3, and excluding 4 through 7)</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>Only the IP address of the Proxy Set is considered (not the port).</li> <li>If a Proxy Set has multiple IP addresses, the device considers the Proxy Set as one entity and includes all its IP addresses in the same IDS count.</li> </ul>                                                                                                                                                                                                                                                                                           |
| Subnet<br>CLI: subnet<br><b>[IDSMatch_Subnet]</b>                     | <p>Defines the subnet(s) to which the IDS policy is assigned. This indicates the subnets from where the attacks are coming from. The following syntax can be used:</p> <ul style="list-style-type: none"> <li>Basic syntax is a subnet in CIDR notation (e.g., 10.1.0.0/16 means all sources with IP address in the range 10.1.0.0–10.1.255.255)</li> <li>An IP address can be specified without the prefix length to refer to the specific IP address.</li> <li>Each subnet can be negated by prefixing it with "!", which means all IP addresses outside that subnet.</li> <li>Multiple subnets can be specified by separating them with "&amp;" (and) or " " (or) operations. For example: <ul style="list-style-type: none"> <li>✓ 10.1.0.0/16   10.2.2.2: includes subnet 10.1.0.0/16 and IP address 10.2.2.2.</li> <li>✓ !10.1.0.0/16 &amp; !10.2.2.2: includes all addresses except those of subnet 10.1.0.0/16 and IP address 10.2.2.2. Note that the exclamation mark "!" appears before each subnet.</li> <li>✓ 10.1.0.0/16 &amp; !10.1.1.1: includes subnet 10.1.0.0/16, except IP address 10.1.1.1.</li> </ul> </li> </ul> |
| Policy<br>CLI: policy<br><b>[IDSMatch_Policy]</b>                     | <p>Selects the IDS policy, configured in 'Configuring IDS Policies' on page <a href="#">122</a>.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |



### 13.3.4 Viewing IDS Alarms

The device uses SNMP (and Syslog) to notify the detection of malicious attacks. The trap displays the IDS Policy and Rule, and the Policy-Match index.

The device sends the SNMP alarm, `acIDSPolicyAlarm` whenever a threshold of a specific IDS Policy rule is crossed. For each scope that crosses this threshold, the device sends an additional SNMP event (trap) - `acIDSThresholdCrossNotification` - indicating the specific details (IP address or IP address:port). If the trap severity level is raised, the alarm of the former severity is cleared and the device then sends a new alarm with the new severity.

The SNMP alarm is cleared after a user-defined period (configured by the ini file parameter, `IDSAlarmClearPeriod`) during which no thresholds have been crossed. However, this "quiet" period must be at least twice the Threshold Window value (configured in 'Configuring IDS Policies' on page 122). For example, if `IDSAlarmClearPeriod` is set to 20 sec and the Threshold Window is set to 15 sec, the `IDSAlarmClearPeriod` parameter is ignored and the alarm is cleared only after 30 seconds (2 x 15 sec).

The figure below shows an example of IDS alarms in the Active Alarms table (Viewing Active Alarms), where a minor threshold alarm is cleared and replaced by a major threshold alarm:

**Figure 13-8: IDS Alarms in Active Alarms Table**

|    |         |                              |                                                                                         |                      |
|----|---------|------------------------------|-----------------------------------------------------------------------------------------|----------------------|
| 17 | Minor   | Board#1/IDSMATCH#2/IDSRULE#0 | Policy 2 (Proxy): minor threshold (5) of signaling-msg cross in ip scope                | 24.10.2012 , 9:48:53 |
| 18 | cleared | Board#1/IDSMATCH#2/IDSRULE#0 | Alarm cleared: Policy 2 (Proxy): minor threshold (5) of signaling-msg cross in ip scope | 24.10.2012 , 9:48:53 |
| 19 | Major   | Board#1/IDSMATCH#2/IDSRULE#0 | Policy 2 (Proxy): major threshold (10) of signaling-msg cross in ip scope               | 24.10.2012 , 9:48:53 |

You can also view the IDS alarms in the CLI:

- To view active IDS alarms:  

```
show voip security ids active-alarm all
```
- To view all IP addresses that crossed the threshold for an active IDS alarm:  

```
show voip security ids active-alarm match * rule *
```

The device also sends IDS notifications in Syslog messages to a Syslog server (if enabled - see Configuring Syslog). The table below shows the Syslog text message per malicious event:

**Table 13-6: Types of Malicious Events and Syslog Text String**

| Type                      | Description                                                                                                                                                                                                                                                                                            | Syslog String                                                                                                                                                                                                                                                  |
|---------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Connection Abuse</b>   | TLS authentication failure                                                                                                                                                                                                                                                                             | abuse-tls-auth-fail                                                                                                                                                                                                                                            |
| <b>Malformed Messages</b> | <ul style="list-style-type: none"> <li>▪ Message exceeds a user-defined maximum message length (50K)</li> <li>▪ Any SIP parser error</li> <li>▪ Message policy match</li> <li>▪ Basic headers not present</li> <li>▪ Content length header not present (for TCP)</li> <li>▪ Header overflow</li> </ul> | <ul style="list-style-type: none"> <li>▪ malformed-invalid-msg-len</li> <li>▪ malformed-parse-error</li> <li>▪ malformed-message-policy</li> <li>▪ malformed-miss-header</li> <li>▪ malformed-miss-content-len</li> <li>▪ malformed-header-overflow</li> </ul> |
| <b>Authentication</b>     | <ul style="list-style-type: none"> <li>▪ Local authentication ("Bad digest" errors)</li> </ul>                                                                                                                                                                                                         | <ul style="list-style-type: none"> <li>▪ auth-establish-fail</li> </ul>                                                                                                                                                                                        |



| Type                                | Description                                                                                                                                                                                                             | Syslog String                                                                                                                                                            |
|-------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Failure</b>                      | <ul style="list-style-type: none"> <li>Remote authentication (SIP 401/407 is sent if original message includes authentication)</li> </ul>                                                                               | <ul style="list-style-type: none"> <li>auth-reject-response</li> </ul>                                                                                                   |
| <b>Dialog Establishment Failure</b> | <ul style="list-style-type: none"> <li>Classification failure</li> <li>Routing failure</li> <li>Other local rejects (prior to SIP 180 response)</li> <li>Remote rejects (prior to SIP 180 response)</li> </ul>          | <ul style="list-style-type: none"> <li>establish-classify-fail</li> <li>establish-route-fail</li> <li>establish-local-reject</li> <li>establish-remote-reject</li> </ul> |
| <b>Abnormal Flow</b>                | <ul style="list-style-type: none"> <li>Requests and responses without a matching transaction user (except ACK requests)</li> <li>Requests and responses without a matching transaction (except ACK requests)</li> </ul> | <ul style="list-style-type: none"> <li>flow-no-match-tu</li> <li>flow-no-match-transaction</li> </ul>                                                                    |



## 14 Media

This section describes the media-related configuration.

### 14.1 Configuring RTP/RTCP Settings

This section describes configuration relating to Real-Time Transport Protocol (RTP) and RTP Control Protocol (RTCP).

#### 14.1.1 Configuring RTP Base UDP Port

You can configure the range of UDP ports for RTP, RTCP, and T.38. The UDP port range can be configured using media realms in the Media Realm table, allowing you to assign different port ranges (media realms) to different interfaces. However, if you do not use media realms, you can configure the lower boundary of the UDP port used for RTP, RTCP (RTP port + 1) and T.38 (RTP port + 2), using the 'RTP Base UDP Port' (BaseUDPPort) parameter. For example, if the BaseUDPPort is set to 6000, then one channel may use the ports RTP 6000, RTCP 6001, and T.38 6002, while another channel may use RTP 6010, RTCP 6011, and T.38 6012.

The range of possible UDP ports is 6,000 to 64,000 (default base UDP port is 6000). The port range is calculated using the BaseUDPPort parameter as follows: **BaseUDPPort to (BaseUDPPort + <channels -1> \* 10)**

The default local UDP ports for audio and fax media streams is calculated using the following formula: **BaseUDPPort + (Channel ID \* 10) + Port Offset**

Where the port offsets are as follows:

- **Audio RTP:** 0
- **Audio RTCP:** 1
- **Fax T.38:** 2

For example, the local T.38 UDP port for channel 30 is calculated as follows: **6000 + (30\*10) + 2 = 6302**

The maximum (when all channels are required) UDP port range is calculated as follows:

- BaseUDPPort to (BaseUDPPort + 4000\*10)



#### Notes:

- The device allocates the UDP ports randomly to the channels.
- To configure the device to use the same port for both RTP and T.38 packets, set the T38UseRTPPort parameter to 1.
- If you are using Media Realms (see "Configuring Media Realms" on page 130), the port range configured for the Media Realm must be within this range defined by the BaseUDPPort parameter.



The procedure below describes how to configure the RTP base UDP port using the Web interface.

➤ **To configure the RTP base UDP port:**

1. Open the RTP/RTCP Settings page (**Configuration** tab > **VoIP** menu > **Media** submenu > **RTP/RTCP Settings**). The relevant parameter is listed under the 'General Settings' group, as shown below:

**Figure 14-1: RTP Based UDP Port in RTP/RTCP Settings Page**

|                                                                                                     |                                   |
|-----------------------------------------------------------------------------------------------------|-----------------------------------|
|  RTP Base UDP Port | <input type="text" value="6000"/> |
|-----------------------------------------------------------------------------------------------------|-----------------------------------|

2. Set the 'RTP Base UDP Port' parameter to the required value.
3. Click **Submit**.
4. Reset the device for the settings to take effect.

## 14.2 Configuring Media Realms

The Media Realm Table page allows you to define a pool of up to 64 SIP media interfaces, termed *Media Realms*. Media Realms allow you to divide a Media-type interface, which is configured in the Multiple Interface table, into several realms, where each realm is specified by a UDP port range. You can also define the maximum number of sessions per Media Realm. Once configured, Media Realms can be assigned to IP Groups (see "Configuring IP Groups" on page 164) or SRDs (see "Configuring SRD Table" on page 159).

Once you have configured a Media Realm, you can configure it with the following:

- Quality of Experience parameters for reporting to AudioCodes SEM server used for monitoring the quality of calls (see Configuring Quality of Experience Parameters per Media Realm on page 132)
- Bandwidth management (see "Configuring Bandwidth Management per Media Realm" on page 135)



**Notes:**

- If different Media Realms are assigned to an IP Group and to an SRD, the IP Group's Media Realm takes precedence.
- For this setting to take effect, a device reset is required.
- The Media Realm table can also be configured using the table ini file parameter, CpMediaRealm.



➤ **To define a Media Realm:**

1. Open the Media Realm Table page (**Configuration** tab > **VoIP** menu > **Media** submenu > **Media Realm Configuration**).
2. Click the **Add** button; the following appears:

**Figure 14-2: Media Realm Page - Add Record Dialog Box**

3. Configure the parameters as required. See the table below for a description of each parameter
4. Click **Submit** to apply your settings.
5. Reset the device to save the changes to flash memory (see "Saving Configuration" on page 308).

**Table 14-1: Media Realm Table Parameter Descriptions**

| Parameter                                         | Description                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Index<br>[CpMediaRealm_Index]                     | Defines the required table index number.                                                                                                                                                                                                                                                                                                                    |
| Media Realm Name<br>[CpMediaRealm_MediaRealmName] | Defines an arbitrary, identifiable name for the Media Realm. The valid value is a string of up to 40 characters.<br><b>Notes:</b> <ul style="list-style-type: none"> <li>▪ This parameter is mandatory.</li> <li>▪ The name assigned to the Media Realm must be unique.</li> <li>▪ This Media Realm name is used in the SRD and IP Groups table.</li> </ul> |
| IPv4 Interface Name<br>[CpMediaRealm_IPv4IF]      | Assigns an IPv4 interface to the Media Realm. This is name of the interface as configured for the Interface Name field in the Multiple Interface table.                                                                                                                                                                                                     |
| IPv6 Interface Name<br>[CpMediaRealm_IPv6IF]      | Assigns an IPv6 interface to the Media Realm. This is name of the interface as configured for the Interface Name field in the Multiple Interface table.                                                                                                                                                                                                     |
| Port Range Start<br>[CpMediaRealm_PortRangeStart] | Defines the starting port for the range of Media interface UDP ports.<br><b>Notes:</b> <ul style="list-style-type: none"> <li>▪ You must either configure all media realms with port</li> </ul>                                                                                                                                                             |



| Parameter                                                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                | <p>ranges or all without; not some with and some without.</p> <ul style="list-style-type: none"> <li>The available UDP port range is calculated using the BaseUDPport parameter: <ul style="list-style-type: none"> <li>✓ BaseUDPport to BaseUDPport + 4000*10</li> </ul> </li> <li>Port ranges over 60,000 must not be used.</li> <li>Media Realms must not have overlapping port ranges.</li> </ul>                                                                                                                                                                                                                                            |
| Number of Media Session Legs<br>[CpMediaRealm_MediaSessionLeg] | Defines the number of media sessions associated with the range of ports. This is the number of media sessions available in the port range. For example, 100 ports correspond to 10 media sessions, since ports are allocated in chunks of 10.                                                                                                                                                                                                                                                                                                                                                                                                    |
| Port Range End<br>[CpMediaRealm_PortRangeEnd]                  | Read-only field displaying the ending port for the range of Media interface UDP ports. This field is calculated by adding the 'Media Session Leg' field (multiplied by the port chunk size) to the 'Port Range Start' field. A value appears once a row has been successfully added to the table.                                                                                                                                                                                                                                                                                                                                                |
| Is Default<br>[CpMediaRealm_IsDefault]                         | <p>Defines the Media Realm as the default Media Realm. This default Media Realm is used when no Media Realm is configured for an IP Group or SRD for a specific call.</p> <ul style="list-style-type: none"> <li>[0] No (default)</li> <li>[1] Yes</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter can be set to Yes for only <b>one</b> defined Media Realm.</li> <li>If this parameter is not configured, then the first Media Realm in the table is used as the default.</li> <li>If the table is not configured, then the default Media Realm includes all the configured media interfaces.</li> </ul> |

## 14.2.1 Configuring Quality of Experience per Media Realm

You can configure Quality of Experience (QoE) per Media Realm. This enables you to monitor and analyze media and signaling traffic, allowing you to detect problems causing service degradation. The device can save call information and statistics at call start, at call end, or at specific changes in the call. The information is stored as call records on an external server. The device connects, as a client, to the server using TLS over TCP.

You can specify the call parameters to monitor and configure their upper and lower thresholds. If these thresholds are exceeded, the device can be configured to do the following:

- Reports the change in the monitored parameter to the monitoring server (default).
- Sends RFC 2198 RTP redundancy packets on the call leg that crossed the threshold. This enables the device to adapt to the changed network status. In this option, you can also configure the redundancy depth. The channel configuration is unchanged if the change requires channel reopening. Currently, this option is applicable only when the monitored parameter is remote packet loss.

The device can be configured to monitor the following parameters on the local (i.e., at the device) or remote side:

- Packet loss
- Mean Opinion Score (MOS)
- Jitter



- Packet delay
- Residual Echo Return Loss (RERL)

At any given time during a call, each of these parameters can be in one of the following states according to its value in the last RTCP / RTCP XR packet:

- Gray - indicates that the value is unknown
- Green - indicates good call quality
- Yellow - indicates medium call quality
- Red - indicates poor call quality

The mapping between the values of the parameters and the color is according to the configured threshold of these parameters, per Media Realm. The call itself also has a state (color), which is the worst-state color of all the monitored parameters. Each time a color of a parameter changes, the device sends a report to the external server. A report is also sent at the end of each call.



**Notes:**

- The QoE feature is available only if the device is installed with the relevant Software License Key.
- To configure the address of the AudioCodes Session Experience Manager (SEM) server to where the device reports the QoE, see "Configuring SEM Server for Media Quality of Experience" on page 137.
- You can also configure QoE per Media Realm using the table *ini* file parameter QOERules.

➤ **To configure QoE per Media Realm:**

1. Open the Media Realm Table page (**Configuration** tab > **VoIP** menu > **Media** submenu > **Media Realm Configuration**).
2. Select the Media Realm for which you want to configure Quality of Experience, and then click the **Quality Of Experience** link; the Quality Of Experience page appears.
3. Click the **Add** button; the following dialog box appears:

**Figure 14-3: Quality of Experience Page - Add Record Dialog Box**

| Add Record                                                                               |                 |
|------------------------------------------------------------------------------------------|-----------------|
| Index                                                                                    | 1               |
| Monitored Parameter                                                                      | MOS             |
| Direction                                                                                | Device Side     |
| Profile                                                                                  | Low Sensitivity |
| Green Yellow Threshold                                                                   | 3.4             |
| Green Yellow Hysteresis                                                                  | 0.1             |
| Yellow Red Threshold                                                                     | 2.7             |
| Yellow Red Hysteresis                                                                    | 0.1             |
| Green Yellow Operation                                                                   | Notify          |
| Green Yellow Operation Details                                                           | 1               |
| Yellow Red Operation                                                                     | Notify          |
| Yellow Red Operation Details                                                             | 1               |
| <div> <input type="button" value="Submit"/> <input type="button" value="Cancel"/> </div> |                 |



The figure above shows value thresholds for the MOS parameter, which are assigned using pre-configured values of the Low Sensitivity profile. In this example setting, if the MOS value changes by 0.1 (hysteresis) to 3.3 or 3.5, the device sends a report to the SEM indicating this change. If the value changes to 3.3, it sends a yellow state (i.e., medium quality); if the value changes to 3.5, it sends a green state.

4. Configure the parameters as required. See the table below for a description of each parameter.
5. Click **Submit** to apply your settings.

**Table 14-2: Quality of Experience Parameter Descriptions**

| Parameter                                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|-------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Index<br>[QOERules_RuleIndex]                               | Defines the table index entry. Up to four table row entries can be configured per Media Realm.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Monitored Parameter<br>[QOERules_MonitoredParam]            | Defines the parameter to monitor and report. <ul style="list-style-type: none"> <li>▪ [0] MOS (default)</li> <li>▪ [1] Delay</li> <li>▪ [2] Packet Loss</li> <li>▪ [3] Jitter</li> <li>▪ [4] RERL</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Direction<br>[QOERules_Direction]                           | Defines the monitoring direction. <ul style="list-style-type: none"> <li>▪ [0] Device Side (default)</li> <li>▪ [1] Remote Side</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Profile<br>[QOERules_Profile]                               | Defines the pre-configured threshold profile to use. <ul style="list-style-type: none"> <li>▪ [0] No Profile = No profile is used and you need to define the thresholds in the parameters described below.</li> <li>▪ [1] Low Sensitivity = Automatically sets the thresholds to low sensitivity values. Therefore, reporting is done only if changes in parameters' values is significant.</li> <li>▪ [2] Default Sensitivity = Automatically sets the thresholds to a medium sensitivity.</li> <li>▪ [3] High Sensitivity = Automatically sets the thresholds to high sensitivity values. Therefore, reporting is done for small fluctuations in parameters' values.</li> </ul> |
| Green Yellow Threshold<br>[QOERules_GreenYellowThreshold]   | Defines the parameter threshold values between green (good quality) and yellow (medium quality) states.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Green Yellow Hysteresis<br>[QOERules_GreenYellowHysteresis] | Defines the hysteresis (fluctuation) for the green-yellow threshold. When the threshold is exceeded by this hysteresis value, the device sends a report to the SEM indicating this change.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Yellow Red Threshold<br>[QOERules_YellowRedThreshold]       | Defines the parameter threshold values between yellow (medium quality) and red (poor quality). When this threshold is exceeded, the device sends a report to the SEM indicating this change.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
| Yellow Red Hysteresis<br>[QOERules_YellowRedHysteresis]     | Defines the hysteresis (fluctuation) for the yellow-red threshold. When the threshold is exceeded by this hysteresis value, the device sends a report to the SEM indicating this change.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |



| Parameter                                                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Green Yellow Operation<br>[QOERules_GreenYellowOperation]                | <p>Defines the action that is done if the green-yellow threshold is crossed.</p> <ul style="list-style-type: none"> <li>▪ [1] Notify = (Default) Device sends a report to the SEM server.</li> <li>▪ [2] Activate 2198 = RTP redundancy packets are sent to the relevant call leg.</li> </ul> <p><b>Note:</b> This field is applicable only if the monitored parameter is remote packet loss.</p>                                                              |
| Green Yellow Operation Details<br>[QOERules_GreenYellowOperationDetails] | <p><b>Note:</b> This field is currently not supported.</p> <p>Defines the desired RTP redundancy depth. The actual redundancy depth on the relevant call leg is the minimum between the desired depth and the maximum supported depth on that call leg.</p> <p><b>Note:</b> This field is applicable only if the 'Green Yellow Operation' field is set to <b>Activate 2198</b>.</p>                                                                            |
| Yellow Red Operation<br>[QOERules_YellowRedOperation]                    | <p><b>Note:</b> This field is currently not supported.</p> <p>Defines the action that is done if the yellow-red threshold is crossed.</p> <ul style="list-style-type: none"> <li>▪ [1] Notify = (Default) Device sends a report to the SEM server.</li> <li>▪ [2] Activate 2198 = RTP redundancy packets are sent to the relevant call leg.</li> <li>▪ <b>Note:</b> This field is applicable only if the monitored parameter is remote packet loss.</li> </ul> |
| Yellow Red Operation Details<br>[QOERules_YellowRedOperationDetails]     | <p><b>Note:</b> This field is currently not supported.</p> <p>Defines the desired RTP redundancy depth. The actual redundancy depth on the relevant call leg is the minimum between the desired depth and the maximum supported depth on that call leg.</p> <p><b>Note:</b> This field is applicable only if the 'Yellow Red Operation' field is set to <b>Activate 2198</b>.</p>                                                                              |

## 14.2.2 Configuring Bandwidth Management per Media Realm

Bandwidth management enables you to configure bandwidth utilization thresholds per Media Realm which when exceeded, the device can do one of the following:

- Generate an appropriate SNMP alarm, which is cleared when the bandwidth utilization returns to normal.
- Block any additional calls on the Media Realm.

Bandwidth management includes the following bandwidth utilization states:

- Normal
- High threshold
- Critical threshold

When a transition occurs between two bandwidth threshold states, based on threshold and hysteresis values, the device executes the configured action. The transition possibilities include Normal-High threshold state changes and High-Critical threshold state changes. Thus, up to two thresholds can be configured per Media Realm; one for each state transition.



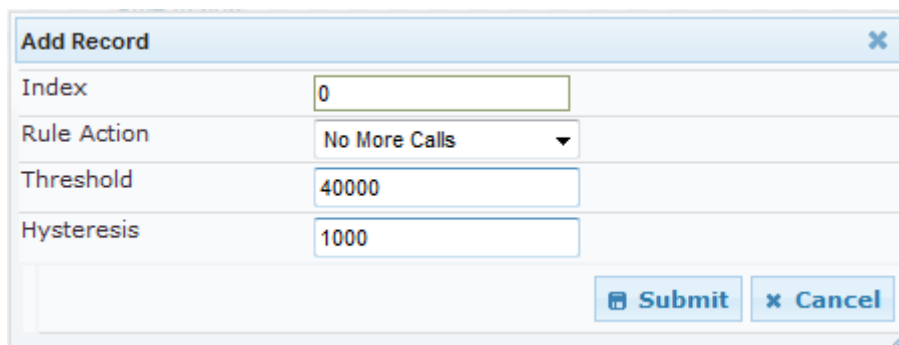

**Notes:**

- This feature is available only if the device is installed with the relevant Software License Key.
- For your bandwidth management settings to take effect, you must reset the device.
- You can also use the BWManagement *ini* file parameter to configure bandwidth management per Media Realm.

➤ **To configure bandwidth management rules per Media Realm:**

1. Open the Media Realm Table page (**Configuration** tab > **VoIP** menu > **Media** submenu > **Media Realm Configuration**).
2. Select the Media Realm for which you want to configure bandwidth management rules, and then click the **Bandwidth Management** link; the Bandwidth Management page appears.
3. Click the **Add** button; the following dialog box appears:

**Figure 14-4: Bandwidth Management Page - Add record Dialog Box**



The figure above shows an example where if the bandwidth for this Media Realm reaches 41,000 Bps (i.e., 40,000 plus 1,000 hysteresis), the device blocks any additional calls. If the bandwidth later decreases to 39,000 Bps (i.e., 40,000 minus 1,000 hysteresis), the device allows additional calls.

4. Configure the parameters as required. See the table below for a description of each parameter.
5. Click **Submit** to apply your settings.
6. Reset the device for your settings to take effect.

**Table 14-3: Bandwidth Management Parameter Descriptions**

| Parameter                                       | Description                                                                                                                                                                                                                                 |
|-------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Index<br><b>BWManagement_ThresholdIndex]</b>    | Defines the index of the table row entry. This index determines the bandwidth threshold type for the rule: <ul style="list-style-type: none"> <li>▪ <b>[0]</b> High Threshold Rule</li> <li>▪ <b>[1]</b> Critical Threshold Rule</li> </ul> |
| Rule Action<br><b>[BWManagement_RuleAction]</b> | Defines the action that the device performs when the configured threshold is exceeded: <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Report Only (default)</li> <li>▪ <b>[1]</b> No more calls</li> </ul>                             |
| Threshold<br><b>[BWManagement_Threshold]</b>    | Defines the bandwidth threshold in bytes per second (Bps). The default is 0.                                                                                                                                                                |



| Parameter                               | Description                                                                                                                                  |
|-----------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------|
| Hysteresis<br>[BWManagement_Hysteresis] | Defines the bandwidth fluctuation (change) from the threshold value at which the device performs the configured action.<br>The default is 0. |

## 14.3 Configuring Server for Media Quality of Experience

The device can be configured to report voice (media) quality of experience to AudioCodes Session Experience Manager (SEM) server, a plug-in for AudioCodes EMS. The reports include real-time metrics of the quality of the actual call experience and processed by the SEM.



### Notes:

- To support this feature, the device must be installed with the relevant Software License Key.
- To configure the parameters to report and their thresholds per Media Realm, see "Configuring Quality of Experience per Media Realm" on page 132.
- For information on the SEM server, refer to the *EMS User's Manual*.

### ➤ To configure QoE reporting of media:

1. Open the Media Quality of Experience page (**Configuration** tab > **VoIP** menu > **Media** submenu > **Media Quality of Experience**).

**Figure 14-5: Media Quality of Experience Page**

| Quality of Experience |              |
|-----------------------|--------------|
| ⚡ Server Ip           | 0.0.0.0      |
| Port                  | 5000         |
| ⚡ Interface Name      | DEFAULT      |
| Connection Mode       | VQMClient ▼  |
| Information Level     | VQStandard ▼ |
| Use Mos LQ            | Disable ▼    |

2. Configure the parameters as required
  - 'Server Ip' (QOEServerIP) - defines the IP address of the SEM server
  - 'Port' (QOEPort) - defines the port of the SEM server
  - 'Interface Name' (QOEInterfaceName) - defines the device's IP network interface on which the SEM reports are sent
  - 'Use Mos LQ' (QOEUseMosLQ) - defines the reported MOS type (listening or conversational)
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 308.



## 14.4 Configuring Media Security

The device supports Secured RTP (SRTP) according to RFC 3711. SRTP is used to encrypt RTP and RTCP transport for protecting VoIP traffic. SRTP requires a key exchange mechanism that is performed according to RFC 4568 – “Session Description Protocol (SDP) Security Descriptions for Media Streams”. The key exchange is done by adding a 'crypto' attribute to the SDP. This attribute is used (by both sides) to declare the various supported cipher suites and to attach the encryption key. If negotiation of the encryption data is successful, the call is established.

SRTP supports the following cipher suites (all other suites are ignored):

- AES\_CM\_128\_HMAC\_SHA1\_32
- AES\_CM\_128\_HMAC\_SHA1\_80

When the device is the offering side, it generates an MKI of a size configured by the 'Master Key Identifier (MKI) Size' parameter. The length of the MKI is limited to four bytes. If the remote side sends a longer MKI, the key is ignored. The key lifetime field is not supported. However, if it is included in the key it is ignored and the call does not fail.

The device supports the following session parameters (as defined in RFC 4568, SDP Security Descriptions for Media Streams):

- UNENCRYPTED\_SRTP
- UNENCRYPTED\_SRTCP
- UNAUTHENTICATED\_SRTP

Session parameters should be the same for the local and remote sides. When the device is the offering side, the session parameters are configured by the following parameter - 'Authentication On Transmitted RTP Packets', 'Encryption On Transmitted RTP Packets, and 'Encryption On Transmitted RTCP Packets'. When the device is the answering side, the device adjusts these parameters according to the remote offering. Unsupported session parameters are ignored, and do not cause a call failure.

Below is an example of crypto attributes usage:

```
a=crypto:1 AES_CM_128_HMAC_SHA1_80
inline:PsKoMpHlCg+b5X0YLuSvNrImEh/dAe
a=crypto:2 AES_CM_128_HMAC_SHA1_32
inline:IsPtLoGkBf9a+c6XVzRuMqHlDnEiAd
```

The device also supports symmetric MKI negotiation, whereby it can be configured to forward the MKI size received in the SDP offer crypto line in the SDP answer crypto line.

To configure the device's mode of operation if negotiation of the cipher suite fails, use the 'Media Security Behavior' parameter. This parameter can be set to enforce SRTP, whereby incoming calls that don't include encryption information are rejected.



### Notes:

- For a detailed description of the SRTP parameters, see SRTP Parameters on page 409.
- When SRTP is used, the channel capacity may be reduced.



➤ **To configure media security:**

1. Open the Media Security page (**Configuration** tab > **VoIP** menu > **Media** submenu > **Media Security**).

|                                           |                                     |
|-------------------------------------------|-------------------------------------|
| ▼ General Media Security Settings         |                                     |
| ⚡ Media Security                          | Disable ▼                           |
| Media Security Behavior                   | Preferable ▼                        |
| Authentication On Transmitted RTP Packets | Active ▼                            |
| Encryption On Transmitted RTP Packets     | Active ▼                            |
| Encryption On Transmitted RTCP Packets    | Active ▼                            |
| ▼ SRTP Setting                            |                                     |
| Master Key Identifier (MKI) Size          | 0                                   |
| Enable symmetric MKI negotiation          | Disable ▼                           |
| ◆ SRTP offered Suites                     |                                     |
| CIPHER SUITES AES CM 128 HMAC SHA1 80     | <input checked="" type="checkbox"/> |
| CIPHER SUITES AES CM 128 HMAC SHA1 32     | <input checked="" type="checkbox"/> |
| CIPHER SUITES ARIA CM 128 HMAC SHA1 80    | <input checked="" type="checkbox"/> |
| CIPHER SUITES ARIA CM 192 HMAC SHA1 80    | <input checked="" type="checkbox"/> |

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 308.



## Reader's Notes



## 15 Services

This section describes configuration for various supported services.

### 15.1 Routing Based on LDAP Active Directory Queries

The device supports Lightweight Directory Access Protocol (LDAP), enabling call routing decisions based on information stored on a third-party LDAP server (or Microsoft's Active Directory™ enterprise directory server). This feature enables the usage of a single common, popular database to manage and maintain information regarding user's availability, presence, and location.

#### 15.1.1 Configuring the LDAP Server

The basic LDAP mechanism is described below:

- **Connection:** The device connects and binds to the remote LDAP server either during the service's initialization (at device start-up) or whenever the LDAP server's IP address and port is changed. Service makes 10 attempts to connect and bind to the remote LDAP server with a timeout of 20 seconds between attempts. If connection fails, the service remains in disconnected state until either the LDAP server's IP address or port is changed.

If connection to the LDAP server later fails, the service attempts to reconnect, as described previously. The SNMP alarm `acLDAPLostConnection` is sent when connection is broken. Upon successful reconnection, the alarm is cleared.

Binding to the LDAP server can be anonymous or not. For anonymous binding, the `LDAPBindDN` and `LDAPPassword` parameters must not be defined or set to an empty string.

The address of the LDAP server can be a DNS name / FQDN configured by the `LDAPServerDomainName` parameter, or an IP address configured by the `LDAPServerIP` parameter.



**Note:** If you configure an FQDN, make sure that the `LDAPServerIP` parameter is left empty.

- **Search:** For the device to run a search using the LDAP service, the path to the directory's subtree (or DN) where the search is to be done must be configured using the `LDAPSearchDN` parameter. Up to three DNs can be configured. The search key, or *filter* in LDAP references, which defines the exact DN to be found and one or more attributes whose values should be returned, must also be defined.

If connection to the LDAP server is disrupted during the search, all search requests are dropped and an alarm indicating a failed status is sent to client applications.

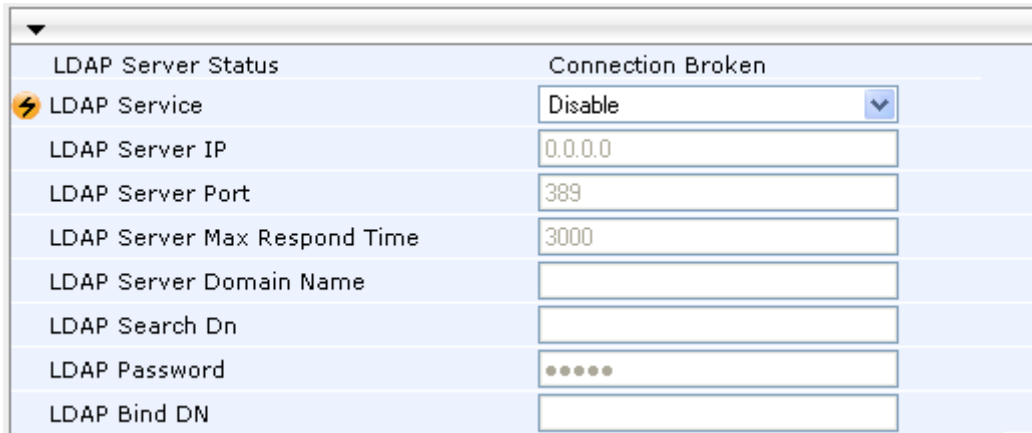
The LDAP Settings page is used for configuring the LDAP server parameters. For a full description of these parameters, see "Configuration Parameters Reference" on page [387](#).



➤ **To configure the LDAP server parameters:**

1. Open the LDAP Settings page (**Configuration** tab > **VoIP** menu > **Services** submenu > **LDAP Settings**).

**Figure 15-1: LDAP Settings Page**



|                              |                   |
|------------------------------|-------------------|
| LDAP Server Status           | Connection Broken |
| ⚡ LDAP Service               | Disable           |
| LDAP Server IP               | 0.0.0.0           |
| LDAP Server Port             | 389               |
| LDAP Server Max Respond Time | 3000              |
| LDAP Server Domain Name      |                   |
| LDAP Search Dn               |                   |
| LDAP Password                | •••••             |
| LDAP Bind DN                 |                   |

The read-only 'LDAP Server Status' field displays one of the following possibilities:

- "Not Applicable"
  - "Connection Broken"
  - "Connecting"
  - "Connected"
2. Configure the parameters as required.
  3. Click **Submit** to apply your changes.
  4. To save the changes to flash memory, see "Saving Configuration" on page 308.

## 15.1.2 Configuring the Device's LDAP Cache

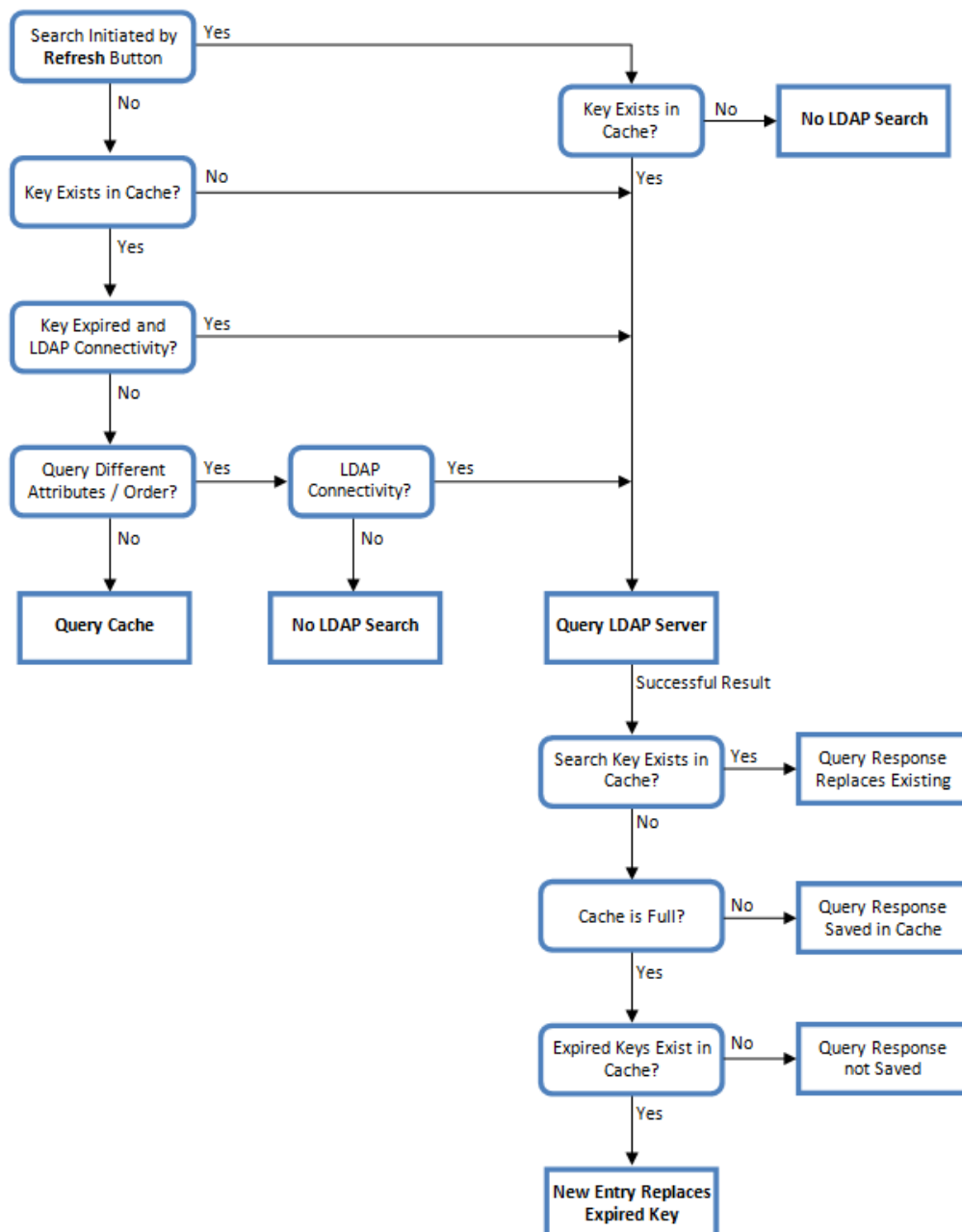
The device provides an option for storing recent LDAP queries and responses in its local cache. The cache is used for subsequent queries and/or in case of LDAP server failure. The advantage of enabling this feature includes the following:

- Improves routing decision performance by using local cache for subsequent LDAP queries
- Reduces number of queries performed on an LDAP server and corresponding bandwidth consumption
- Provides partial survivability in case of intermittent LDAP server failure (or network isolation)



The handling of LDAP queries with the LDAP cache is shown in the flowchart below:

**Figure 15-2: LDAP Query Process with Local LDAP Cache**



The LDAP Settings page is used for configuring the LDAP cache parameters.



**Notes:**

- The LDAP cache parameters are available only if you have enabled the LDAP service (see "Configuring the LDAP Server" on page 141).
- If on the first LDAP query, the result fails for at least one attribute and is successful for at least one, the partial result is cached. However, for subsequent queries, the device does not use the partially cached result, but does a new query with the LDAP server again.
- For a full description of the cache parameters, see "Configuration Parameters Reference" on page 387.



➤ **To configure the LDAP cache parameters:**

1. Open the LDAP Settings page (**Configuration** tab > **VoIP** menu > **Services** submenu > **LDAP Settings**).

**Figure 15-3: LDAP Settings Page - Cache Parameters**

|                                  |                                          |
|----------------------------------|------------------------------------------|
| LDAP Cache                       |                                          |
| LDAP Cache Service               | Enable                                   |
| LDAP Cache Entry Timeout         | 1200                                     |
| LDAP Cache Entry Removal Timeout | 0                                        |
| LDAP Cache Actions               |                                          |
| LDAP Refresh Cache By Key        | <input type="text"/>                     |
|                                  | <input type="button" value="Refresh"/>   |
| LDAP Clear All Cache             | <input type="button" value="Clear All"/> |

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 308.

The LDAP Settings page also provides you with the following buttons:

- **LDAP Refresh Cache By Key:** Refreshes a saved LDAP entry response in the cache of a specified LDAP search key. If a request with the specified key exists in the cache, the request is resent to the LDAP server.
- **LDAP Clear All Cache:** Removes all LDAP entries in the cache.

### 15.1.3 Active Directory based Tel-to-IP Routing for Microsoft Lync

Typically, enterprises wishing to deploy Microsoft® Lync™ Server 2010 (formerly known as Office Communication Server 2007) are faced with a complex, call routing dial plan when migrating users from their existing PBX or IP PBX to the Lync Server 2010 platform. As more and more end-users migrate to the new voice system, dialing plan management and PBX link capacity can be adversely impacted. To resolve this issue, enterprises can employ Microsoft's Active Directory (AD), which provides a central database to manage and maintain information regarding user's availability, presence, and location.

The device supports Tel-to-IP call routing decisions based on information stored on the AD. Based on queries sent to the AD, the device can route the Tel call to one of the following IP domains:

- Lync client (formally OCS) - users connected to Lync Server 2010 through the Mediation Server
- PBX or IP PBX - users not yet migrated to Lync Server 2010
- Mobile - mobile number
- Private - private telephone line for Lync users (in addition to the primary telephone line)

#### 15.1.3.1 Querying the AD and Routing Priority

The device queries the AD using the initial destination number (i.e., called number). The query can return up to four user phone numbers, each pertaining to one of the IP domains (i.e., private number, Lync / OCS number, PBX / IP PBX number, and mobile number). The configuration parameters listed in the table below are used to configure the query attribute keys that defines the AD attribute that you wish to query in the AD:



Table 15-1: Parameters for Configuring Query Attribute Key

| Parameter                            | Queried User Domain (Attribute) in AD                                                                                    | Query or Query Result Example        |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------|--------------------------------------|
| <b>MSLDAPPBXNumAttributeName</b>     | PBX or IP PBX number (e.g., "telephoneNumber" - default)                                                                 | telephoneNumber=+3233554447          |
| <b>MSLDAPOCSNumAttributeName</b>     | Mediation Server / Lync client number (e.g., "msRTCSIP-line")                                                            | msRTCSIP-line=john.smith@company.com |
| <b>MSLDAPMobileNumAttributeName</b>  | Mobile number (e.g., "mobile")                                                                                           | mobile=+3247647156                   |
| <b>MSLDAPPrivateNumAttributeName</b> | Any attribute (e.g., "msRTCSIP-PrivateLine")<br><b>Note:</b> Used only if set to same value as Primary or Secondary key. | msRTCSIP-PrivateLine=+3233554480     |
| <b>MSLDAPPrimaryKey</b>              | Primary Key query search instead of PBX key - can be any AD attribute                                                    | msRTCSIP-PrivateLine=+3233554480     |
| <b>MSLDAPSecondaryKey</b>            | Secondary Key query key search if Primary Key fails - can be any attribute                                               | -                                    |

The process for querying the AD and subsequent routing based on the query results is as follows:

1. If the Primary Key is configured, it uses the defined string as a primary key instead of the one defined in MSLDAPPBXNumAttributeName. It requests the attributes which are described below.
2. If the primary query is not found in the AD and the Secondary Key is configured, it does a second query for the destination number using a second AD attribute key name, configured by the MSLDAPSecondaryKey parameter.
3. If none of the queries are successful, it routes the call to the original dialed destination number according to the routing rule matching the "LDAP\_ERR" destination prefix number value, or rejects the call with a SIP 404 "Not Found" response.
4. For each query (primary or secondary), it requests to query the following attributes (if they're not configured as an empty string):
  - MSLDAPPBXNumAttributeName
  - MSLDAPOCSNumAttributeName
  - MSLDAPMobileNumAttributeName
 In addition, it queries the special attribute defined in MSLDAPPrivateNumAttributeName, only if the query key (primary or secondary) is equal to its value.
5. If the query is found: The AD returns up to four attributes - Lync / OCS, PBX / IP PBX, private (only if it equals Primary or Secondary key), and mobile.



6. The device adds unique prefix keywords to the query results in order to identify the query type (i.e., IP domain). These prefixes are used as the prefix destination number value in the Outbound IP Routing table to denote the IP domains:
  - "PRIVATE" (PRIVATE:<private\_number>): used to match a routing rule based on query results of the private number (MSLDAPPrivateNumAttributeName)
  - "OCS" (OCS:<Lync\_number>): used to match a routing rule based on query results of the Lync client number (MSLDAPOCSNumAttributeName)
  - "PBX" (PBX:<PBX\_number>): used to match a routing rule based on query results of the PBX / IP PBX number (MSLDAPPBXNumAttributeName)
  - "MOBILE" (MOBILE:<mobile\_number>): used to match a routing rule based on query results of the mobile number (MSLDAPMobileNumAttributeName)
  - "LDAP\_ERR": used to match a routing rule based on a failed query result when no attribute is found in the AD



**Note:** These prefixes are involved only in the routing and manipulation processes; they are not used as the final destination number.

7. The device uses the Outbound IP Routing table to route the call based on the LDAP query result. The device routes the call according to the following priority:
  1. **Private line:** If the query is done for the private attribute and it's found, then the device routes the call according to this attribute.
  2. **Mediation Server SIP address (Lync / OCS):** If the private attribute does not exist or is not queried, then the device routes the call to the Mediation Server (which then routes the call to the Lync client).
  3. **PBX / IP PBX:** If the Lync / OCS client is not found in the AD, it routes the call to the PBX / IP PBX.
  4. **Mobile number:** If the Lync / OCS client (or Mediation Server) is unavailable (e.g., SIP response 404 "Not Found" upon INVITE sent to Lync client), and the PBX / IP PBX is also unavailable, then the device routes the call to the user's mobile number (if exists in the AD).
  5. **Alternative route:** If the call routing to all the above fails (e.g., due to unavailable destination - call busy), the device can route the call to an alternative destination if an alternative routing rule is configured.
  6. **"Redundant" route:** If the query failed (i.e., no attribute found in the AD), the device uses the routing rule matching the "LDAP\_ERR" prefix destination number value.

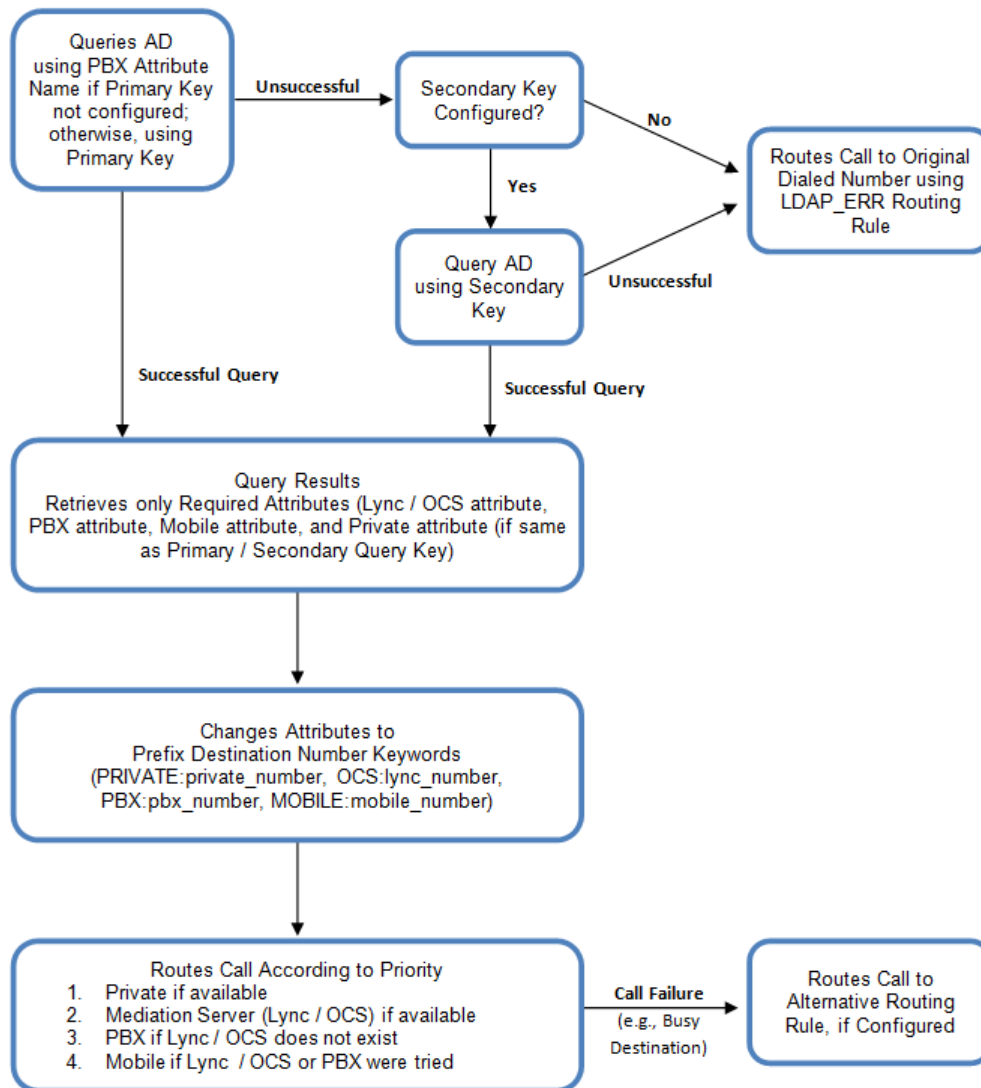


**Note:** For Enterprises implementing a PBX / IP PBX system, but yet to migrate to Lync Server 2010, if the PBX / IP PBX system is unavailable or has failed, the device uses the AD query result for the user's mobile phone number, routing the call through the PSTN to the mobile destination.



The flowchart below summarizes the device's process for querying the AD and routing the call based on the query results:

**Figure 15-4: LDAP Query Flowchart**



**Note:** If you are using the device's local LDAP cache, see "Configuring the Device's LDAP Cache" on page 142 for the LDAP query process.

### 15.1.3.2 Configuring AD-Based Routing Rules

The procedure below describes how to configure Tel-to-IP routing based on LDAP queries.

➤ **To configure LDAP-based Tel-to-IP routing for Lync Server 2010:**

1. Configure the LDAP server parameters, as described in "Configuring the LDAP Server" on page 141.
2. Configure the AD attribute names used in the LDAP query:



- a. Open the Advanced Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** submenu > **Advanced Parameters**).

**Figure 15-5: LDAP Parameters for Microsoft Lync Server 2010**

| MS LDAP Settings                     |                             |
|--------------------------------------|-----------------------------|
| MS LDAP OCS Number attribute name    | msRTCSIP-PrimaryUserAddress |
| MS LDAP PBX Number attribute name    | telephoneNumber             |
| MS LDAP MOBILE Number attribute name | mobile                      |

- b. Configure the LDAP attribute names as desired.
3. Configure AD-based IP-to-IP routing rules:
  - a. Open the IP-to-IP Routing Table page (Configuration tab > VoIP menu > SBC submenu > Routing SBC > IP to IP Routing Table). For more information, see Configuring SBC IP-to-IP Routing on page 236.
  - b. Configure query-result routing rules for each IP domain (private, PBX / IP PBX, Lync / OCS clients, and mobile), using the LDAP keywords (case-sensitive) in the Destination Username Prefix field:
    - ◆ PRIVATE: Private number
    - ◆ OCS: Lync / OCS client number
    - ◆ PBX: PBX / IP PBX number
    - ◆ MOBILE: Mobile number
    - ◆ LDAP\_ERR: LDAP query failure
  - c. Configure a routing rule for routing the initial call (LDAP query) to the LDAP server, by setting the 'Destination Type' field to LDAP for denoting the IP address of the LDAP server.
  - d. For alternative routing, enable the alternative routing mechanism and configure corresponding SIP reasons for alternative routing. For this feature, alternative routing starts from the table row located under the LDAP query row.

The table below shows an example for configuring AD-based SBC routing rules in the IP-to-IP Routing Table:

**Table 15-2: AD-Based SBC IP-to-IP Routing Rule Configuration Examples**

| Index | Destination Username Prefix | Destination Type | Destination Address |
|-------|-----------------------------|------------------|---------------------|
| 1     | PRIVATE:                    | Dest Address     | 10.33.45.60         |
| 2     | PBX:                        | Dest Address     | 10.33.45.65         |
| 3     | OCS:                        | Dest Address     | 10.33.45.68         |
| 4     | MOBILE:                     | Dest Address     | 10.33.45.100        |
| 5     | LDAP_ERR                    | Dest Address     | 10.33.45.80         |
| 6     | *                           | LDAP             |                     |
| 7     | *                           | Dest Address     | 10.33.45.72         |

The configured routing rule example is explained below:

- **Rule 1:** Sends call to private telephone line (at 10.33.45.60) upon successful AD query result for the private attribute.
- **Rule 2:** Sends call to IP PBX (at 10.33.45.65) upon successful AD query result for the PBX attribute.
- **Rule 3:** Sends call to Lync client (i.e., Mediation Server at 10.33.45.68) upon successful AD query result for the Lync attribute.



- **Rule 4:** Sends call to user's mobile phone number (to PSTN through the device's IP address at 10.33.45.100) upon successful AD query result for the Mobile attribute.
- **Rule 5:** Sends call to IP address of device (10.33.45.80) if AD query failure (e.g., no response from LDAP server or attribute not found).
- **Rule 6:** Sends query for original destination number of received call to the LDAP server.
- **Rule 7:** Alternative routing rule that sends the call of original dialed number to IP destination 10.33.45.72. This rule is applied in any of the following cases
  - LDAP functionality is disabled.
  - LDAP query is successful but call fails (due to, for example, busy line) to all the relevant attribute destinations (private, Lync, PBX, and mobile), and a relevant SBC Alternative Routing Reason (see Configuring Alternative Routing Reasons on page 243) has been configured.

Once the device receives the original incoming call, the first rule that it uses is Rule 6, which queries the AD server. When the AD replies, the device searches the table, from the first rule down, for the matching destination phone prefix (i.e., "PRIVATE:", "PBX:", "OCS:", "MOBILE:", and "LDAP\_ERR:"), and then sends the call to the appropriate destination.

## 15.2 Least Cost Routing

This section provides a description of the device's least cost routing (LCR) feature and how to configure it.

### 15.2.1 Overview

The LCR feature enables the device to choose the outbound IP destination routing rule based on lowest call cost. This is useful in that it enables service providers to optimize routing costs for customers. For example, you may wish to define different call costs for local and international calls, or different call costs for weekends and weekdays (specifying even the time of call). The device sends the calculated cost of the call to a Syslog server (as Information messages), thereby enabling billing by third-party vendors.

LCR is implemented by defining Cost Groups and assigning them to routing rules in the Outbound IP Routing table. The device searches this routing table for matching routing rules, and then selects the rule with the lowest call cost. If two routing rules have identical costs, then the rule appearing higher up in the table is used (i.e., first-matched rule). If a selected route is unavailable, the device selects the next least-cost routing rule. However, even if a matched rule is not assigned a Cost Group, the device can select it as the preferred route over other matched rules with Cost Groups. This is determined according to the settings of the Default Cost parameter in the Routing Rule Groups table.

The Cost Group defines a fixed connection cost (*connection cost*) and a charge per minute (*minute cost*). Cost Groups can also be configured with time segments (*time bands*), which define connection cost and minute cost based on specific days of the week and time of day (e.g., from Saturday through Sunday, between 6:00 and 18:00). If multiple time bands are configured per Cost Group and a call spans multiple time bands, the call cost is calculated using only the time band in which the call was initially established.

In addition to Cost Groups, the device can calculate the call cost using an optional, user-defined average call duration value. The logic in using this option is that a Cost Group may be cheap if the call duration is short, but due to its high minute cost, may prove very expensive if the duration is lengthy. Thus, together with Cost Groups, the device can use this option to determine least cost routing. The device calculates the Cost Group call cost as follows: Total Call Cost = Connection Cost + (Minute Cost \* Average Call Duration).

The below table shows an example of call cost when taking into consideration call duration. This example shows four defined Cost Groups and the total call cost if the average call duration is 10 minutes:



**Table 15-3: Call Cost Comparison between Cost Groups for different Call Durations**

| Cost Group | Connection Cost | Minute Cost | Total Call Cost per Duration |            |
|------------|-----------------|-------------|------------------------------|------------|
|            |                 |             | 1 Minute                     | 10 Minutes |
| A          | 1               | 6           | 7                            | 61         |
| B          | 0               | 10          | 10                           | 100        |
| C          | 0.3             | 8           | 8.3                          | 80.3       |
| D          | 6               | 1           | 7                            | 16         |

If four matching routing rules are located in the routing table and each one is assigned a different Cost Group as listed in the table above, then the rule assigned Cost Group "D" is selected. Note that for one minute, Cost Groups "A" and "D" are identical, but due to the average call duration, Cost Group "D" is cheaper. Therefore, average call duration is an important factor in determining the cheapest routing role.

Below are a few examples of how you can implement LCR:

- **Example 1:** This example uses two different Cost Groups for routing local calls and international calls:

Two Cost Groups are configured as shown below:

| Cost Group               | Connection Cost | Minute Cost |
|--------------------------|-----------------|-------------|
| 1. "Local Calls"         | 2               | 1           |
| 2. "International Calls" | 6               | 3           |

The Cost Groups are assigned to routing rules for local and international calls in the Outbound IP Routing table:

| Routing Index | Dest Phone Prefix | Destination IP | Cost Group ID           |
|---------------|-------------------|----------------|-------------------------|
| 1             | 2000              | x.x.x.x        | 1 "Local Calls"         |
| 2             | 00                | x.x.x.x        | 2 "International Calls" |

- **Example 2:** This example shows how the device determines the cheapest routing rule in the Outbound IP Routing table:

The Default Cost parameter (global) in the Routing Rule Groups table is set to **Min**, meaning that if the device locates other matching LCR routing rules (with Cost Groups assigned), the routing rule without a Cost Group is considered the lowest cost route.

- The following Cost Groups are configured:

| Cost Group | Connection Cost | Minute Cost |
|------------|-----------------|-------------|
| 1. "A"     | 2               | 1           |
| 2. "B"     | 6               | 3           |

- The Cost Groups are assigned to routing rules in the Outbound IP Routing table:

| Routing Index | Dest Phone Prefix | Destination IP | Cost Group ID |
|---------------|-------------------|----------------|---------------|
| 1             | 201               | x.x.x.x        | "A"           |
| 2             | 201               | x.x.x.x        | "B"           |
| 3             | 201               | x.x.x.x        | 0             |



| Routing Index | Dest Phone Prefix | Destination IP | Cost Group ID |
|---------------|-------------------|----------------|---------------|
| 4             | 201               | x.x.x.x        | "B"           |

The device calculates the optimal route in the following index order: 3, 1, 2, and then 4, due to the following logic:

- Index 1 - Cost Group "A" has the lowest connection cost and minute cost
- Index 2 - Cost Group "B" takes precedence over Index 4 entry based on the first-matched method rule
- Index 3 - no Cost Group is assigned, but as the Default Cost parameter is set to **Min**, it is selected as the cheapest route
- Index 4 - Cost Group "B" is only second-matched rule (Index 1 is the first)

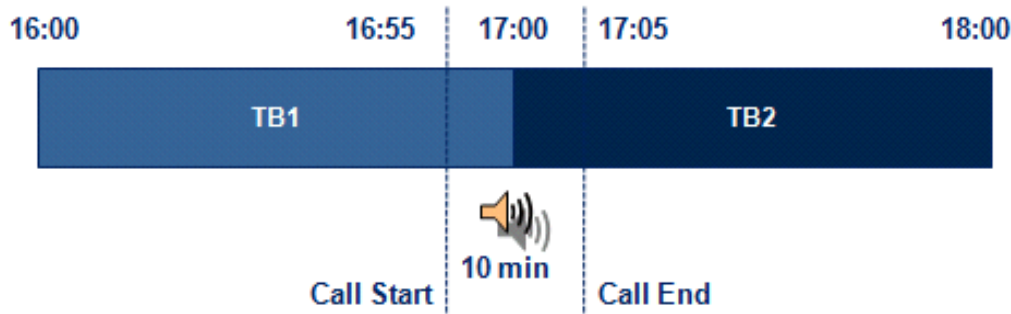
■ **Example 3:** This example shows how the cost of a call is calculated if the call spans over multiple time bands:

Assume a Cost Group, "CG Local" is configured with two time bands, as shown below:

| Cost Group | Time Band | Start Time | End Time | Connection Cost | Minute Cost |
|------------|-----------|------------|----------|-----------------|-------------|
| CG Local   | TB1       | 16:00      | 17:00    | 2               | 1           |
|            | TB2       | 17:00      | 18:00    | 7               | 2           |

Assume that the call duration is 10 minutes, occurring between 16:55 and 17:05. In other words, the first 5 minutes occurs in time band "TB1" and the next 5 minutes occurs in "TB2", as shown below:

**Figure 15-6: LCR using Multiple Time Bands (Example)**



The device calculates the call using the time band in which the call was initially established, regardless of whether the call spans over additional time bands:

**Total call cost** = "TB1" Connection Cost + ("TB1" Minute Cost x call duration) = 2 + 1 x 10 min = 12

## 15.2.2 Configuring LCR

The following main steps need to be done to configure LCR:

1. Enable the LCR feature and configure the average call duration and default call connection cost - see "Enabling LCR and Configuring Default LCR" on page 152.
2. Configure Cost Groups - see "Configuring Cost Groups" on page 153.
3. Configure Time Bands for a Cost Group - see "Configuring Time Bands for Cost Groups" on page 154.
4. Assign Cost Groups to outbound IP routing rules - see "Assigning Cost Groups to Routing Rules" on page 156.



### 15.2.2.1 Enabling the LCR Feature

The procedure below describes how to enable the LCR feature. This also includes configuring the average call duration and default call cost for routing rules that are not assigned Cost Groups in the Outbound IP Routing table.

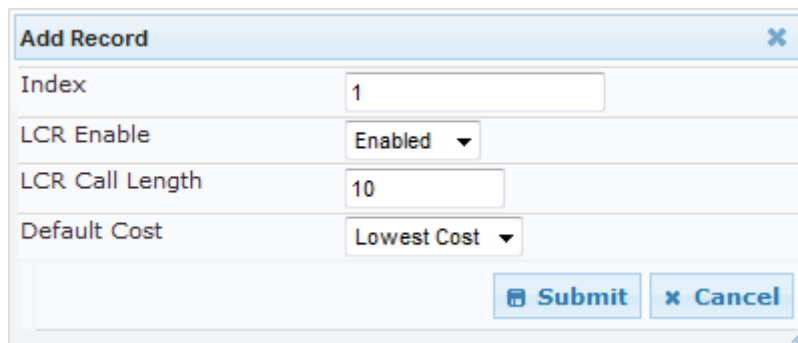


**Note:** The Routing Rule Groups table can also be configured using the table ini file parameter, RoutingRuleGroups.

➤ **To enable LCR:**

1. Open the Routing Rule Groups Table page (**Configuration** tab > **VoIP** menu > **Services** submenu > **Least Cost Routing** > **Routing Rule Groups Table**).
2. Click the **Add** button; the Add Record dialog box appears:

**Figure 15-7: Routing Rule Groups Table - Add Record**



3. Configure the parameters as required. For a description of the parameters, see the table below.
4. Click **Submit**; the entry is added to the Routing Rule Groups table.

**Table 15-4: Routing Rule Groups Table Description**

| Parameter                                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|-------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Index<br>[RoutingRuleGroups_Index]                          | Defines the table index entry.<br><b>Note:</b> Only one index entry can be configured.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| LCR Enable<br>[RoutingRuleGroups_LCREnable]                 | Enables the LCR feature: <ul style="list-style-type: none"> <li>▪ [0] Disabled (default)</li> <li>▪ [1] Enabled</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| LCR Call Length<br>[RoutingRuleGroups_LCRAverageCallLength] | Defines the average call duration (in minutes) and is used to calculate the variable portion of the call cost. This is useful, for example, when the average call duration spans over multiple time bands. The LCR is calculated as follows: cost = call connect cost + (minute cost * average call duration)<br>The valid value range is 0-65533. The default is 1.<br>For example, assume the following Cost Groups: <ul style="list-style-type: none"> <li>▪ "Weekend A": call connection cost is 1 and charge per minute is 6. Therefore, a call of 1 minute cost 7 units.</li> <li>▪ "Weekend_B": call connection cost is 6 and charge per minute is 1. Therefore, a call of 1 minute cost 7 units.</li> </ul> Therefore, for calls under one minute, "Weekend A" carries the lower cost. However, if the average call duration is more |



| Parameter                                          | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|----------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                    | than one minute, then "Weekend B" carries the lower cost.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Default Cost<br>[RoutingRuleGroups_LCRDefaultCost] | <p>Determines whether routing rules in the Outbound IP Routing table without an assigned Cost Group are considered a higher cost or lower cost route compared to other matched routing rules that are assigned Cost Groups.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Lowest Cost = If the device locates other matching LCR routing rules, this routing rule is considered the lowest cost route and therefore, it is selected as the route to use (default.)</li> <li>▪ <b>[1]</b> Highest Cost = If the device locates other matching LCR routing rules, this routing rule is considered as the highest cost route and therefore, is not used or used only if the other cheaper routes are unavailable.</li> </ul> <p><b>Note:</b> If more than one valid routing rule without a defined Cost Group exists, the device selects the first-matched rule.</p> |

### 15.2.2.2 Configuring Cost Groups

The procedure below describes how to configure Cost Groups. Cost Groups are defined with a fixed call connection cost and a call rate (charge per minute). Once configured, you can configure Time Bands for each Cost Group. Up to 10 Cost Groups can be configured.



**Note:** The Cost Group table can also be configured using the table ini file parameter, CostGroupTable.

➤ **To configure Cost Groups:**

1. Open the Cost Group Table page (**Configuration** tab > **VoIP** menu > **Services** submenu > **Least Cost Routing** > **Cost Group Table**).
2. Click the **Add** button; the Add Record dialog box appears:

3. Configure the parameters as required. For a description of the parameters, see the table below.
4. Click **Submit**; the entry is added to the Cost Group table.



Table 15-5: Cost Group Table Description

| Parameter                                                      | Description                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Index<br>[CostGroupTable_Index]                                | Defines the table index entry.                                                                                                                                                                                                                                                                                                                            |
| Cost Group Name<br>[CostGroupTable_CostGroupName]              | Defines an arbitrary name for the Cost Group.<br>The valid value is a string of up to 30 characters.<br><b>Note:</b> Each Cost Group must have a unique name.                                                                                                                                                                                             |
| Default Connect Cost<br>[CostGroupTable_DefaultConnectionCost] | Defines the call connection cost (added as a fixed charge to the call) for a call outside the time bands.<br>The valid value range is 0-65533. The default is 0.<br><b>Note:</b> When calculating the cost of a call, if the current time of the call is not within a time band configured for the Cost Group, then this default connection cost is used. |
| Default Time Cost<br>[CostGroupTable_DefaultMinuteCost]        | Defines the call charge per minute for a call outside the time bands.<br>The valid value range is 0-65533. The default is 0.<br><b>Note:</b> When calculating the cost of a call, if the current time of the call is not within a time band configured for the Cost Group, then this default charge per minute is used.                                   |

### 15.2.2.3 Configuring Time Bands for Cost Groups

The procedure below describes how to configure Time Bands for a Cost Group. The time band defines the day and time range for which the time band is applicable (e.g., from Saturday 05:00 to Sunday 24:00) as well as the fixed call connection charge and call rate per minute for this interval. Up to 70 time bands can be configured, and up to 21 time bands can be assigned to each Cost Group.


**Notes:**

- You cannot define overlapping time bands.
- The Time Band table can also be configured using the table ini file parameter, CostGroupTimebands.

➤ **To configure Time Bands for a Cost Group:**

- Open the Cost Group Table page (**Configuration** tab > **VoIP** menu > **Services** submenu > **Least Cost Routing** > **Cost Group Table**).
- Select a Cost Group for which you want to assign Time Bands, and then click the **Time Band** link located below the table; the Time Band table for the selected Cost Group appears.
- Click the **Add** button; the Add Record dialog box appears:



4. Configure the parameters as required. For a description of the parameters, see the table below.
5. Click **Submit**; the entry is added to the Time Band table for the relevant Cost Group.

**Table 15-6: Time Band Table Description**

| Parameter                                              | Description                                                                                                                                                                                                                                                                                                                                                                              |
|--------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Index<br>[CostGroupTimebands_TimebandIndex]            | Defines the table index entry.                                                                                                                                                                                                                                                                                                                                                           |
| Start Time<br>[CostGroupTimebands_StartTime]           | <p>Defines the day and time of day from when this time band is applicable. The format is ddd:hh:mm (e.g., sun:06:00), where:</p> <ul style="list-style-type: none"> <li>▪ <i>ddd</i> is the day (i.e., sun, mon, tue, wed, thu, fri, or sat)</li> <li>▪ <i>hh</i> and <i>mm</i> denote the time of day, where <i>hh</i> is the hour (00-23) and <i>mm</i> the minutes (00-59)</li> </ul> |
| End Time<br>[CostGroupTimebands_EndTime]               | Defines the day and time of day until when this time band is applicable. For a description of the valid values, see the parameter above.                                                                                                                                                                                                                                                 |
| Connection Cost<br>[CostGroupTimebands_ConnectionCost] | <p>Defines the call connection cost during this time band. This is added as a fixed charge to the call.</p> <p>The valid value range is 0-65533. The default is 0.</p> <p><b>Note:</b> The entered value must be a whole number (i.e., not a decimal).</p>                                                                                                                               |
| Minute Cost<br>[CostGroupTimebands_MinuteCost]         | <p>Defines the call cost per minute charge during this timeband.</p> <p>The valid value range is 0-65533. The default is 0.</p> <p><b>Note:</b> The entered value must be a whole number (i.e., not a decimal).</p>                                                                                                                                                                      |



#### **15.2.2.4 Assigning Cost Groups to Routing Rules**

Once you have configured your Cost Groups, you need to assign them to routing rules in the IP-to-IP Routing table - see [Configuring SBC IP-to-IP Routing](#) on page [236](#).



## 16 Enabling Applications

The device supports the following main applications:

- Stand-Alone Survivability (SAS) application
- Session Border Control (SBC) application

The procedure below describes how to enable these applications. Once an application is enabled, the Web GUI provides menus and parameter fields relevant to the application.



### Notes:

- This page displays the application only if the device is installed with the relevant Software License Key supporting the application (see "Loading Software License Key" on page 320).
- For configuring the SAS application, see "Stand-Alone Survivability (SAS) Application" on page 255.
- For configuring the SBC application, see Session Border Controller on page 199.
- For enabling an application, a device reset is required.

### ➤ To enable an application:

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

|                   |           |
|-------------------|-----------|
| ▼                 |           |
| ⚡ SAS Application | Disable ▼ |
| ⚡ SBC Application | Enable ▼  |

2. From the relevant application drop-down list, select **Enable**.
3. Save (burn) the changes to the device's flash memory with a device reset (see "Saving Configuration" on page 308).



## Reader's Notes



# 17 Control Network

This section describes configuration of the network at the SIP control level.

## 17.1 Configuring SRD Table

The SRD Settings page allows you to configure up to 32 signaling routing domains (SRD). An SRD is configured with a unique name and assigned a Media Realm. Additional SBC attributes such as media anchoring and user registration can also be configured.

An SRD is a set of definitions together creating multiple, virtual multi-service IP gateways:

- Multiple and different SIP signaling interfaces (SRD associated with a SIP Interface) and RTP media (associated with a Media Realm) for multiple Layer-3 networks. Due to the B2BUA nature of the SBC application, different interfaces can be assigned to each leg of the call.
- Can operate with multiple gateway customers that may reside either in the same or in different Layer-3 networks as the device. This allows separation of signaling traffic between different customers. In such a scenario, the device is configured with multiple SRD's.

Typically, one SRD is defined for each group of SIP UAs (e.g. proxies, IP phones, application servers, gateways, and softswitches) that communicate with each other. This provides these entities with VoIP services that reside on the same Layer-3 network (must be able to communicate without traversing NAT devices and must not have overlapping IP addresses). Routing from one SRD to another is possible, whereby each routing destination (IP Group or destination address) indicates the SRD to which it belongs.

Once configured, you can use the SRD as follows:

- Associate it with a SIP Interface (see "Configuring SIP Interface Table" on page 161)
- Associate it with an IP Group (see "Configuring IP Groups" on page 164)
- Associate it with a Proxy Set (see "Configuring Proxy Sets Table" on page 171)
- Apply an Admission Control rule to it (see Configuring Admission Control Table on page 226)
- Define it as a Classification rule for the incoming SIP request (see "Configuring Classification Rules" on page 230)
- Use it as a destination IP-to-IP routing rule (see "Configuring SBC IP-to-IP Routing" on page 236)

The SRD Settings page also displays the IP Groups, Proxy Sets, and SIP Interfaces associated with a selected SRD index.



### Notes:

- On the SRD Settings page, you can also configure a SIP Interface in the SIP Interface table, instead of navigating to the SIP Interface Table page as described in "Configuring SIP Interface Table" on page 161.
- The SRD table can also be configured using the table ini file parameter, SRD.



➤ **To configure SRDs:**

1. Open the SRD Settings page (**Configuration** tab > **VoIP** menu > **Control Network** submenu > **SRD Table**).

**Figure 17-1: SRD Settings Page**

|                                       |                      |
|---------------------------------------|----------------------|
| ▼                                     |                      |
| SRD Index                             | 0 - Not Exist ▼      |
| ▼ Common Parameters                   |                      |
| SRD Name                              | <input type="text"/> |
| Media Realm                           | <input type="text"/> |
| ▼ SBC Parameters                      |                      |
| Internal SRD Media Anchoring          | Anchor Media ▼       |
| Block Unregistered Users              | No ▼                 |
| Max Number Of Registered Users        | -1                   |
| Enable Un-Authenticated Registrations | Yes ▼                |

2. From the 'SRD Index' drop-down list, select an index for the SRD, and then configure it according to the table below.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 308.

**Table 17-1: SRD Table Parameters**

| Parameter                                                        | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SRD Name<br>[SRD_Name]                                           | Mandatory descriptive name of the SRD.<br>The valid value can be a string of up to 21 characters.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Media Realm<br>[SRD_MediaRealm]                                  | Defines the Media Realm associated with the SRD. The entered string value must be identical (and case-sensitive) to the Media Realm name configured in the Media Realm table (see "Configuring Media Realms" on page 130).<br>The valid value is a string of up to 40 characters.<br><b>Notes:</b> <ul style="list-style-type: none"> <li>▪ If the Media Realm is later deleted from the Media Realm table, then this value becomes invalid in the SRD table.</li> <li>▪ For configuring Media Realms, see "Configuring Media Realms" on page 130.</li> </ul>                                                                                                                                                                                                                                            |
| SBC Parameters                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Internal SRD Media Anchoring<br>[SRD_IntraSRDMediaAnchorin<br>g] | Determines whether the device performs media anchoring or not on media for the SRD. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Anchor Media = (Default) RTP traverses the device and each leg uses a different coder or coder parameters.</li> <li>▪ <b>[1]</b> Don't Anchor Media = The RTP packet flow does not traverse the device; instead, the two SIP UA's establish a direct RTP/SRTP (media) flow between one another.</li> </ul> <b>Notes:</b> <ul style="list-style-type: none"> <li>▪ When No Media Anchoring is enabled: <ul style="list-style-type: none"> <li>✓ The device does not perform manipulation on SDP data (offer/answer transactions) such as ports, IP address, and coders.</li> <li>✓ Opening voice channels and allocation of IP media ports</li> </ul> </li> </ul> |



| Parameter                                                                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                          | <p>are not required.</p> <ul style="list-style-type: none"> <li>When two UA's pertain to the same SRD and this parameter is set to <b>[1]</b>, and one of the UA's is defined as a foreign user (example, "follow me service") located on the WAN while the other UA is located on the LAN, then calls between these two UA's can't be established until this parameter is set to 0, as the device doesn't interfere in the SIP signaling. In other words, parameters such as IP addresses are not manipulated for calls between LAN and WAN (although required).</li> <li>When the global parameter SBCDirectMedia is disabled, you cannot enable No Media Anchoring for two UA's pertaining to separate SRDs; No Media Anchoring can only be enable for two UA's pertaining to the same SRD.</li> <li>For more information on media handling, see SBC Media Handling on page 205.</li> </ul> |
| Block Unregistered Users<br><b>[SRD_BlockUnRegUsers]</b>                                 | <p>Determines whether the device blocks (rejects) incoming calls (INVITE requests) from unregistered users (pertaining to User-type IP Groups) for the SRD.</p> <ul style="list-style-type: none"> <li><b>[0]</b> No = Calls from unregistered users are not blocked (default).</li> <li><b>[1]</b> Yes = Blocks calls from unregistered users.</li> </ul> <p><b>Note:</b> When the call is blocked, the device sends a SIP 500 "Server Internal Error" response to the remote end.</p>                                                                                                                                                                                                                                                                                                                                                                                                        |
| Max Number of Registered Users<br><b>[SRD_MaxNumOfRegUsers]</b>                          | <p>Maximum number of users belonging to this SRD that can register with the device. By default, no limitation exists for registered users</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Enable Un-Authenticated Registrations<br><b>[SRD_EnableUnAuthenticatedRegistrations]</b> | <p>Determines whether the device blocks REGISTER requests from new users (i.e., users not registered in the device's registration database) when the destination is a User-type IP Group.</p> <ul style="list-style-type: none"> <li><b>[0]</b> No = The device sends REGISTER requests to the SIP proxy server and only if authenticated by the server does the device add the user registration to its database.</li> <li><b>[1]</b> Yes = The device adds REGISTER requests to its database even if the requests are not authenticated by a SIP proxy (default).</li> </ul>                                                                                                                                                                                                                                                                                                                 |

## 17.2 Configuring SIP Interface Table

The SIP Interface table allows you to configure up to 32 SIP Interfaces. The SIP Interface defines a listening port and type (UDP, TCP, or TLS) for SIP signaling traffic on a specific logical IP network interface configured for the device (in the Multiple Interface table).

The SIP Interface is configured for a specific application (i.e., SAS and SBC) and associated with an SRD. For each SIP Interface, you can assign a SIP message policy, enable TLS mutual authentication, enable TCP keepalive, and determine the SIP response sent upon classification failure.

SIP Interfaces can be used, for example, for the following:

- Using SIP signaling interfaces per call leg (i.e., each SIP entity communicates with a specific SRD).
- Using different SIP listening ports for a single or for multiple IP network interfaces.
- Differentiating between applications by creating SIP Interfaces per application.



- Separating signaling traffic between networks (e.g., different customers) to use different routing tables, manipulations, SIP definitions, and so on.

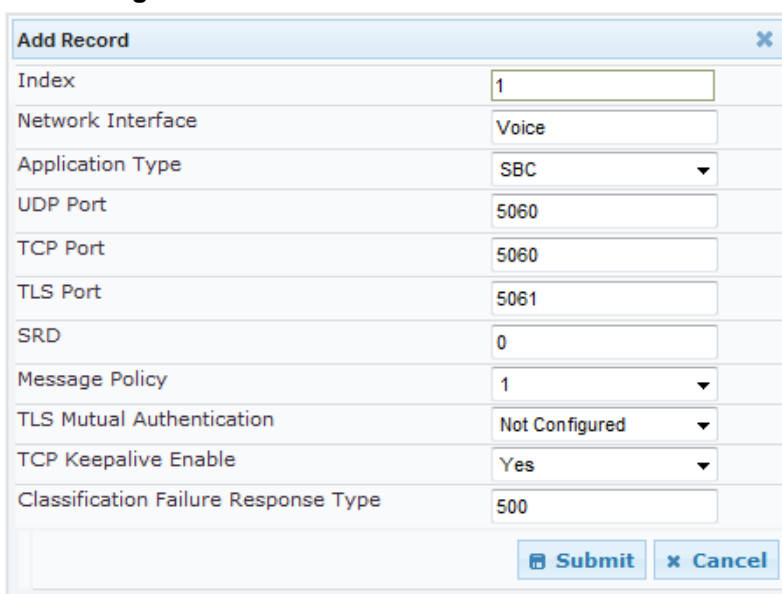


**Note:** The SIP Interface table can also be configured using the table *ini* file parameter, SIPInterface.

➤ **To configure the SIP Interface table:**

1. Open the SIP Interface Table page (**Configuration** tab > **VoIP** menu > **Control Network** submenu > **SIP Interface Table**).
2. Click the **Add** button; the following dialog box appears:

**Figure 17-2: SIP Interface Table – Add Record**



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

**Table 17-2: SIP Interface Table Parameters**

| Parameter                                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Network Interface<br>[SIPInterface_NetworkInterface] | <p>Defines the Control-type IP network interface that you want to associate with the SIP Interface. This value string must be identical (including case-sensitive) to that configured in the 'Interface Name' field of the Multiple Interface table (see "Configuring IP Network Interfaces" on page 90).</p> <p>The default is not configured.</p> <p><b>Note:</b> SIP Interfaces that are assigned to a specific SRD must be defined with the same network interface. For example, if you define three SIP Interfaces for SRD ID #8, all these SIP Interfaces must be defined with the same network interface (e.g., "SIP1").</p> |
| Application Type<br>[SIPInterface_ApplicationType]   | <p>Defines the application type associated with the SIP Interface.</p> <ul style="list-style-type: none"> <li>■ [1] SAS = Stand-Alone Survivability (SAS) application.</li> <li>■ [2] SBC = SBC application.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                             |
| UDP Port                                             | Defines the listening and source UDP port.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |



| Parameter                                                           | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
|---------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| [SIPInterface_UDPPort]                                              | <p>The valid range is 1 to 65534. The default is 5060.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This port must be outside of the RTP port range.</li> <li>Each SIP Interface must have a unique signaling port (i.e., no two SIP Interfaces can share the same port - no port overlapping).</li> </ul>                                                                                                                                                                                                                                                                                                          |
| TCP Port<br>[SIPInterface_TCPPort]                                  | <p>Defines the listening TCP port.</p> <p>The valid range is 1 to 65534. The default is 5060.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This port must be outside of the RTP port range.</li> <li>Each SIP Interface must have a unique signaling port (i.e., no two SIP Interfaces can share the same port - no port overlapping).</li> </ul>                                                                                                                                                                                                                                                                   |
| TLS Port<br>[SIPInterface_TLSPort]                                  | <p>Defines the listening TLS port.</p> <p>The valid range is 1 to 65534. The default is 5061.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This port must be outside of the RTP port range.</li> <li>Each SIP Interface must have a unique signaling port (i.e., no two SIP Interfaces can share the same port - no port overlapping).</li> </ul>                                                                                                                                                                                                                                                                   |
| SRD<br>[SIPInterface_SRD]                                           | <p>Assigns an SRD ID to the SIP Interface.</p> <p>The default is 0.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>Each SRD can be associated with up to three SIP Interfaces, where each SIP Interface pertains to a different Application Type (SAS, and SBC).</li> <li>SIP Interfaces that are assigned to a specific SRD must be defined with the same network interface. For example, if you define three SIP Interfaces for SRD ID #8, all these SIP Interfaces must be defined with the same network interface (e.g., "SIP1").</li> <li>To configure SRDs, see "Configuring SRD Table" on page 159.</li> </ul> |
| Message Policy<br>[SIPInterface_MessagePolicy]                      | <p>Assigns a SIP message policy to the SIP interface.</p> <p><b>Note:</b> To configure SIP message policies, see "Configuring SIP Message Policy Rules".</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| TLS Mutual Authentication<br>[SIPInterface_TLSMutualAuthentication] | <p>Enables TLS mutual authentication per SIP Interface.</p> <ul style="list-style-type: none"> <li><b>[-1]</b> Not Configured = (Default) The SIPRequireClientCertificate global parameter setting is applied.</li> <li><b>[0]</b> Disable = Device does not request the client certificate for TLS connection.</li> <li><b>[1]</b> Enable = Device requires receipt and verification of the client certificate to establish the TLS connection.</li> </ul>                                                                                                                                                                            |



| Parameter                                                                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| TCP Keepalive Enable<br>[SIPInterface_TCPKeepaliveEnable]                                | <p>Enables the TCP Keep-Alive mechanism with the IP entity on this SIP interface. TCP keepalive can be used, for example, to keep a NAT entry open for clients located behind a NAT server or simply to check that the connection to the IP entity is available.</p> <ul style="list-style-type: none"> <li>[0] No (default)</li> <li>[1] Yes</li> </ul> <p><b>Note:</b> For configuring TCP keepalive, use the following ini file parameters: TCP TCPKeepAliveTime, TCPKeepAliveInterval, and TCPKeepAliveRetry.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
| Classification Failure Response Type<br>[SIPInterface_ClassificationFailureResponseType] | <p>Defines the SIP response code that the device sends if a received SIP request (OPTIONS, REGISTER, or INVITE) has failed the SBC classification process.</p> <p>The valid value can be a SIP response code from 400 through 699, or it can be set to 0 to not send any response at all. The default response code is 500 (Server Internal Error).</p> <p>This feature is important for preventing Denial of Service (DoS) attacks, typically initiated from the WAN. Malicious attackers can use SIP scanners to detect ports used by SIP devices. These scanners scan devices by sending UDP packets containing a SIP request to a range of specified IP addresses, listing those that return a valid SIP response. Once the scanner finds a device that supports SIP, it extracts information from the response and identifies the type of device (IP address and name) and can execute DoS attacks. A way to defend the device against such attacks is to not send a SIP reject response to these unclassified "calls" so that the attacker assumes that no device exists at such an IP address and port.</p> <p><b>Note:</b> This parameter is applicable only if the device is set to reject unclassified calls. This is configured using the 'Unclassified Calls' parameter on the General Settings page (<b>Configuration</b> tab &gt; <b>VoIP</b> menu &gt; <b>SBC</b> &gt; <b>General Settings</b>).</p> |

## 17.3 Configuring IP Groups

The IP Group Table page allows you to create up to 32 IP Groups. The IP Group represents a SIP entity on the network with which the device communicates. This can be a server (e.g., IP PBX or ITSP) or it can be a group of users (e.g., LAN IP phones). For servers, the IP Group is typically used to define the server's IP address by associating it with a Proxy Set (see 'Configuring Proxy Sets Table' on page 171).

This table can also be used to classify incoming SIP dialog-initiating requests (e.g., INVITE messages) to specific IP Groups based on the associated Proxy Set ID. However, it is highly recommended to use the Classification table for classifying incoming SIP dialogs to the IP Groups (see 'Configuring Classification Rules' on page 230). See the 'Classify by Proxy Set' parameter below for a detailed description of this feature and for important recommendations.

IP Groups are used for IP-to-IP routing rules where they represent the source and destination of the call (see 'Configuring SBC IP-to-IP Routing' on page 236).



**Notes:**

- IP Group ID 0 cannot be used. This IP Group is set to default values and is used by the device when IP Groups are not implemented.
- When operating with multiple IP Groups, the default Proxy server must not be used (i.e., the parameter IsProxyUsed must be set to 0).
- If different SRDs are configured in the IP Group and Proxy Set tables, the SRD defined for the Proxy Set takes precedence.
- You can also configure the IP Groups table using the table ini file parameter, IPGroup (see "Configuration Parameters Reference" on page 387).

➤ **To configure IP Groups:**

1. Open the IP Group Table page (**Configuration** tab > **VoIP** menu > **Control Network** submenu > **IP Group Table**).
2. Click the **Add** button: the following dialog box appears:

**Figure 17-3: IP Group Table – Add Record**

3. Configure the IP Group parameters according to the table below.
4. Click **Submit**.
5. To save the changes to flash memory, see "Saving Configuration" on page 308.

**Table 17-3: IP Group Parameters**

| Parameter                | Description                                                                                                                                                                                                          |
|--------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Common Parameters</b> |                                                                                                                                                                                                                      |
| Type<br>[IPGroup_Type]   | Defines the type of IP Group: <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Server = Used when the destination address, configured by the Proxy Set, of the IP Group (e.g., ITSP, Proxy, IP-PBX, or</li> </ul> |



| Parameter                                   | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|---------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                             | <p>Application server) is known.</p> <ul style="list-style-type: none"> <li>▪ <b>[1] User</b> = Represents a group of users such as IP phones and softphones where their location is dynamically obtained by the device when REGISTER requests and responses traverse (or are terminated) by the device. These users are considered remote (far-end) users.</li> </ul> <p>Typically, this IP Group is configured with a Serving IP Group that represents an IP-PBX, Application or Proxy server that serves this User-type IP Group. Each SIP request sent by a user of this IP Group is proxied to the Serving IP Group. For registrations, the device updates its internal database with the AOR and contacts of the users.</p> <p>Digest authentication using SIP 401/407 responses (if needed) is performed by the Serving IP Group. The device forwards these responses directly to the SIP users.</p> <p>To route a call to a registered user, a rule must be configured in the SBC IP-to-IP Routing table. The device searches the dynamic database (by using the request URI) for an entry that matches a registered AOR or Contact. Once an entry is found, the IP destination is obtained from this entry, and a SIP request is sent to the destination.</p> <p>The device also supports NAT traversal for the SIP clients located behind NAT. In this case, the device must be defined with a global IP address.</p> <ul style="list-style-type: none"> <li>▪ <b>[2] Gateway</b> = This is applicable only to the SBC application in scenarios where the device receives requests to and from a gateway representing multiple users. This IP Group type is necessary as the other IP Group types are not suitable: <ul style="list-style-type: none"> <li>✓ The IP Group cannot be defined as a Server since its destination address is unknown during configuration.</li> <li>✓ The IP Group cannot be defined as a User since the SIP Contact header of the incoming REGISTER does not represent a specific user. The Request-URI user part can change and therefore, the device is unable to identify an already registered user and therefore, adds an additional record to the database.</li> </ul> </li> </ul> <p>The IP address of the Gateway IP Group is obtained dynamically from the host part of the Contact header in the REGISTER request received from the IP Group. Therefore, routing to this IP Group is possible only once a REGISTER request is received. If a REGISTER refresh request arrives, the device updates the new location (i.e., IP address) of the IP Group. If the REGISTER fails, no update is performed. If an UN-REGISTER request arrives, the IP address associated with the IP Group is deleted and therefore, no routing to the IP Group is done.</p> |
| Description<br><b>[IPGroup_Description]</b> | <p>Defines a brief description for the IP Group.</p> <p>The valid value is a string of up to 29 characters. The default is an empty field.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Proxy Set ID<br><b>[IPGroup_ProxySetId]</b> | <p>Assigns a Proxy Set ID to the IP Group. All INVITE messages destined to this IP Group are sent to the IP address configured for the Proxy Set.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ Proxy Set ID 0 must <b>not</b> be used; this is the device's default</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |



| Parameter                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
|------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                          | <p>Proxy.</p> <ul style="list-style-type: none"> <li>The Proxy Set is applicable only to Server-type IP Groups.</li> <li>The SRD configured for this Proxy Set in the Proxy Set table is automatically assigned to this IP Group (see the 'SRD' field below).</li> <li>To configure Proxy Sets, see "Configuring Proxy Sets Table" on page 171.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| SIP Group Name<br>[IPGroup_SIPGroupName] | <p>Defines the SIP Request-URI host name used in INVITE and REGISTER messages sent to this IP Group, or the host name in the From header of INVITE messages received from this IP Group. The valid value is a string of up to 100 characters. The default is an empty field.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>If this parameter is not configured, the value of the global parameter, ProxyName is used instead (see "Configuring Proxy and Registration Parameters" on page 179).</li> <li>If the IP Group is of User type, this parameter is used internally as a host name in the Request-URI for Tel-to-IP initiated calls. For example, if an incoming call from the device's T1 trunk is routed to a User-type IP Group, the device first creates the Request-URI (&lt;destination_number&gt;@&lt;SIP Group Name&gt;), and then it searches the internal database for a match.</li> </ul> |
| Contact User<br>[IPGroup_ContactUser]    | <p>Defines the user part of the From, To, and Contact headers of SIP REGISTER messages, and the user part of the Contact header of INVITE messages received from this IP Group and forwarded by the device to another IP Group.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable only to Server-type IP Groups.</li> <li>This parameter is overridden by the 'Contact User' parameter in the 'Account' table (see "Configuring Account Table" on page 177).</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                             |
| Local Host Name<br>[IPGroup_ContactName] | <p>Defines the host name (string) that the device uses in the SIP message's Via and Contact headers. This is typically used to define an FQDN as the host name. The device uses this string for Via and Contact headers in outgoing INVITE messages to a specific IP Group, and the Contact header in SIP 18x and 200 OK responses for incoming INVITE messages from a specific IP Group. The Inbound IP Routing table can be used to identify the source IP Group from where the INVITE message was received.</p> <p>If this parameter is not configured (default), these headers are populated with the device's dotted-decimal IP address of the network interface on which the message is sent.</p> <p><b>Note:</b> To ensure proper device handling, this parameter should be a valid FQDN.</p>                                                                                                                           |



| Parameter                                                 | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|-----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SRD<br>[IPGroup_SRD]                                      | <p>Assigns an SRD to the IP Group.<br/>The default is 0.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>To configure SRDs, see Configuring SRD Table on page 159.</li> <li>For Server-type IP Groups, if you assign the IP Group with a Proxy Set ID (in the 'Proxy Set ID' field), the SRD field is automatically set to the SRD value assigned to the Proxy Set in the Proxy Set table.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| Media Realm Name<br>[IPGroup_MediaRealm]                  | <p>Assigns a Media Realm to the IP Group. The string value must be identical (including case-sensitive) to the Media Realm name defined in the Media Realm table.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>If the Media Realm is later deleted from the Media Realm table, then this value becomes invalid.</li> <li>For configuring Media Realms, see Configuring Media Realms on page 130.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| IP Profile ID<br>[IPGroup_ProfileId]                      | <p>Assigns an IP Profile to the IP Group.<br/>The default is 0.</p> <p><b>Note:</b> To configure IP Profiles, see "Configuring IP Profiles" on page 189.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| <b>SBC Parameters</b>                                     |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Classify By Proxy Set<br>[IPGroup_ClassifyByProxySet<br>] | <p>Defines whether the incoming INVITE is classified to an IP Group according to its associated Proxy Set ID.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable</li> <li><b>[1]</b> Enable (default)</li> </ul> <p>This classification occurs only if classification according to the device's database fails to (i.e., received INVITE is not from a registered user). The classification proceeds with checking whether the INVITE's IP address (if host names, then according to the dynamically resolved IP address list) is defined for a Proxy Set ID (in the Proxy Set table). If a Proxy Set ID has such an IP address, the device classifies the INVITE as belonging to the IP Group associated with this Proxy Set. The Proxy Set ID is assigned to the IP Group using the IP Group table's 'Proxy Set ID' parameter (see above).</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>In cases where multiple IP Groups are associated with the same Proxy Set ID, do not enable this feature. If enabled, the device is unable to correctly classify the incoming INVITEs to the appropriate IP Groups.</li> <li>To enhance security, it is highly recommended to disable this parameter so that the device can use the Classification table rules to classify the call. If this parameter is enabled, the Classification table is not used if an associated Proxy Set is found.</li> <li>This parameter is applicable only to Server-type IP Groups.</li> </ul> |



| Parameter                                                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|----------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Max Number Of Registered Users<br><b>[IPGroup_MaxNumOfRegUse rs]</b> | <p>Defines the maximum number of users in this IP Group that can register with the device. By default, no limitation exists for registered users.</p> <p><b>Note:</b> This field is applicable only to User-type IP Groups.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Source URI Input<br><b>[IPGroup_SourceUriInput]</b>                  | <p>Defines the SIP header in the incoming INVITE to use for call matching characteristics based on source URIs.</p> <ul style="list-style-type: none"> <li>▪ <b>[-1]</b> Not Configured (default)</li> <li>▪ <b>[0]</b> From</li> <li>▪ <b>[1]</b> To</li> <li>▪ <b>[2]</b> Request-URI</li> <li>▪ <b>[3]</b> P-Asserted - First Header</li> <li>▪ <b>[4]</b> P-Asserted - Second Header</li> <li>▪ <b>[5]</b> P-Preferred</li> <li>▪ <b>[6]</b> Route</li> <li>▪ <b>[7]</b> Diversion</li> <li>▪ <b>[8]</b> P-Associated-URI</li> <li>▪ <b>[9]</b> P-Called-Party-ID</li> <li>▪ <b>[10]</b> Contact</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This parameter is applicable only when classification is done according to the Classification table.</li> <li>▪ If the configured SIP header does not exist in the incoming INVITE message, the classification of the message to a source IP Group fails.</li> <li>▪ If the device receives an INVITE as a result of a REFER request or a 3xx response, then the incoming INVITE is routed according to the Request-URI. The device identifies such INVITES according to a specific prefix in the Request-URI header, configured by the SBCXferPrefix parameter. Therefore, in this scenario, the device ignores this parameter setting.</li> </ul> |
| Destination URI Input<br><b>[IPGroup_DestUriInput]</b>               | <p>Defines the SIP header in the incoming INVITE to use for call matching characteristics based on destination URIs.</p> <ul style="list-style-type: none"> <li>▪ <b>[-1]</b> Not Configured (default)</li> <li>▪ <b>[0]</b> From</li> <li>▪ <b>[1]</b> To</li> <li>▪ <b>[2]</b> Request-URI</li> <li>▪ <b>[3]</b> P-Asserted - First Header</li> <li>▪ <b>[4]</b> P-Asserted - Second Header</li> <li>▪ <b>[5]</b> P-Preferred</li> <li>▪ <b>[6]</b> Route</li> <li>▪ <b>[7]</b> Diversion</li> <li>▪ <b>[8]</b> P-Associated-URI</li> <li>▪ <b>[9]</b> P-Called-Party-ID</li> <li>▪ <b>[10]</b> Contact</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This parameter is applicable only when classification is done according to the Classification table.</li> <li>▪ If the configured SIP header does not exist in the incoming INVITE message, the classification of the message to a source IP</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                        |



| Parameter                                                            | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|----------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                      | <p>Group fails.</p> <ul style="list-style-type: none"> <li>If the device receives an INVITE as a result of a REFER request or a 3xx response, then the incoming INVITE is routed according to the Request-URI. The device identifies such INVITEs according to a specific prefix in the Request-URI header, configured by the SBCXferPrefix parameter. Therefore, in this scenario, the device ignores this parameter setting.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Inbound Message Manipulation Set<br><b>[IPGroup_InboundManSet]</b>   | Assigns a Message Manipulation Set (rule) to the IP Group for SIP message manipulation on the inbound message. The Message Manipulation rules are configured using the MessageManipulations parameter (see Configuring SIP Message Manipulation on page 182).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Outbound Message Manipulation Set<br><b>[IPGroup_OutboundManSet]</b> | Message Manipulation Set (rule) that you want to assign to this IP Group for SIP message manipulation on the outbound message. The Message Manipulation rules are configured using the MessageManipulations parameter (see Configuring SIP Message Manipulation on page 182).                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
| Registration Mode<br><b>[IPGroup_RegistrationMode]</b>               | <p>Defines the registration mode for the IP Group:</p> <ul style="list-style-type: none"> <li><b>[0]</b> User initiates registrations (default)</li> <li><b>[1]</b> SBC initiate registrations = Used when the device serves as a client (e.g., with an IP PBX). This functions only with User Info file.</li> <li><b>[2]</b> No registrations needed = The device adds users to its database in active state.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Authentication Mode<br><b>[IPGroup_AuthenticationMode]</b>           | <p>Defines the authentication mode.</p> <ul style="list-style-type: none"> <li><b>[0]</b> User Authenticates = (Default) The device does not handle the authentication, but simply passes the authentication messages between the SIP user agents.</li> <li><b>[1]</b> SBC as client = The device authenticates as a client. It receives the 401/407 response from the proxy requesting for authentication. The device sends the proxy the authorization credentials (i.e., user name and password) according to one of the following: 1) account defined in the Account table (only if authenticating Server-type IP Group), 2) global username and password parameters (only if authenticating Server-type IP Group), 3) User Information file, or 4) sends request to users requesting credentials (only if authenticating User-type IP Group).</li> <li><b>[2]</b> SBC as Server = The device authenticates as a server (using the User Information file).</li> </ul> |
| Authentication Method List<br><b>[IPGroup_MethodList]</b>            | <p>Defines SIP methods that the device must challenge. Multiple entries are separated by the backslash "\". If you set this parameter to an empty value, no methods are challenged.</p> <p>The default value is "INVITE\REGISTER".</p> <p><b>Note:</b> This parameter is applicable only if the 'Authentication Mode' parameter is set to SBC as Server [2].</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |



| Parameter                                                                                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                               |
|-------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| SBC Client Forking Mode<br>CLI: enable-sbc-client-forking<br><b>[IPGroup_EnableSBCClient Forking]</b> | <p>Defines call forking of INVITE messages to up to five separate SIP outgoing legs for User-type IP Groups. This occurs if multiple contacts are registered under the same AoR in the device's registration database.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Sequential = (Default) Sequentially sends the INVITE to each contact. If there is no answer from the first contact, it sends the INVITE to the second contact, and so on until a contact answers. If no contact answers, the call fails or is routed to an alternative destination, if configured.</li> <li>▪ <b>[1]</b> Parallel = Sends the INVITE simultaneously to all contacts. The call is established with the first contact that answers.</li> <li>▪ <b>[2]</b> Sequential Available Only = Sequentially sends the INVITE only to available contacts (i.e., not busy). If there is no answer from the first available contact, it sends the INVITE to the second contact, and so on until a contact answers. If no contact answers, the call fails or is routed to an alternative destination, if configured.</li> </ul> <p><b>Note:</b> The device can also fork INVITE messages received for a Request-URI of a specific contact (user) registered in the database to all other users located under the same AoR as the specific contact. This is configured using the SBCSendInviteToAllContacts parameter.</p> |

## 17.4 Configuring Proxy Sets Table

The Proxy Sets Table page allows you to define *Proxy Sets*. A Proxy Set is a group of Proxy servers defined by IP address or fully qualified domain name (FQDN). You can define up to 32 Proxy Sets, each with up to five Proxy server addresses. For each Proxy server address you can define the transport type (i.e., UDP, TCP, or TLS). In addition, Proxy load balancing and redundancy mechanisms can be applied per Proxy Set if it contains more than one Proxy address.

Proxy Sets can later be assigned to Server-type IP Groups (see "Configuring IP Groups" on page 164). When the device sends an INVITE message to an IP Group, it is sent to the IP address or domain name defined for the Proxy Set that is associated with the IP Group. In other words, the Proxy Set represents the **destination** of the call. Typically, for IP-to-IP call routing, at least two Proxy Sets are defined for call destination – one for each leg (IP Group) of the call (i.e., both directions). For example, one Proxy Set for the Internet Telephony Service provider (ITSP) interfacing with one 'leg' of the device and another Proxy Set for the second SIP entity (e.g., ITSP) interfacing with the other 'leg' of the device.



### Notes:

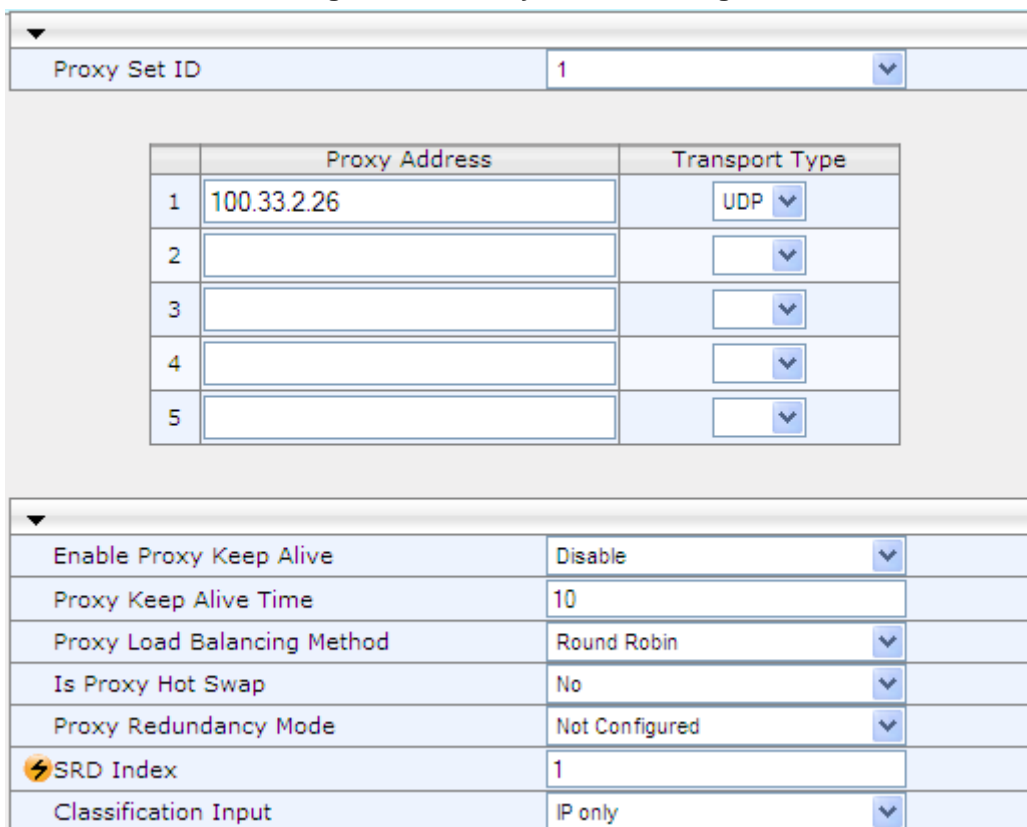
- Proxy Sets can be assigned only to Server-type IP Groups.
- To enable classification of IP Groups according to Proxy Set ID, in the IP Group table, set the 'Classify By Proxy Set' parameter to Enable.
- The Proxy Set table can also be configured using two complementary tables:
  - Proxy Set ID with IP addresses: Table ini file parameter, ProxyIP.
  - Attributes for the Proxy Set: Table ini file parameter, ProxySet.



➤ **To configure Proxy Sets:**

1. Open the Proxy Sets Table page (**Configuration** tab > **VoIP** menu > **Control Network** submenu > **Proxy Sets Table**).

**Figure 17-4: Proxy Sets Table Page**



Proxy Set ID: 1

|   | Proxy Address | Transport Type |
|---|---------------|----------------|
| 1 | 100.33.2.26   | UDP            |
| 2 |               |                |
| 3 |               |                |
| 4 |               |                |
| 5 |               |                |

Enable Proxy Keep Alive: Disable  
 Proxy Keep Alive Time: 10  
 Proxy Load Balancing Method: Round Robin  
 Is Proxy Hot Swap: No  
 Proxy Redundancy Mode: Not Configured  
 SRD Index: 1  
 Classification Input: IP only

2. From the 'Proxy Set ID' drop-down list, select an ID for the desired group.
3. Configure the Proxy parameters, as required. For a description of the parameters, see the table below.
4. Click **Submit**.
5. To save the changes to flash memory, see "Saving Configuration" on page 308.

**Table 17-4: Proxy Sets Table Parameters**

| Parameter                             | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
|---------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Web: Proxy Set ID<br>[ProxySet_Index] | <p>Defines the Proxy Set identification number.</p> <p>The valid value is 0 to 31. Proxy Set ID 0 is used as the default Proxy Set.</p> <p>To summarize, if the default Proxy Set is used, the INVITE message is sent according to the following preferences:</p> <p>Typically, when IP Groups are used, there is no need to use the default Proxy and all routing and registration rules can be configured using IP Groups and the Account tables (see "Configuring Account Table" on page 177).</p> |
| Proxy Address<br>[ProxyIp_IpAddress]  | <p>Defines the address (and optionally, port number) of the Proxy server. Up to five addresses can be configured per Proxy Set.</p> <p>The address can be defined as an IP address in dotted-decimal notation (e.g., 201.10.8.1) or FQDN. You can also specify the port in the format:</p>                                                                                                                                                                                                            |



| Parameter                                                              | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
|------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                        | <ul style="list-style-type: none"> <li>For IPv4 address: &lt;IP address&gt;:&lt;port&gt; (e.g., 201.10.8.1:5060)</li> <li>For IPv6 address: &lt;[IPV6 address]&gt;:&lt;port&gt; (e.g., [2000::1:200:200:86:14]:5060)</li> </ul> <p>If you enable Proxy Redundancy (by setting the parameter EnableProxyKeepAlive to 1 or 2), the device can operate with multiple Proxy servers. If there is no response from the first (<i>primary</i>) Proxy defined in the list, the device attempts to communicate with the other (<i>redundant</i>) Proxies in the list. When a redundant Proxy is located, the device either continues operating with it until the next failure occurs or reverts to the primary Proxy (refer to the parameter ProxyRedundancyMode). If none of the Proxy servers respond, the device goes over the list again.</p> <p>The device also provides real-time switching (Hot-Swap mode) between the primary and redundant proxies (refer to the parameter IsProxyHotSwap). If the first Proxy doesn't respond to the INVITE message, the same INVITE message is immediately sent to the next Proxy in the list. The same logic applies to REGISTER messages (if RegistrarIP is not defined).</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>If EnableProxyKeepAlive is set to 1 or 2, the device monitors the connection with the Proxies by using keep-alive messages (OPTIONS or REGISTER).</li> <li>To use Proxy Redundancy, you must specify one or more redundant Proxies.</li> <li>When a port number is specified (e.g., domain.com:5080), DNS NAPTR/SRV queries aren't performed, even if ProxyDNSQueryType is set to 1 or 2.</li> </ul> |
| Transport Type<br><b>[ProxyIp_TransportType]</b>                       | Defines the transport type of the proxy server. <ul style="list-style-type: none"> <li><b>[0]</b> UDP</li> <li><b>[1]</b> TCP</li> <li><b>[2]</b> TLS</li> <li><b>[-1]</b> = Undefined</li> </ul> <p><b>Note:</b> If no transport type is selected, the value of the global parameter SIPTransportType is used.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Web: Enable Proxy Keep Alive<br><b>[ProxySet_EnableProxyKeepAlive]</b> | Enables the Keep-Alive mechanism with the Proxy server(s). <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default).</li> <li><b>[1]</b> Using Options = Enables Keep-Alive with Proxy using SIP OPTIONS messages.</li> <li><b>[2]</b> Using Register = Enables Keep-Alive with Proxy using SIP REGISTER messages.</li> </ul> <p>If set to 'Using Options', the SIP OPTIONS message is sent every user-defined interval (configured by the parameter ProxyKeepAliveTime). If set to 'Using Register', the SIP REGISTER message is sent every user-defined interval (configured by the SBCProxyRegistrationTime parameter for SBC application). Any response from the Proxy, either success (200 OK) or failure (4xx response) is considered as if the Proxy is communicating correctly.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For Survivability mode for User-type IP Groups, this parameter must be enabled (1 or 2).</li> <li>This parameter must be set to 'Using Options' when Proxy</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |



| Parameter                                                               | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|-------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                         | <p>redundancy is used.</p> <ul style="list-style-type: none"> <li>When this parameter is set to 'Using Register', the homing redundancy mode is disabled.</li> <li>When the active proxy doesn't respond to INVITE messages sent by the device, the proxy is tagged as 'offline'. The behavior is similar to a Keep-Alive (OPTIONS or REGISTER) failure.</li> <li>If this parameter is enabled and the proxy uses the TCP/TLS transport type, you can enable CRLF Keep-Alive mechanism, using the UsePingPongKeepAlive parameter.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Web: Proxy Keep Alive Time<br>[ProxySet_ProxyKeepAliveTime]             | <p>Defines the Proxy keep-alive time interval (in seconds) between Keep-Alive messages.</p> <p>The valid range is 5 to 2,000,000. The default is 60.</p> <p><b>Note:</b> This parameter is applicable only if the parameter EnableProxyKeepAlive is set to 1 (OPTIONS). When the parameter EnableProxyKeepAlive is set to 2 (REGISTER), the time interval between Keep-Alive messages is determined by the SBCProxyRegistrationTime parameter for the SBC application.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Web: Proxy Load Balancing Method<br>[ProxySet_ProxyLoadBalancingMethod] | <p>Enables the Proxy Load Balancing mechanism per Proxy Set ID.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = Load Balancing is disabled (default)</li> <li><b>[1]</b> Round Robin</li> <li><b>[2]</b> Random Weights</li> </ul> <p>When the Round Robin algorithm is used, a list of all possible Proxy IP addresses is compiled. This list includes all IP addresses per Proxy Set, after necessary DNS resolutions (including NAPTR and SRV, if configured). After this list is compiled, the Proxy Keep-Alive mechanism (according to parameters EnableProxyKeepAlive and ProxyKeepAliveTime) tags each entry as 'offline' or 'online'. Load balancing is only performed on Proxy servers that are tagged as 'online'.</p> <p>All outgoing messages are equally distributed across the list of IP addresses. REGISTER messages are also distributed unless a RegistrarIP is configured.</p> <p>The IP addresses list is refreshed according to ProxyIPListRefreshTime. If a change in the order of the entries in the list occurs, all load statistics are erased and balancing starts over again.</p> <p>When the Random Weights algorithm is used, the outgoing requests are not distributed equally among the Proxies. The weights are received from the DNS server by using SRV records. The device sends the requests in such a fashion that each Proxy receives a percentage of the requests according to its assigned weight. A single FQDN should be configured as a Proxy IP address. The Random Weights Load Balancing is not used in the following scenarios:</p> <ul style="list-style-type: none"> <li>The Proxy Set includes more than one Proxy IP address.</li> <li>The only Proxy defined is an IP address and not an FQDN.</li> <li>SRV is not enabled (DNSQueryType).</li> <li>The SRV response includes several records with a different Priority value.</li> </ul> |
| Web: Is Proxy Hot-Swap<br>[ProxySet_IsProxyHotSwap]                     | <p>Enables the Proxy Hot-Swap redundancy mode.</p> <ul style="list-style-type: none"> <li><b>[0]</b> No (default)</li> <li><b>[1]</b> Yes</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |



| Parameter                                                     | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
|---------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                               | <p>If Proxy Hot-Swap is enabled, the SIP INVITE/REGISTER message is initially sent to the first Proxy/Registrar server. If there is no response from the first Proxy/Registrar server after a specific number of retransmissions (configured by the parameter HotSwapRtx), the message is resent to the next redundant Proxy/Registrar server.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| Web: Redundancy Mode<br><b>[ProxySet_ProxyRedundancyMode]</b> | <p>Determines whether the device switches back to the primary Proxy after using a redundant Proxy.</p> <ul style="list-style-type: none"> <li>▪ <b>[-1]</b> Not configured = (Default) The global parameter, ProxyRedundancyMode applies.</li> <li>▪ <b>[0]</b> Parking = The device continues operating with a redundant (now active) Proxy until the next failure, after which it operates with the next redundant Proxy.</li> <li>▪ <b>[1]</b> Homing = The device always attempts to operate with the primary Proxy server (i.e., switches back to the primary Proxy whenever it's available).</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ To use the Proxy Redundancy mechanism, you need to enable the keep-alive with Proxy option, by setting the parameter EnableProxyKeepAlive to 1 or 2.</li> <li>▪ If this parameter is configured, then the global parameter is ignored.</li> </ul> |
| Web: SRD Index<br><b>[ProxySet_ProxySet_SRD]</b>              | <p>Defines the SRD associated with the Proxy Set ID. The default is SRD 0.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ For this parameter to take effect, a device reset is required.</li> <li>▪ To configure SRDs, see Configuring SRD Table on page 159.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Web: Classification Input<br><b>[ClassificationInput]</b>     | <p>Defines how the device classifies an IP call to the Proxy Set.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Compare only IP = (Default) The call is classified to the Proxy Set according to its IP address only.</li> <li>▪ <b>[1]</b> Compare IP, port and transport type = The call is classified to the Proxy Set according to its IP address, port, and transport type.</li> </ul> <p><b>Note:</b> This parameter is applicable only if the IP Group table's parameter, 'Classify by Proxy Set' is set to Enable.</p>                                                                                                                                                                                                                                                                                                                                                                                      |



## Reader's Notes



## 18 SIP Definitions

This section describes configuration of SIP parameters.

### 18.1 Configuring SIP Parameters

Many of the stand-alone SIP parameters associated with various features can be configured in the following pages:

- **SIP General Parameters page:** Provides SIP parameters for configuring general SIP features. To access this page, use the following path: **Configuration** tab > **VoIP** menu > **SIP Definitions** > **General Parameters**.
- **SIP Advanced Parameters page:** Provides SIP parameters for configuring advanced SIP features. To access this page, use the following path: **Configuration** tab > **VoIP** menu > **SIP Definitions** > **Advanced Parameters**.

For a description of these parameters, refer to the section corresponding to the feature or see "Configuration Parameters Reference" on page 387.

### 18.2 Configuring Account Table

The Account Table page lets you define up to 32 Accounts per source ("served") IP Group. Accounts are used to register and/or digest authenticate a served IP Group, using a username and password, to a destination ("serving") IP Group. For example, the device can use the Account table to register an IP PBX, which is connected to the device, to an ITSP. The device sends the registration requests to the Proxy Set ID (see 'Configuring Proxy Sets Table' on page 171) that is associated with the serving IP Group.

A served IP Group can register to more than one serving IP Group (e.g., multiple ITSPs). This is done by configuring multiple entries in the Account table for the same served IP Group, but with different serving IP Groups, user name/password, host name, and contact user values.



**Note:** The Account table can also be configured using the table ini file parameter, Account.

#### ➤ To configure Accounts:

1. Open the Account Table page (**Configuration** tab > **VoIP** menu > **SIP Definitions** submenu > **Account Table**).

**Figure 18-1: Account Table Page**

| Index | Served Trunk Group | Serving IP Group | User Name | Password | Host Name | Register | Contact User | Application Type |
|-------|--------------------|------------------|-----------|----------|-----------|----------|--------------|------------------|
| 1     | -1                 | 1                |           | *        |           | No       |              | SBC              |

2. In the 'Add' field, enter the desired table row index, and then click **Add**. A new row appears.
3. Configure the Account parameters according to the table below.
4. Click the **Apply** button to save your changes.
5. To save the changes, see "Saving Configuration" on page 308.
6. To perform registration, click the **Register** button; to unregister, click **Unregister**. The registration method for each Trunk Group is according to the setting of the 'Registration Mode' parameter in the Trunk Group Settings page.



Table 18-1: Account Table Parameters Description

| Parameter                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
|----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Served IP Group<br>[Account_ServedIPGroup]   | Defines the Source IP Group (e.g., IP-PBX) for which registration and/or authentication is done.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| Serving IP Group<br>[Account_ServingIPGroup] | <p>Defines the destination IP Group ID to where the SIP REGISTER requests, if enabled, are sent and authentication is done. The actual destination to where the REGISTER requests are sent is the IP address configured for the Proxy Set ID that is associated with the IP Group.</p> <p>Registration occurs only if the 'Register' parameter in this Account table is set to <b>Yes</b>.</p> <p><b>Note:</b> If no match is found in this table for incoming or outgoing calls, the username and password is taken from the UserName and Password parameters on the Proxy &amp; Registration page.</p>                                                                                                                                                                                                   |
| Username<br>[Account_Username]               | <p>Defines the digest MD5 Authentication user name.</p> <p>The valid value is a string of up to 50 characters.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Password<br>[Account_Password]               | <p>Defines the digest MD5 Authentication password.</p> <p>The valid value is a string of up to 50 characters.</p> <p><b>Note:</b> After you click the <b>Apply</b> button, this password is displayed as an asterisk (*).</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| Host Name<br>[Account_HostName]              | <p>Defines the Address of Record (AOR) host name. It appears in REGISTER From/To headers as ContactUser@HostName. For successful registrations, this host name is also included in the INVITE request's From header URI.</p> <p>This parameter can be up to 49 characters.</p> <p><b>Note:</b> If this parameter is not configured or if registration fails, the 'SIP Group Name' parameter configured in the IP Group table is used instead.</p>                                                                                                                                                                                                                                                                                                                                                          |
| Register<br>[Account_Register]               | <p>Enables registration.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> No (Default)</li> <li>▪ <b>[1]</b> Yes</li> </ul> <p>When enabled, the device sends REGISTER requests to the Serving IP Group. The host name (i.e., host name in SIP From/To headers) and Contact User (user in From/To and Contact headers) are taken from this table upon successful registration. See the example below:</p> <pre>REGISTER sip:xyz SIP/2.0 Via: SIP/2.0/UDP 10.33.37.78;branch=z9hG4bKac1397582418 From: &lt;sip:ContactUser@HostName&gt;;tag=1c1397576231 To: &lt;sip: ContactUser@HostName &gt; Call-ID: 1397568957261200022256@10.33.37.78 CSeq: 1 REGISTER Contact: &lt;sip:ContactUser@10.33.37.78&gt;;expires=3600 Expires: 3600 User-Agent: Sip-Gateway/v.6.00A.008.002 Content-Length: 0</pre> |
| Contact User<br>[Account_ContactUser]        | <p>Defines the AOR user name. This appears in REGISTER From/To headers as ContactUser@HostName, and in INVITE/200 OK Contact headers as ContactUser@&lt;device's IP address&gt;.</p> <p><b>Notes:</b></p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |



| Parameter                                     | Description                                                                                                                                                                                                                                                                  |
|-----------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                               | <ul style="list-style-type: none"> <li>If this parameter is not configured, the 'Contact User' parameter in the IP Group table is used instead.</li> <li>If registration fails, then the user part in the INVITE Contact header contains the source party number.</li> </ul> |
| Application Type<br>[Account_ApplicationType] | Defines the application type: <ul style="list-style-type: none"> <li>[2] SBC = SBC application.</li> </ul>                                                                                                                                                                   |


## 18.3 Configuring Proxy and Registration Parameters

The Proxy & Registration page allows you to configure the Proxy server and registration parameters. For a description of the parameters appearing on this page, see "Configuration Parameters Reference" on page 387.

➤ **To configure the Proxy and registration parameters:**

1. Open the Proxy & Registration page (**Configuration** tab > **VoIP** menu > **SIP Definitions** submenu > **Proxy & Registration**).

**Figure 18-2: Proxy & Registration Page**


|                                               |                                                                                     |
|-----------------------------------------------|-------------------------------------------------------------------------------------|
| Use Default Proxy                             | Yes                                                                                 |
| Proxy Set Table                               |  |
| Proxy Name                                    | <input type="text"/>                                                                |
| Redundancy Mode                               | Parking                                                                             |
| Proxy IP List Refresh Time                    | 60                                                                                  |
| Enable Fallback to Routing Table              | Disable                                                                             |
| Prefer Routing Table                          | No                                                                                  |
| Use Routing Table for Host Names and Profiles | Disable                                                                             |
| Always Use Proxy                              | Disable                                                                             |
| Redundant Routing Mode                        | Routing Table                                                                       |
| SIP ReRouting Mode                            | Standard Mode                                                                       |
| Enable Registration                           | Disable                                                                             |
| Gateway Name                                  | <input type="text"/>                                                                |
| Gateway Registration Name                     | <input type="text"/>                                                                |
| DNS Query Type                                | A-Record                                                                            |
| Proxy DNS Query Type                          | A-Record                                                                            |
| Subscription Mode                             | Per Endpoint                                                                        |
| Number of RTX Before Hot-Swap                 | 3                                                                                   |
| Use Gateway Name for OPTIONS                  | No                                                                                  |
| User Name                                     | joe                                                                                 |
| Password                                      | mikey                                                                               |
| Cnonce                                        | Default_Cnonce                                                                      |
| Registration Mode                             | Per Endpoint                                                                        |
| Set Out-Of-Service On Registration Failure    | Disable                                                                             |
| Challenge Caching Mode                        | None                                                                                |
| Mutual Authentication Mode                    | Optional                                                                            |



2. Configure the parameters as required.
  3. Click **Submit** to apply your changes.
- **To register or un-register the device to a Proxy/Registrar:**
- Click the **Register** button to register.
  - Click **Un-Register** button to un-register.

Instead of registering the entire device, you can register specific entities as listed below by using the **Register** button located on the page in which these entities are configured:

- Accounts - Account table (see "Configuring Account Table" on page 177)

Click the **Proxy Set Table**  button to Open the Proxy Sets Table page to configure groups of proxy addresses. Alternatively, you can open this page from the **Proxy Sets Table** page item (see "Configuring Proxy Sets Table" on page 171 for a description of this page).

### 18.3.1 SIP Message Authentication Example

The device supports basic and digest (MD5) authentication types, according to SIP RFC 3261 standard. A proxy server might require authentication before forwarding an INVITE message. A Registrar/Proxy server may also require authentication for client registration. A proxy replies to an unauthenticated INVITE with a 407 Proxy Authorization Required response, containing a Proxy-Authenticate header with the form of the challenge. After sending an ACK for the 407, the user agent can then re-send the INVITE with a Proxy-Authorization header containing the credentials.

User agents, Redirect or Registrar servers typically use the SIP 401 Unauthorized response to challenge authentication containing a WWW-Authenticate header, and expect the re-INVITE to contain an Authorization header.

The following example shows the Digest Authentication procedure, including computation of user agent credentials:

1. The REGISTER request is sent to a Registrar/Proxy server for registration:

```
REGISTER sip:10.2.2.222 SIP/2.0
Via: SIP/2.0/UDP 10.1.1.200
From: <sip: 122@10.1.1.200>;tag=1c17940
To: <sip: 122@10.1.1.200>
Call-ID: 634293194@10.1.1.200
User-Agent: Sip-Gateway/Mediant Software E-SBC/v.6.60.010.006
CSeq: 1 REGISTER
Contact: sip:122@10.1.1.200:
Expires:3600
```

2. Upon receipt of this request, the Registrar/Proxy returns a 401 Unauthorized response:

```
SIP/2.0 401 Unauthorized
Via: SIP/2.0/UDP 10.2.1.200
From: <sip:122@10.2.2.222 >;tag=1c17940
To: <sip:122@10.2.2.222 >
Call-ID: 634293194@10.1.1.200
Cseq: 1 REGISTER
Date: Mon, 30 Jul 2012 15:33:54 GMT
Server: Columbia-SIP-Server/1.17
Content-Length: 0
WWW-Authenticate: Digest realm="audiocodes.com",
nonce="11432d6bce58ddf02e3b5e1c77c010d2",
stale=FALSE,
algorithm=MD5
```



3. According to the sub-header present in the WWW-Authenticate header, the correct REGISTER request is created.
4. Since the algorithm is MD5:
  - The username is equal to the endpoint phone number "122".
  - The realm return by the proxy is "audiocodes.com".
  - The password from the *ini* file is "AudioCodes".
  - The equation to be evaluated is "122:audiocodes.com:AudioCodes". According to the RFC, this part is called A1.
  - The MD5 algorithm is run on this equation and stored for future usage.
  - The result is "a8f17d4b41ab8dab6c95d3c14e34a9e1".
5. The par called A2 needs to be evaluated:
  - The method type is "REGISTER".
  - Using SIP protocol "sip".
  - Proxy IP from *ini* file is "10.2.2.222".
  - The equation to be evaluated is "REGISTER:sip:10.2.2.222".
  - The MD5 algorithm is run on this equation and stored for future usage.
  - The result is "a9a031cfddcb10d91c8e7b4926086f7e".
6. Final stage:
  - A1 result: The nonce from the proxy response is "11432d6bce58ddf02e3b5e1c77c010d2".
  - A2 result: The equation to be evaluated is "A1:11432d6bce58ddf02e3b5e1c77c010d2:A2".
  - The MD5 algorithm is run on this equation. The outcome of the calculation is the response needed by the device to register with the Proxy.
  - The response is "b9c45d0234a5abf5ddf5c704029b38cf".

At this time, a new REGISTER request is issued with the following response:

```
REGISTER sip:10.2.2.222 SIP/2.0
Via: SIP/2.0/UDP 10.1.1.200
From: <sip: 122@10.1.1.200>;tag=1c23940
To: <sip: 122@10.1.1.200>
Call-ID: 654982194@10.1.1.200
Server: Audiocodes-Sip-Gateway/Mediant Software E-
SBC/v.6.60.010.006
CSeq: 1 REGISTER
Contact: sip:122@10.1.1.200:
Expires:3600
Authorization: Digest, username: 122,
realm="audiocodes.com",
nonce="11432d6bce58ddf02e3b5e1c77c010d2",
uri="10.2.2.222",
response="b9c45d0234a5abf5ddf5c704029b38cf"
```

7. Upon receiving this request and if accepted by the Proxy, the Proxy returns a 200 OK response, completing the registration transaction:

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.1.1.200
From: <sip: 122@10.1.1.200>;tag=1c23940
To: <sip: 122@10.1.1.200>
Call-ID: 654982194@10.1.1.200
Cseq: 1 REGISTER
Date: Thu, 26 Jul 2012 09:34:42 GMT
```



```
Server: Columbia-SIP-Server/1.17
Content-Length: 0
Contact: <sip:122@10.1.1.200>; expires="Thu, 26 Jul 2012
10:34:42 GMT"; action=proxy; q=1.00
Contact: <122@10.1.1.200:>; expires="Tue, 19 Jan 2038 03:14:07
GMT"; action=proxy; q=0.00
Expires: Thu, 26 Jul 2012 10:34:42 GMT
```

## 18.4 Configuring SIP Message Manipulation

The Message Manipulations page allows you to define up to 100 SIP message manipulation rules. Each manipulation rule can be assigned any Manipulation Set ID (0 to 19), enabling you to create groups (sets) of manipulation rules whereby rules of a group are configured with the same Manipulation Set ID number. To use these Manipulation Sets, you need to assign them to IP Groups in the IP Group table (see 'Configuring IP Groups' on page 164) where they can be applied to inbound and/or outbound SIP messages.

SIP message manipulation enables the normalization of SIP messaging fields between communicating network segments. For example, it allows service providers to design their own policies on the SIP messaging fields that must be present before a SIP call enters their network. Similarly, enterprises and small businesses may have policies for the information that can enter or leave their networks for policy or security reasons from a service provider. The manipulations can also be implemented to resolve incompatibilities between SIP devices inside the enterprise network.

SIP message manipulation supports the following:

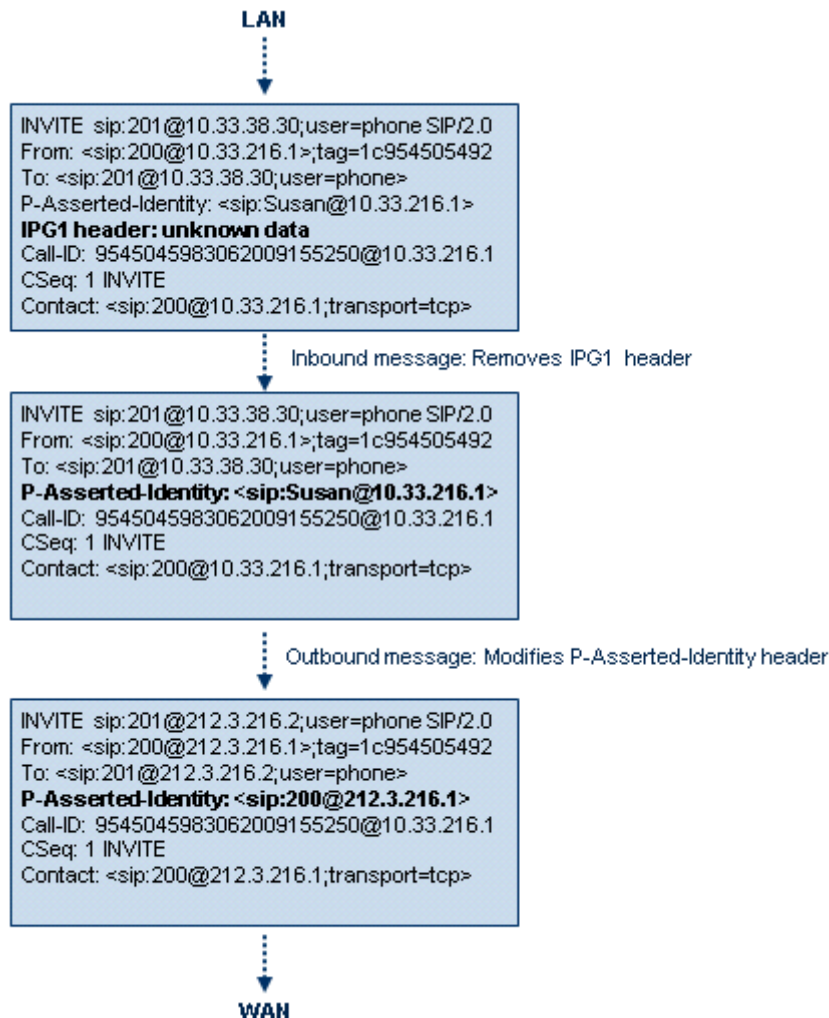
- Addition of new headers.
- Removal of headers ("Black list").
- Modification of header components - value, header value (e.g., URI value of the P-Asserted-Identity header can be copied to the From header), call's parameter values.
- Deletion of SIP body (e.g., if a message body isn't supported at the destination network this body is removed).
- Translating one SIP response code to another.
- Topology hiding (generally present in SIP headers such as Via, Record Route, Route and Service-Route).
- Configurable identity hiding (information related to identity of subscribers for example, P-Asserted-Identity, Referred-By, Identity and Identity-Info).
- Apply conditions per rule - the condition can be on parts of the message or call's parameters.
- Multiple manipulation rules on the same SIP message.

The manipulation is performed on SIP messages according to the Classification table (source/destination of username/host prefixes, and source IP address). The manipulation can be performed on message type (Method, Request/Response, and Response type) and multiple manipulation rules can be configured for the same SIP message.



The figure below illustrates a SIP message manipulation example:

**Figure 18-3: SIP Header Manipulation Example**



**Notes:**

- For a detailed description of the syntax for configuring SIP message manipulation rules, refer to *SIP Message Manipulations Quick Reference Guide*.
- The values entered in the table are not case-sensitive.
- For the SBC application, SIP message manipulation is done only after the Classification, inbound/outbound number manipulations, and routing processes.
- Each message can be manipulated twice - on the source leg and on the destination leg (i.e., source and destination IP Groups).
- Unknown SIP parts can only be added or removed.
- SIP manipulations do not allow you to remove or add mandatory SIP headers. They can only be modified and only on requests that initiate new dialogs. Mandatory SIP headers include To, From, Via, CSeq, Call-Id, and Max-Forwards.
- The Message Manipulations table can also be configured using the table *ini* file parameter, MessageManipulations.

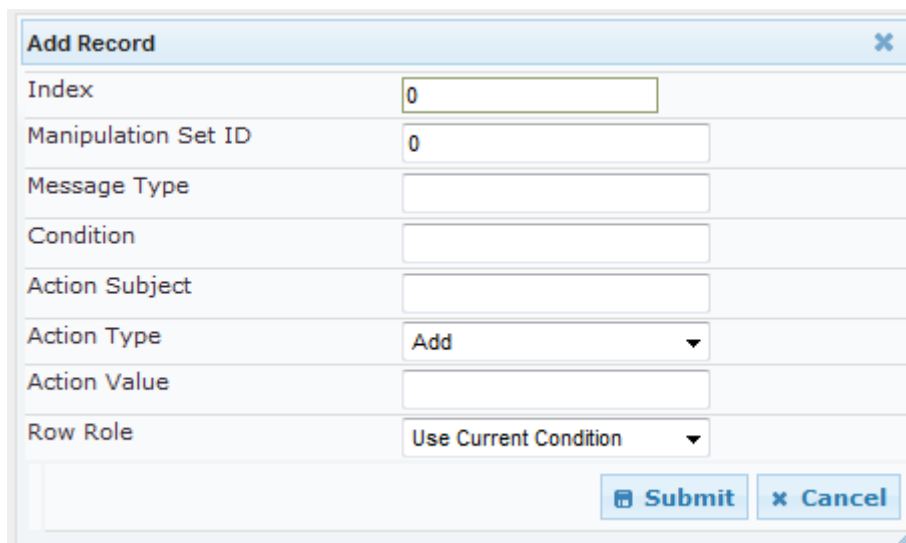




➤ **To configure SIP message manipulation rules:**

1. Open the Message Manipulations page (**Configuration** tab > **VoIP** menu > **SIP Definitions** submenu > **Msg Policy & Manipulation** > **Message Manipulations**).
2. Click the **Add** button; the following dialog box appears:

**Figure 18-4: Message Manipulations Table - Add Record Dialog Box**



3. Configure the SIP message manipulation rule as required. See the table below for a description of each parameter.
4. Click **Submit** to apply your changes.

The figure below displays an example of configured message manipulation rules:

- Index 0 - adds the suffix ".com" to the host part of the To header.
- Index 1 - changes the user part of the From header to the user part of the P-Asserted-ID.
- Index 2 - changes the user part of the SIP From header to "200".
- Index 3 - if the user part of the From header equals "unknown", then it is changed according to the srcIPGroup call's parameter.
- Index 4 - removes the Priority header from an incoming INVITE message.

**Figure 18-5: Message Manipulations Page**

| Index | Manipulation Set ID | Message Type        | Condition                   | Action Subject       | Action Type | Action Value                  |
|-------|---------------------|---------------------|-----------------------------|----------------------|-------------|-------------------------------|
| 0     | 0                   | invite.response.200 |                             | header.to.url.user   | Add Prefix  | '.com'                        |
| 1     | 1                   | invite.response.200 |                             | header.from.url.user | Modify      | header.p-asserted-id.url.user |
| 2     | 2                   | invite.request      |                             | header.from.url.user | Modify      | '200'                         |
| 3     | 3                   | invite.request      | header.from.url.user=='Unkn | header.from.url.user | Modify      | param.ipq.src.user            |
| 4     | 4                   | invite.request      |                             | header.priority      | Remove      |                               |

**Table 18-2: Message Manipulations Parameters**

| Parameter                                                                          | Description                                                                                                                                                                                                                                                                          |
|------------------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Index<br>[MessageManipulations_Index]                                              | Defines the table row index for the rule.<br>The valid value is 0 to 99. The default is 0.<br><b>Note:</b> Each rule must be configured with a unique index.                                                                                                                         |
| Manipulation Set ID<br>CLI: manipulation-set-id<br>[MessageManipulations_ManSetID] | Defines a Manipulation Set ID for the rule. You can define the same Manipulation Set ID for multiple rules to create a group of rules. The Manipulation Set ID is used to assign the manipulation rules to an IP Group (in the IP Group table) for inbound and/or outbound messages. |



| Parameter                                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
|------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                            | The valid value is 0 to 19. The default is 0.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| <b>Matching Characteristics</b>                            |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Message Type<br>[MessageManipulations<br>_MessageType]     | <p>Defines the SIP message type that you want to manipulate.<br/>The valid value is a string denoting the SIP message.<br/>For example:</p> <ul style="list-style-type: none"> <li>▪ Empty = rule applies to all messages</li> <li>▪ Invite = rule applies to all INVITE requests and responses</li> <li>▪ Invite.Request = rule applies to INVITE requests</li> <li>▪ Invite.Response = rule applies to INVITE responses</li> <li>▪ subscribe.response.2xx = rule applies to SUBSCRIBE confirmation responses</li> </ul> <p><b>Note:</b> Currently, SIP 100 Trying messages cannot be manipulated.</p>                                                                                                                                                                           |
| Condition<br>[MessageManipulations<br>_Condition]          | <p>Defines the condition that must exist for the rule to apply.<br/>The valid value is a string.<br/>For example:</p> <ul style="list-style-type: none"> <li>▪ header.from.url.user== '100' (indicates that the user part of the From header must have the value "100")</li> <li>▪ header.contact.param.expires &gt; '3600'</li> <li>▪ header.to.url.host contains 'domain'</li> <li>▪ param.call.dst.user != '100'</li> </ul>                                                                                                                                                                                                                                                                                                                                                    |
| <b>Operation</b>                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Action Subject<br>[MessageManipulations<br>_ActionSubject] | Defines the SIP header upon which the manipulation is performed.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Action Type<br>[MessageManipulations<br>_ActionType]       | <p>Defines the type of manipulation.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Add (default) = adds new header/param/body (header or parameter elements).</li> <li>▪ <b>[1]</b> Remove = removes header/param/body (header or parameter elements).</li> <li>▪ <b>[2]</b> Modify = sets element to the new value (all element types).</li> <li>▪ <b>[3]</b> Add Prefix = adds value at the beginning of the string (string element only).</li> <li>▪ <b>[4]</b> Add Suffix = adds value at the end of the string (string element only).</li> <li>▪ <b>[5]</b> Remove Suffix = removes value from the end of the string (string element only).</li> <li>▪ <b>[6]</b> Remove Prefix = removes value from the beginning of the string (string element only).</li> </ul> |
| Action Value<br>[MessageManipulations<br>_ActionValue]     | <p>Defines a value (string) that you want to use in the manipulation.<br/>The syntax is as follows:</p> <ul style="list-style-type: none"> <li>▪ string/&lt;message-element&gt;/&lt;call-param&gt; +</li> <li>▪ string/&lt;message-element&gt;/&lt;call-param&gt;</li> </ul> <p>For example:</p> <ul style="list-style-type: none"> <li>▪ 'itsp.com'</li> <li>▪ header.from.url.user</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                   |



| Parameter                                      | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                | <ul style="list-style-type: none"> <li>param.call.dst.user</li> <li>param.call.dst.host + '.com'</li> <li>param.call.src.user + '&lt;' + header.from.url.user + '@' + header.p-asserted-id.url.host + '&gt;'</li> </ul> <p><b>Note:</b> Only single quotation marks must be used.</p>                                                                                                                                                                                                                                                                                                                                                                                |
| Row Role<br>[MessageManipulations<br>_RowRole] | <p>Determines which condition must be used for the rule of this table row.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Use Current Condition = The condition entered in this row must be matched in order to perform the defined action (default).</li> <li><b>[1]</b> Use Previous Condition = The condition of the rule configured directly above this row must be used in order to perform the defined action. This option allows you to configure multiple actions for the same condition.</li> </ul> <p><b>Note:</b> When multiple manipulations rules apply to the same header, the next rule applies to the result string of the previous rule.</p> |

## 18.5 Configuring SIP Message Policy Rules

You can configure SIP message policy rules for blocking (blacklist) unwanted incoming SIP messages or allowing (whitelist) receipt of desired messages. This feature allows you to define legal and illegal characteristics of a SIP message. Message policies can be applied globally (default) or per signaling domain by assigning it to a SIP interface in the SIP Interface table (see "Configuring SIP Interface Table" on page 161).

This feature is helpful against VoIP fuzzing (also known as robustness testing), which sends different types of packets to its "victims" for finding bugs and vulnerabilities. For example, the attacker might try sending a SIP message containing either an over-sized parameter or too many occurrences of a parameter.

Each message policy rule can be configured with the following:

- Maximum message length
- Maximum SIP header length
- Maximum message body length
- Maximum number of headers
- Maximum number of bodies
- Option to send 400 "Bad Request" response if message request is rejected
- Blacklist and whitelist for defined SIP methods (e.g., INVITE)
- Blacklist and whitelist for defined SIP bodies



**Note:** The Message Policy table can also be configured using the table ini file parameter, MessagePolicy.



➤ **To configure SIP message policy rules:**

1. Open the Message Policy Table page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Msg Policy & Manipulation** > **Message Policy Table**).
2. Click the **Add** button; the Add Record dialog box appears:

**Figure 18-6: Message Policy Table - Add Record Dialog Box**

|                    |                  |
|--------------------|------------------|
| Index              | 1                |
| Max Message Length | 1400             |
| Max Header Length  | 300              |
| Max Body Length    | 300              |
| Max Num Headers    | 20               |
| Max Num Bodies     | 5                |
| Send Rejection     | Policy Reject    |
| Method List        | INVITE/REFER     |
| Method List Type   | Policy Blacklist |
| Body List          |                  |
| Body List Type     | Policy Blacklist |

The policy defined above limits SIP messages to 32,768 characters, headers to 256 characters, bodies to 512 characters, number of headers to 16, and only permits two bodies. Invalid requests are rejected. Only INVITE and BYE requests are permitted and there are no restrictions on bodies.

3. Configure the SIP message policy rule as required. See the table below for a description of each parameter.
4. Click **Submit** to apply your changes.
5. To save the changes to flash memory, see "Saving Configuration" on page 308.

**Table 18-3: SIP Message Policy Parameters**

| Parameter                                              | Description                                                                                                                                                                                                                                                                                                                             |
|--------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Index<br>[MessagePolicy_Index]                         | Defines the table index entry.                                                                                                                                                                                                                                                                                                          |
| Max Message Length<br>[MessagePolicy_MaxMessageLength] | Defines the maximum SIP message length.<br>The valid value is up to 32,768 characters. The default is 32,768.                                                                                                                                                                                                                           |
| Max Header Length<br>[MessagePolicy_MaxHeaderLength]   | Defines the maximum SIP header length.<br>The valid value is up to 512 characters. The default is 512.                                                                                                                                                                                                                                  |
| Max Body Length<br>[MessagePolicy_MaxBodyLength]       | Defines the maximum SIP message body length. This is the value of the Content-Length header.<br>The valid value is up to 1,024 characters. The default is 1,024.                                                                                                                                                                        |
| Max Num Headers<br>[MessagePolicy_MaxNumHeaders]       | Defines the maximum number of SIP headers.<br>The valid value is any number up to 32. The default is 32.<br><b>Note:</b> The device supports up to 20 SIP Record-Route headers that can be received in a SIP INVITE request or 200 OK response. If it receives more than this, it responds with a SIP 513 'Message Too Large' response. |



| Parameter                                                 | Description                                                                                                                                                                                                                                                                                                                                                                       |
|-----------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Max Num Bodies<br><b>[MessagePolicy_MaxNumBodies]</b>     | Defines the maximum number of bodies (e.g., SDP) in the SIP message.<br><br>The valid value is any number up to 8. The default is 8.                                                                                                                                                                                                                                              |
| Send Rejection<br><b>[MessagePolicy_SendRejection]</b>    | Determines whether the device sends a 400 "Bad Request" response if a message request is rejected. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Policy Reject = (Default) If the message is a request, then the device sends a response to reject the request.</li> <li>▪ <b>[1]</b> Policy Drop = The device ignores the message without sending any response.</li> </ul> |
| Method List<br><b>[MessagePolicy_MethodList]</b>          | Defines the SIP methods (e.g., INVITE\BYE) to which the rule applies. The syntax for entering the methods is as follows: <ul style="list-style-type: none"> <li>▪ Methods must be separated by a backslash (\).</li> <li>▪ The entered value is not case sensitive.</li> </ul>                                                                                                    |
| Method List Type<br><b>[MessagePolicy_MethodListType]</b> | Determines the policy for the SIP methods. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Policy Blacklist = The specified methods (in the 'Method List' field) are rejected by the policy.</li> <li>▪ <b>[1]</b> Policy Whitelist = (Default) The specified methods (in the 'Method List' field) are allowed by the policy.</li> </ul>                                      |
| Body List<br><b>[MessagePolicy_BodyList]</b>              | Defines the SIP body (i.e., value of the Content-Type header) to which the rule applies.                                                                                                                                                                                                                                                                                          |
| Body List Type<br><b>[MessagePolicy_BodyListType]</b>     | Determines the policy for the defined SIP body. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Policy Blacklist = The specified SIP body (in the 'Body List' field) is rejected by the policy.</li> <li>▪ <b>[1]</b> Policy Whitelist = (Default) The specified SIP body (in the 'Body List' field) is allowed by the policy.</li> </ul>                                     |



## 19 Configuring IP Profiles

The IP Profile Settings table allows you to define up to nine *IP Profiles*. An IP Profile is a set of special call configuration behaviors relating to signaling (e.g., SIP message terminations such as REFER) and media (e.g., coder used) applied to specific IP calls (inbound and/or outbound). Therefore, IP Profiles provide high-level adaptation when the device interworks between different IP entities (for Tel and IP sides), each of which may require different handling by the device. For example, if a specific IP entity uses the G.711 coder only, you can configure an IP Profile with G.711 for this IP entity.

Many of the parameters in the IP Profile Settings table have a corresponding "global" parameter. If an IP Profile is not associated with specific calls, the settings of the global parameters are applied to these calls.

IP Profiles are assigned to IP Groups - see Configuring IP Groups on page 164.



### Notes:

- IP Profiles can also be implemented when using a Proxy server (when the AlwaysUseRouteTable parameter is set to 1).
- RxDTMFOption configures the received DTMF negotiation method: [-1] not configured, use the global parameter; [0] don't declare RFC 2833; [1] declare RFC 2833 payload type is SDP.
- You can also configure IP Profiles using the table ini file parameter, IPProfile (see Configuration Parameters Reference on page 387).

### ➤ To configure IP Profiles:

1. Open the IP Profile Settings page (**Configuration** tab > **VoIP** menu > **Coders and Profiles** submenu > **IP Profile Settings**).
2. From the 'Profile ID' drop-down list, select the IP Profile index.
3. In the 'Profile Name' field, enter an arbitrary name that allows you to easily identify the IP Profile.
4. From the 'Profile Preference' drop-down list, select the priority of the IP Profile, where '1' is the lowest priority and '20' is the highest. If both IP and Tel profiles apply to the same call, the coders and other common parameters (noted by an asterisk) of the preferred Profile are applied to that call. If the Preference of the Tel and IP Profiles is identical, the Tel Profile parameters are applied.  
**Note:** If the coder lists of both IP and Tel Profiles apply to the same call, only the coders common to both are used. The order of the coders is determined by the preference.
5. Configure the parameters as required.
6. Click **Submit** to apply your changes.

**Table 19-1: IP Profile Parameters Description**

| Parameter                                    | Description                                               |
|----------------------------------------------|-----------------------------------------------------------|
| Web: Profile ID<br>[IpProfile_Index]         | Defines a unique index number for the IP Profile.         |
| Web: Profile Name<br>[IpProfile_ProfileName] | (Optional) Defines a descriptive name for the IP Profile. |
| <b>Common Parameters</b>                     |                                                           |
| Web: RTP IP DiffServ                         | For a description, see the global parameter               |



| Parameter                                                                                     | Description                                                                     |
|-----------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------|
| <b>[IpProfile_IPDiffServ]</b>                                                                 | PremiumServiceClassMediaDiffServ.                                               |
| Web: Signaling DiffServ<br><b>[IpProfile_SigIPDiffServ]</b>                                   | For a description, see the global parameter PremiumServiceClassControlDiffServ. |
| Web: Disconnect on Broken Connection<br><b>[IpProfile_DisconnectOnBrokenConnection]</b>       | For a description, see the global parameter DisconnectOnBrokenConnection.       |
| Web: Media IP Version Preference<br><b>[IpProfile_MediaIPVersionPreference]</b>               | For a description, see the global parameter MediaIPVersionPreference.           |
| Web: Dynamic Jitter Buffer Minimum Delay<br><b>[IpProfile_JitterBufMinDelay]</b>              | For a description, see the global parameter DJBufMinDelay.                      |
| Web: Dynamic Jitter Buffer Optimization Factor<br><b>[IpProfile_JitterBufOptFactor]</b>       | For a description, see the global parameter DJBufOptFactor.                     |
| Web: RTP Redundancy Depth<br><b>[IpProfile_RTPRedundancyDepth]</b>                            | For a description, see the global parameter RTPRedundancyDepth.                 |
| Web: Echo Canceled<br><b>[IpProfile_EnableEchoCanceller]</b>                                  | For a description, see the global parameter EnableEchoCanceller.                |
| Web: Input Gain<br><b>[IpProfile_InputGain]</b>                                               | For a description, see the global parameter InputGain.                          |
| Web: Voice Volume<br><b>[IpProfile_VoiceVolume]</b>                                           | For a description, see the global parameter VoiceVolume.                        |
| Web: Symmetric MKI Negotiation<br><b>[IpProfile_EnableSymmetricMKI]</b>                       | For a description, see the global parameter EnableSymmetricMKI.                 |
| Web: MKI Size<br><b>[IpProfile_MKISize]</b>                                                   | For a description, see the global parameter SRTPTxPacketMKISize.                |
| Web: Fax Signaling Method<br><b>[IpProfile_IsFaxUsed]</b>                                     | For a description, see the global parameter IsFaxUsed.                          |
| Web: Play Ringback Tone to IP<br><b>[IpProfile_PlayRBTone2IP]</b>                             | For a description, see the global parameter PlayRBTone2IP.                      |
| Web: Enable Early Media<br><b>[IpProfile_EnableEarlyMedia]</b>                                | For a description, see the global parameter EnableEarlyMedia.                   |
| Web: Copy Destination Number to Redirect Number<br><b>[IpProfile_CopyDest2RedirectNumber]</b> | For a description, see the global parameter CopyDest2RedirectNumber.            |
| Web: Media Security Behavior<br><b>[IpProfile_MediaSecurityBehaviour]</b>                     | For a description, see the global parameter MediaSecurityBehaviour.             |



| Parameter                                                                  | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |
|----------------------------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Web: Number of Calls Limit<br><b>[IpProfile_CallLimit]</b>                 | <p>Defines the maximum number of concurrent calls (incoming and outgoing). If the number of concurrent calls reaches this limit, the device rejects any new incoming and outgoing calls belonging to this IP Profile.</p> <p>This parameter can also be set to the following:</p> <ul style="list-style-type: none"> <li>▪ <b>[-1]</b> = (Default) No limitation on calls.</li> <li>▪ <b>[0]</b> = Calls are rejected.</li> </ul> <p><b>Note:</b> For IP-to-IP calls, you can configure the device to route calls to an alternative IP Group when this maximum number of concurrent calls is reached. To do so, you need to add an alternative routing rule in the Outbound IP Routing table that reroutes the call to an alternative IP Group. You also need to add a rule to the Reason for Alternative Routing table to initiate an alternative rule for Tel-to-IP calls using cause 805.</p> |
| Web: Progress Indicator to IP<br><b>[IpProfile_ProgressIndicator2IP]</b>   | For a description, see the global parameter ProgressIndicator2IP.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                |
| Web: Coder Group<br><b>[IpProfile_CodersGroupID]</b>                       | For a description, see the global parameter CodersGroup.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Web: Remote RTP Base UDP Port<br><b>[IpProfile_RemoteBaseUDPPort]</b>      | For a description, see the global parameter RemoteBaseUDPPort.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |
| Web: First Tx DTMF Option<br><b>[IpProfile_FirstTxDtmfOption]</b>          | For a description, see the global parameter TxDTMFOption.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Web: Second Tx DTMF Option<br><b>[IpProfile_SecondTxDtmfOption]</b>        | For a description, see the global parameter TxDTMFOption.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Web: Declare RFC 2833 in SDP<br><b>[IpProfile_RxDTMFOption]</b>            | For a description, see the global parameter RxDTMFOption.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                        |
| Web: Enable Hold<br><b>[IpProfile_EnableHold]</b>                          | For a description, see the global parameter EnableHold.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| <b>SBC Parameters</b>                                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Web: Allowed Coders Group ID<br><b>[IpProfile_SBCAllowedCodersGroupID]</b> | <p>Associates a Coders Group ID for defining the coders that can be used for this IP entity.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ For a description of the Allowed Coders feature, see Restricting Coders.</li> <li>▪ To configure Allowed Coders Groups, see Configuring Allowed Coder Groups.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Web: Allowed Coders Mode<br><b>[IpProfile_SBCAllowedCodersMode]</b>        | <p>Determines the mode of the Allowed Coders feature for this IP Profile.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Restriction = In the incoming SDP offer, the device uses only coders that are also listed in the Allowed Coders Group; the rest are removed from the SDP offer (i.e., only coders common between SDP offered coders and Allowed Coders Group are used). If an Extension Coders Group is also selected (using the IP Profile's SBCExtensionCodersGroupID parameter), these coders are</li> </ul>                                                                                                                                                                                                                                                                                                                                                                |



| Parameter                                                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
|------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                              | <p>added to the SDP offer.</p> <ul style="list-style-type: none"> <li><b>[1] Preference</b> = The device re-arranges the priority (order) of the coders in the incoming SDP offer according to their order of appearance in the Allowed Coders Group list. This option also retains all the coders received in the SDP offer.</li> <li><b>[2] Restriction and Preference</b> = Performs both Restriction and Preference.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>If the AllowedCodersGroup parameter is set to None, this parameter is not applicable.</li> <li>To select the Allowed Coders Group ID, use the AllowedCodersGroup parameter.</li> <li>To select the Extension Coders Group ID, use the CodersGroups parameter.</li> <li>For more information on the Allowed Coders feature, see Restricting Coders.</li> </ul>                            |
| Web: Diversion Mode<br><b>[IpProfile_SBCDiversionMode]</b>                   | <p>Determines the device's handling of the SIP Diversion header. For more information on interworking of the History-Info and Diversion headers, see Interworking SIP Diversion and History-Info Headers.</p> <ul style="list-style-type: none"> <li><b>[0] Don't Care</b> = (Default) Diversion header is not handled.</li> <li><b>[1] Add</b> = History-Info header converted to a Diversion header.</li> <li><b>[2] Remove</b> = Removes the Diversion header and the conversion to the History-Info header depends on the settings of the SBCHistoryInfoMode parameter.</li> </ul>                                                                                                                                                                                                                                                                                                   |
| Web: History Info Mode<br><b>[IpProfile_SBCHistoryInfoMode]</b>              | <p>Determines the device's handling of the History-Info header. For more information on interworking of the History-Info and Diversion headers, see Interworking SIP Diversion and History-Info Headers.</p> <ul style="list-style-type: none"> <li><b>[0] Don't Care</b> = (Default) History-Info header is not handled.</li> <li><b>[1] Add</b> = Diversion header converted to a History-Info header.</li> <li><b>[2] Remove</b> = History-Info header removed from the SIP dialog and the conversion to the Diversion header depends on the settings of the SBCDiversionMode parameter.</li> </ul>                                                                                                                                                                                                                                                                                   |
| Web: Media Security Behavior<br><b>[IpProfile_SBCMediaSecurityBehaviour]</b> | <p>Determines the transcoding method between SRTP and RTP and enforce an SBC leg to use SRTP or RTP.</p> <ul style="list-style-type: none"> <li><b>[0] As is</b> = (Default) No special handling for RTP\SRTP is done.</li> <li><b>[1] SRTP</b> = SBC legs negotiate only SRTP media lines, and RTP media lines are removed from the incoming SDP offer\answer.</li> <li><b>[2] RTP</b> = SBC legs negotiate only RTP media lines, and SRTP media lines are removed from the incoming offer\answer.</li> <li><b>[3] Both</b> = Each offer\answer is extended (if not already) to two media lines - one RTP and the other SRTP.</li> </ul> <p>If two SBC legs (after offer\answer negotiation) use different security types (i.e., one RTP and the other SRTP), the device performs RTP-SRTP transcoding. To transcode between RTP and SRTP, the following prerequisites must be met:</p> |



| Parameter                                                                    | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                              | <ul style="list-style-type: none"> <li>At least one supported SDP "crypto" attribute and parameters</li> <li>EnableMediaSecurity must be set to 1</li> </ul> <p>If one of the above transcoding prerequisites is not met, then:</p> <ul style="list-style-type: none"> <li>any value other than "As is" is discarded.</li> <li>if the incoming offer is SRTP, force transcoding, coder transcoding, and DTMF extensions are not applied.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
| Web: P-Asserted-Identity<br><b>[IpProfile_SBCAssertIdentity]</b>             | For a description, see the global parameter SBCAssertIdentity.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
| Web: SBC Fax Answer Mode<br><b>[IpProfile_SBCFaxAnswerMode]</b>              | <p>Defines the coders included in the outgoing SDP answer (sent to the calling "fax").</p> <ul style="list-style-type: none"> <li><b>[0]</b> = Use matched coders between the incoming offer coders (from the calling "fax") and the coders of the selected Coders Group ID (configured using the SBCFaxCodersGroupID parameter).</li> <li><b>[1]</b> = (Default) Use only one coder. If the incoming answer (from the called "fax") includes a coder that matches a coder match between the incoming offer coders (from the calling "fax") and the coders of the selected Coders Group ID (SBCFaxCodersGroupID, then the device uses this coder. If no match exists, the device uses the first listed coder of the matched coders between the incoming offer coders (from the calling "fax") and the coders of the selected Coders Group ID.</li> </ul>                                                                                                                |
| Web: SBC Session Expires Mode<br><b>[IpProfile_SBCSessionExpiresMode]</b>    | <p>Determines the required session expires mode of the IP entity.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Transparent = (Default) The device does not interfere with the session expires negotiation.</li> <li><b>[1]</b> Observer = If the SIP Session-Expires header is present, the device does not interfere, but maintains an independent timer for each leg to monitor the session. If the session is not refreshed on time, the device disconnects the call.</li> <li><b>[2]</b> Not Supported = The device does not allow a session timer with this IP entity.</li> <li><b>[3]</b> Supported = The device enables the session timer with this IP entity. If the incoming SIP message does not include any session timers, the device adds the session timer information to the sent message. You can configure the value of the Session-Expires and Min-SE headers, using the SBCSessionExpires and SBCMinSE parameters, respectively.</li> </ul> |
| Web: SBC Remote Early Media RTP<br><b>[IpProfile_SBCRemoteEarlyMediaRTP]</b> | <p>Defines whether the destination UA sends RTP immediately after it sends 18x response.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Immediate = (Default) Remote client sends RTP immediately after it sends 18x response with early media. Device forwards 18x and RTP as is.</li> <li><b>[1]</b> Delayed = After sending 18x response, the remote client waits before sending RTP (e.g., Microsoft Lync environment). For the device's handling of this remote UA support, see Interworking SIP Early Media.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                    |
| Web: SBC Remote Can Play Ringback                                            | Defines whether the destination UA can play a local ringback tone.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                      |



| Parameter                                                                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                             |
|------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>[IpProfile_SBCRemoteCanPlayRingback]</b>                                              | <ul style="list-style-type: none"> <li><b>[0]</b> No = UA does not support local ringback tone. The device sends 18x with delayed SDP to the UA.</li> <li><b>[1]</b> Yes = (Default) UA supports local ringback tone. For the device's handling of this remote UA support, see Interworking SIP Early Media.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                 |
| Web: SBC Remote Supports RFC 3960<br><b>[IpProfile_SBCRemoteSupportsRFC3960]</b>         | <p>Defines whether the destination UA is capable of receiving 18x messages with delayed RTP.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Not Supported = (Default) UA does not support receipt of 18x messages with delayed RTP. For the device's handling of this remote UA support, see Interworking SIP Early Media.</li> <li><b>[1]</b> Supported = UA is capable of receiving 18x messages with delayed RTP.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                  |
| Web: SBC Multiple 18x Support<br><b>[IpProfile_SBCRemoteMultiple18xSupport]</b>          | <p>Determines whether multiple 18x responses (including 180 Ringing, 181 Call is Being Forwarded, 182 Call Queued, and 183 Session Progress) are forwarded to the caller.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Not Supported = Only the first 18x response is forwarded to the caller.</li> <li><b>[1]</b> Supported = (Default) Multiple 18x responses are forwarded to the caller.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                        |
| Web: SBC Early Media Response Type<br><b>[IpProfile_SBCRemoteEarlyMediaResponseType]</b> | <p>Determines the SIP provisional response type - 180 or 183 - for forwarding early media to the caller.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Transparent = (Default) All early media response types are supported; the device forwards all responses as is (unchanged).</li> <li><b>[1]</b> 180 = Early media is sent as 180 response only.</li> <li><b>[2]</b> 183 = Early media is sent as 183 response only.</li> </ul>                                                                                                                                                                                                                                                                                                                                                            |
| Web: SBC Remote Update Support<br><b>[IpProfile_SBCRemoteUpdateSupport]</b>              | <p>Determines whether endpoints support the UPDATE method.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Not Supported = UPDATE method is not supported.</li> <li><b>[1]</b> Supported Only After Connect = UPDATE method is supported only after the call is connected.</li> <li><b>[2]</b> Supported = (Default) UPDATE method is supported during call setup and after call establishment.</li> </ul>                                                                                                                                                                                                                                                                                                                                                                                        |
| Web: SBC Remote Re-Invite Support<br><b>[IpProfile_SBCRemoteReinviteSupport]</b>         | <p>Determines whether the destination UA of the re-INVITE request supports re-INVITE messages and if so, whether it supports re-INVITE with or without SDP.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Not Supported = re-INVITE is not supported and the device does not forward re-INVITE requests. The device sends a SIP response to the re-INVITE request, which can either be a success or a failure, depending on whether the device can bridge the media between the endpoints.</li> <li><b>[1]</b> Supported with SDP = re-INVITE is supported, but only with SDP. If the incoming re-INVITE arrives without SDP, the device creates an SDP and adds it to the outgoing re-INVITE.</li> <li><b>[2]</b> Supported = (Default) re-INVITE is supported with or without SDP.</li> </ul> |
| Web: SBC Remote Refer Behavior<br><b>[IpProfile_SBCRemoteReferBehavior]</b>              | <p>For a description, see the global parameter SBCReferBehavior.</p>                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                    |



| Parameter                                                                                | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
|------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Web: SBC Remote Early Media Support<br><b>[IpProfile_SBCRemoteEarlyMediaSupport]</b>     | Determines whether a remote side can accept early media or not. <ul style="list-style-type: none"> <li><b>[0]</b> Not Supported = Early media is not supported.</li> <li><b>[1]</b> Supported = (Default) Early media is supported.</li> </ul>                                                                                                                                                                                                                                                                                                                               |
| Web: SBC Remote 3xx Behavior<br><b>[IpProfile_SBCRemote3xxBehavior]</b>                  | For a description, see the global parameter SBC3xxBehavior.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                  |
| Web: SBC Remote Delayed Offer Support<br><b>[IpProfile_SBCRemoteDelayedOfferSupport]</b> | Determines whether the remote endpoint supports delayed offer (i.e., initial INVITEs without an SDP offer). <ul style="list-style-type: none"> <li><b>[0]</b> Not Supported = Initial INVITE requests without SDP are not supported.</li> <li><b>[1]</b> Supported = (Default) Initial INVITE requests without SDP are supported.</li> </ul> <p>Note: For this parameter to function properly, a valid Extension Coders Group ID needs to be configured for IP Profiles that do not support delayed offer.</p>                                                               |
| Web: SBC PRACK Mode<br><b>[IpProfile_SbcPrackMode]</b>                                   | Determines the PRACK mode required at the remote side: <ul style="list-style-type: none"> <li><b>[1]</b> Optional = PRACK is optional for these UAs. If required, the device performs the PRACK process on behalf of the destination UA.</li> <li><b>[2]</b> Mandatory = PRACK is required for these UAs. Calls from UAs that do not support PRACK are rejected. Calls destined to these UAs are also required to support PRACK.</li> <li><b>[3]</b> Transparent (default) = The device does not intervene with the PRACK process and forwards the request as is.</li> </ul> |
| Web: SBC Enforce MKI Size<br><b>[IpProfile_SBCEnforceMKISize]</b>                        | Enables MKI length negotiation for SRTP-to-SRTP flows between SIP networks (i.e., IP Groups). This feature includes the capability of modifying the MKI length on the inbound or outbound SBC call leg, using IP Profiles. <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) Device forwards the MKI size as is.</li> <li><b>[1]</b> Enable = Device changes the MKI length according to the settings of the IP Profile parameter, MKISize.</li> </ul>                                                                                                   |
| Web: SBC RFC2833 DTMF Payload Type Value<br><b>[IpProfile_SBC2833DTMFPayloadType]</b>    | Defines the RFC 2833 DTMF Payload Type for a specific SBC leg. This enables the interworking of the DTMF payload type for RFC 2833 between different SBC call legs. For example, if two entities require different DTMF payload types, the SDP offer received by the device from one entity is forwarded to the destination entity with its payload type replaced with the configured payload type, and vice versa.<br><br>The value range is 96 to 127. The default is 0 (i.e., the device forwards the received payload type as is).                                       |
| Web: SBC User Registration Time<br><b>[IpProfile_SBCUserRegistrationTime]</b>            | For a description, see the global parameter SBCUserRegistrationTime.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                         |
| Web: SBC Remote Hold Format<br><b>[IPProfile_SBCRemoteHoldFormat]</b>                    | Defines the format of the SDP in the re-INVITE for call hold that the device sends to the held party. <ul style="list-style-type: none"> <li><b>[0]</b> transparent = Device forwards SDP as is.</li> <li><b>[1]</b> send-only = Device sends SDP with 'a=sendonly'.</li> <li><b>[2]</b> send only 0.0.0.0 = Device sends SDP with 'a=sendonly'</li> </ul>                                                                                                                                                                                                                   |



| Parameter                                                                       | Description                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                     |
|---------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
|                                                                                 | <p>and 'c=0.0.0.0'.</p> <ul style="list-style-type: none"> <li>▪ <b>[3]</b> inactive = Device sends SDP with 'a=inactive'.</li> <li>▪ <b>[4]</b> inactive 0.0.0.0 = Device sends SDP with 'a=inactive' and 'c=0.0.0.0'.</li> <li>▪ <b>[5]</b> not supported = Used when remote side cannot identify a call-hold message. The device terminates the received call-hold message (re-INVITE / UPDATE) and sends a 200 OK to the initiator of the call hold. The device plays a held tone to the held party if the 'SBC Play Held Tone' parameter is set to Yes.</li> </ul>                                                                                                                                                                         |
| Web: SBC Play Held Tone<br><b>[IpProfile_SBCPlayHeldTone]</b>                   | <p>Enables the device to play a held tone to the held party. This is useful if the held party does not support playing a local held tone, or for IP entities initiating call hold that do not support the generation of held tones.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> No (default)</li> <li>▪ <b>[1]</b> Yes</li> </ul> <p><b>Note:</b> If this parameter is set to Yes, the device plays the tone only if the 'SBC Remote Hold Format' parameter is set to transparent, send-only, send only 0.0.0.0, or not supported.</p>                                                                                                                                                                                              |
| Web: SBC Reliable Held Tone Source<br><b>[IPProfile_ReliableHoldToneSource]</b> | <p>Enables the device to consider the received call-hold request (re-INVITE/UPDATE) with SDP containing 'a=sendonly', as genuine.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> No (default) = Even if the received SDP contains 'a=sendonly', the device plays a held tone to the held party. This is useful in cases where the initiator of the call hold does not support the generation of held tones.</li> <li>▪ <b>[1]</b> Yes = If the received SDP contains 'a=sendonly', the device does not play a held tone to the held party (and assumes that the initiator of the call hold plays the held tone).</li> </ul> <p><b>Note:</b> The device plays a held tone only if the 'SBC Play Held Tone' parameter is set to Yes.</p> |



# Part V

## Session Border Controller Application







## 20 SBC Overview

This section provides a detailed description of the device's SBC application.

**Notes:**

- For guidelines on how to deploy your E-SBC device based on network topology, refer to the *SBC Design Guide* document.
- For SBC functionality, the Software License Key installed on the device must include the SBC feature.

The SBC application supports the following main features:

- NAT traversal: The device supports NAT traversal, allowing, for example, communication with ITSPs with globally unique IP addresses, for LAN-to-WAN VoIP signaling (and bearer), using two independent legs. This also enables communication for "far-end" users located behind a NAT on the WAN. The device supports this by:
  - Continually registering far-end users in its dynamic database.
  - Maintaining remote NAT binding state by frequent registrations, thereby, off-loading far-end registrations from the LAN IP PBX.
  - Using Symmetric RTP (RFC 4961) to overcome bearer NAT traversal.
- VoIP firewall and security for signaling and media:
  - SIP signaling:
    - ◆ Deep and stateful inspection of all SIP signaling packets.
    - ◆ SIP dialog initiations may be rejected based on values of incoming SIP INVITE message and other Layer-3 characteristics.
    - ◆ Packets not belonging to an authorized SIP dialog are discarded.
  - RTP:
    - ◆ Opening pinholes (ports) in the device's firewall based on Offer-Answer SDP negotiations.
    - ◆ Deep packet inspection of all RTP packets.
    - ◆ Late rouge detection - if a SIP session was gracefully terminated and someone tries to "ride on it" with rouge traffic from the already terminated RTP and SIP context, the VoIP Firewall prevents this from occurring.
    - ◆ Disconnects call (after user-defined time) if RTP connection is broken.
    - ◆ Black/White lists for both Layer-3 firewall and SIP classification.
- Topology hiding: The device intrinsically supports topology hiding, limiting the amount of topology information displayed to external parties. For example, IP addresses of ITSPs' equipment (e.g. proxies, gateways, and application servers) can be hidden from outside parties. The device's topology hiding is provided by implementing back-to-back user agent (B2BUA) leg routing:
  - Strips all incoming SIP Via header fields and creates a new Via value for the outgoing message.
  - Each leg has its own Route/Record Route set.
  - Modifies SIP To, From, and Request-URI host names (must be configured using the Message Manipulations table).
  - Generates a new SIP Call-ID header value (different between legs).
  - Changes the SIP Contact header to the device's own address.
  - Layer-3 topology hiding by modifying source IP address in the SIP IP header.
- SIP normalization: The device supports SIP normalization, whereby the SBC



application can overcome interoperability problems between SIP user agents. This is achieved by the following:

- Manipulation of SIP URI user and host parts.
- Connection to ITSP SIP trunks on behalf of an IP-PBX - the device can register and utilize user and password to authenticate for the IP-PBX.
- Survivability:
  - Routing calls to alternative routes such as the PSTN.
  - Routing calls between user agents in the local network using a dynamic database (built according to registrations of SIP user agents).
- Routing:
  - IP-to-IP routing translations of SIP, UDP, TCP, TLS (when extensive transcoding is not required).
  - Load balancing and redundancy of SIP servers.
  - Routing according to Request-URI\Specific IP address\Proxy\FQDN.
  - Alternative routing.
  - Routing between different Layer-3 networks (e.g., LAN and WAN).
- Load balancing\redundancy of SIP servers.
- ITSP accounts.
- SIP URI user and host name manipulations.
- Coder transcoding.

## 20.1 SIP Network Definitions

The device's SBC application can implement multiple SIP signaling and RTP (media) interfaces.

## 20.2 SIP Dialog Initiation Process

The device's SIP dialog initiation process concerns all incoming SIP dialog initiation requests. This includes SIP methods such as INVITE, SUBSCRIBE, OPTIONS, REFER, INFO, UNSOLICITED NOTIFY, MESSAGE, and REGISTER.

The SIP dialog initiation process consists of the following stages:

1. **Determining source and destination URL:** The SIP protocol has more than one URL in a dialog-establishing request that may represent the source and destination URLs. When handling an incoming request, the device uses specific SIP headers for obtaining the source and destination URLs. Once these URLs are determined, their user and host parts are used as input for the classification process, message manipulation, and call routing.
  - **All SIP requests (e.g., INVITE) except REGISTER dialogs:**
    - ◆ Source URL: The source URL is obtained from the SIP header according to the following logic:
      - ✓ The source URL is obtained from the From header.
      - ✓ If the From header contains the value 'Anonymous', the source URL is obtained from the P-Preferred-Identity header.
      - ✓ If the P-Preferred-Identity header does not exist, the source URL is obtained from the P-Asserted-Identity header.
    - ◆ Destination URL: The destination URL is obtained from the Request-URI.



- **REGISTER dialogs:**
  - ◆ Source URL: The source URL is obtained from the To header.
  - ◆ Destination URL: The destination URL is obtained from the Request-URI.



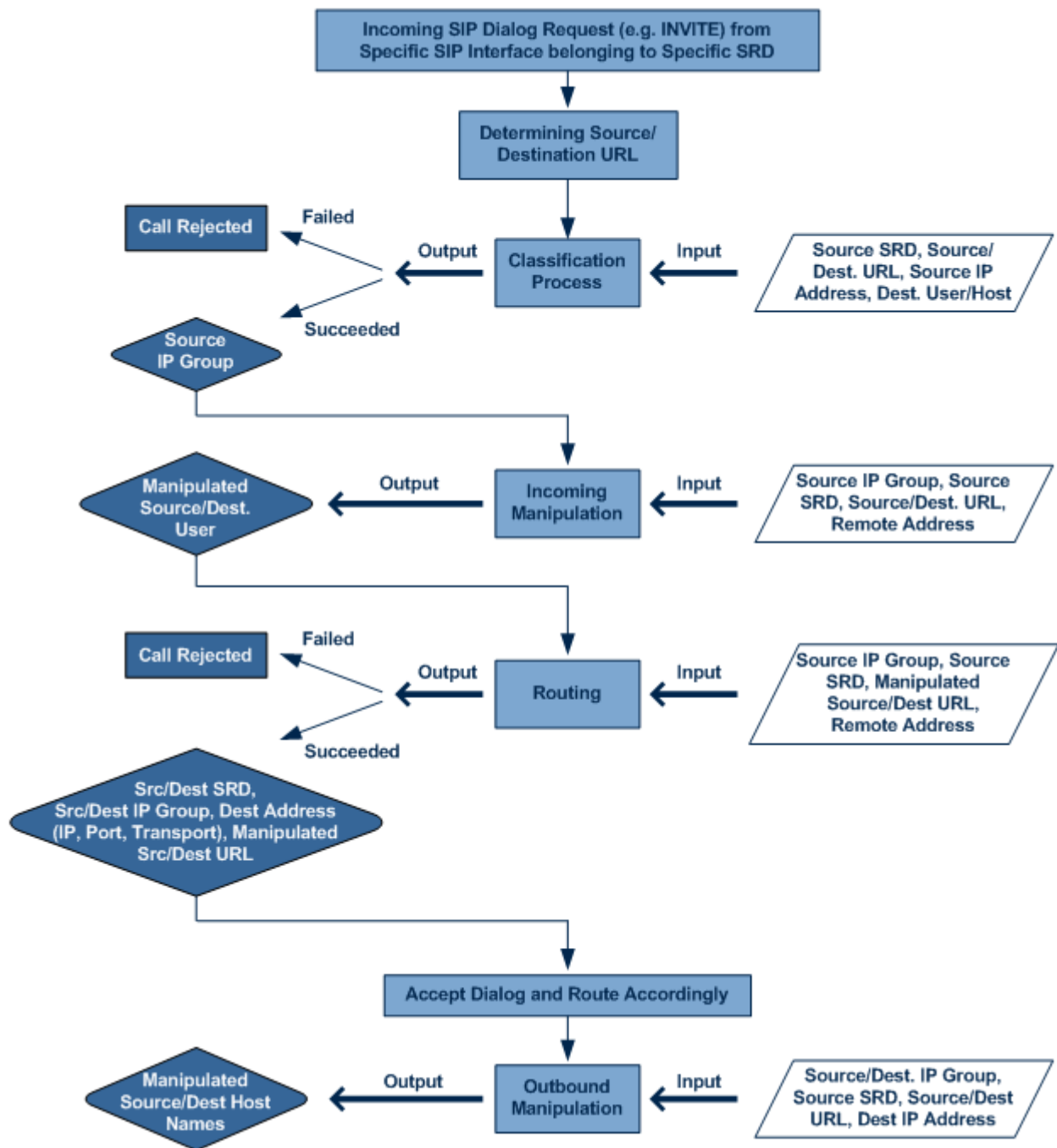
**Note:** You can determine the SIP header from where the device obtains the source URL in the incoming SIP request. This is done in the IP Group table using the 'Source URI Input' parameter.

2. **Classifying incoming SIP dialog-initiating requests to a source IP Group:** The classification identifies the incoming SIP dialog request as belonging to a specific IP Group (from where the SIP dialog request originated). For more information, see "Configuring Classification Rules" on page 230.
3. **SBC IP-to-IP routing:** The device routes the call to a destination that can be configured to one of the following:
  - IP Group - the destination is the address configured for the Proxy Set associated with the IP Group (allows redundancy/load balancing).
  - Specified destination address (can be based on IP address, host name, port, transport type, and/or SRD). Routing to a host name can be resolved using NAPTR/SRV/A-Record.
  - Request-URI of incoming SIP dialog initiating requests.
  - ENUM query.
  - Hunt Group - used for call survivability.
  - IP address (in dotted-decimal notation or FQDN - NAPTR/SRV/A-Record resolutions) according to a specified Dial Plan index listed in the loaded Dial Plan file.
  - LDAP server or LDAP query result.For more information, see "Configuring SBC IP-to-IP Routing" on page 236.
4. **Manipulating SIP URI user part (source and destination) of inbound and/or outbound SIP dialog requests:** You can configure rules for manipulating the SIP URI user part (source and destination) on the inbound and/or outbound leg. For more information, see "SBC Manipulations" on page 244.
5. **SIP message manipulations:** You can configure SIP message manipulation rules that can add, remove, and/or modify SIP headers and parameters. For more information, see "Configuring SIP Message Manipulation" on page 182.



The flowchart below illustrates the SBC process:

**Figure 20-1: Routing Process**



## 20.3 User Registration and Internal Database

To allow registrations to traverse the SBC, the device must be configured with at least one User-type IP Group. These IP Groups represent a group of user agents that share the following characteristics:

- Perform registrations and share the same serving proxy/registrar
- Possess identical SIP and media behavior
- Reside on the same Layer-3 network and are associated with the same SRD



Typically, the device is configured as the user agent's outbound proxy and the device is configured (using the IP-to-IP Routing table) to route requests received from this IP Group to the serving proxy and vice versa. Survivability can be achieved using the alternative routing feature.

### 20.3.1 Initial Registration Request Processing

Registration requests have different processing policies than other SIP methods:

1. Determining source and destination URL's:
  - The source URL is obtained from the To header
  - The destination URL is obtained from the Request URI
2. Classification: The REGISTER classification process is the same as the general classification process (described in previous sections). The source IP Group must be of type User. If classification fails or the source IP Group is not of type User, the registration is rejected.
3. Routing: The REGISTER routing is performed using the IP-to-IP Routing table:
  - The destination type can be an IP Group, specific IP address, Request-URI, or ENUM query (can also use DNS queries).
  - If the destination is a User-type IP Group, then the registration is not be forwarded. Instead, the device accepts (replies with 200 OK response) or rejects (Reply with 4xx) the request according to the user group policy.
4. Internal registration database: If the source IP Group is of type User and registration succeeds (replied with 200 OK by the IP-PBX), then the device adds a record to its database that identified the specific contact of this specific user (AOR). This record is used later to route requests to this specific user (either in normal or in survivability modes).
5. Alternative Routing: Alternative routing can be configured in the IP-to-IP Routing table for REGISTER requests.
6. Inbound Manipulation: The SBC record in the device's database includes the Contact header. Every REGISTER request is added to the database before manipulation, allowing correct user identification in the SBC Classification process for the next received request.
7. Session Admission Control: Applies various limitations on incoming and outgoing REGISTER requests. For example, limiting REGISTER requests from a certain IP Group/SRD. Note that this limitation is only for concurrent register dialogs and not concurrent registrations in the internal database.
8. The device can retain the original value of the SIP Expires header received from the user or proxy, in the outgoing REGISTER message. This feature also applies when the device is in "survivability" state (i.e., REGISTER requests cannot be forwarded to the proxy and is terminated by the device). This is configured by the `SBCUserRegistrationTime`, `SBCProxyRegistrationTime`, and `SBCSurvivabilityRegistrationTime` parameters.
9. By default, the Contact of the outgoing REGISTER is populated with a unique Contact generated by the device and associated with this specific registration. Alternatively, the original user can be retained in the Contact and used in the outgoing REGISTER request (using the `SBCKeepContactUserinRegister` parameter).

### 20.3.2 Internal Database

The device manages a dynamic database that is updated according to registration requests that traverse the SBC. Each database entry represents a binding between an AOR and one or more contact. Database bindings are added upon successful registration



responses. For specific registrations, the AOR is obtained from the SIP To header and the contact is taken from the SIP Contact header.

Database bindings are removed in the following cases:

- Successful de-registration responses (REGISTER with Expires header that equals zero)
- Registration failure responses
- Timeout of the Expires header value (in scenarios where the user agent did not send a refresh registration request)

The database has the following limitations:

- Maximum of five contacts per AOR
- The same contact cannot belong to more than one AOR
- Contacts with identical URIs and different ports and transport types are not supported (same key is created)
- Multiple contacts in a single REGISTER is not supported
- One database is shared between all User-type IP Groups

### 20.3.3 Routing using Internal Database

Typically, routing using the database is applicable to all method types other than registrations. To route to a registered user (using the internal dynamic database), the following steps must be taken:

1. An IP-to-IP Routing rule with the desired input parameters (matching characteristics) and the destination type as IP Group (operation rule).
2. The destination IP Group must be of type User.
3. To find a match for these specific rules, the device attempts to locate a match between the incoming Request-URI and (according to the description order):
  - a. Unique contact - the Contact generated by the SBC and sent in the initial registration request to the serving proxy
  - b. Registered AOR - the AOR of the incoming REGISTER request
  - c. Registered contact - the Contact of the incoming REGISTER request

If registrations are destined to the database (using the above rules), the device does not attempt to find a database match, but instead replies with 200 OK (used for Survivability). Once a match is found, the request is routed either to the contact received in the initial registration or (if the device identifies that the user agent is behind a NAT) to the source IP address of the initial registration.

### 20.3.4 Registration Refreshes

Registration refreshes are incoming REGISTER requests that are associated with a specific registered user. The association is performed by searching the internal registration database. These refreshes are routed to the serving proxy only if the serving proxy Expires time is about to expire; otherwise, the device responds with a 200 OK without routing the REGISTER. Each such refreshes also refresh the internal timer time set on the device for this specific registration.

### 20.3.5 Notification of Expired User Registration to SIP Proxy / Registrar

The device automatically notifies SIP Proxy / Registrar servers of users registered in the device's database whose registration timeout has expired. When a user's registration timer expires, the device removes the user record from its Registration database and sends an unregister notification (REGISTER message with the Expires header set to 0) to the Proxy/Registrar.



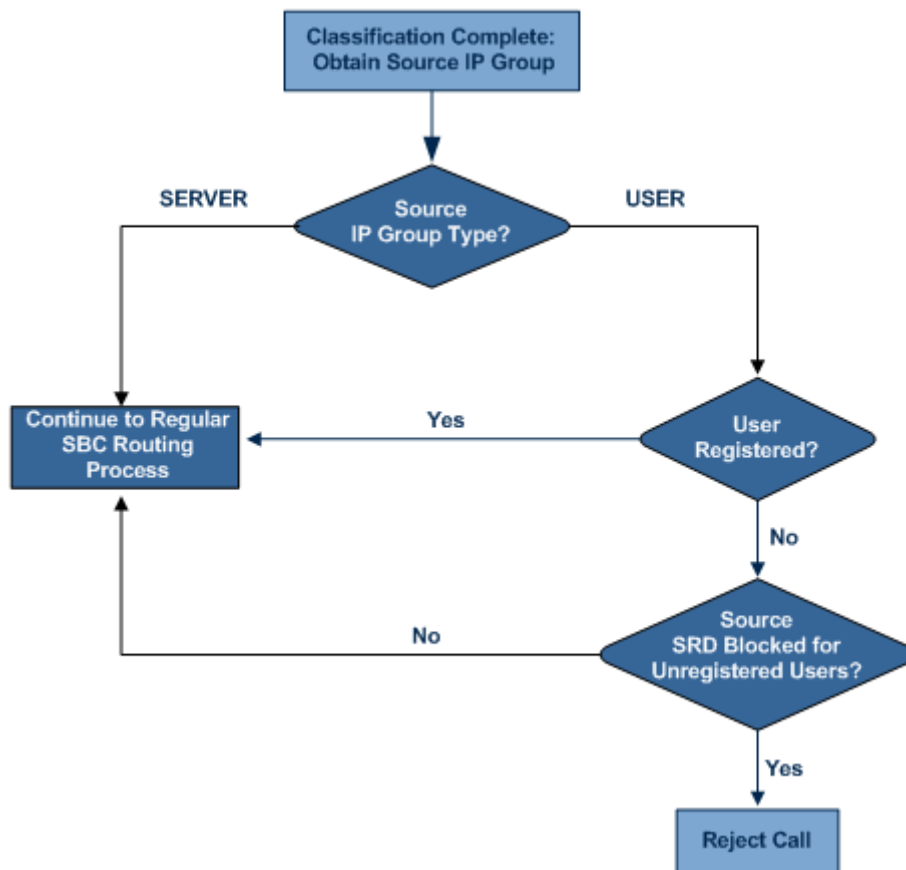
This feature is enabled only if a REGISTER message is sent to an IP Group destination type, configured in the IP-to-IP Routing table.

### 20.3.6 Registration Restriction Control

The device provides flexibility in controlling user registration:

- **Limiting Number of Registrations per Source SRD and/or IP Group:** You can limit the number of users that can register with the device. This limitation can be applied per source IP Group and/or SRD. By default, no limitation exists for registered users. This is configured using the parameters SRD or IPGroup.
- **Blocking Incoming Calls from Unregistered Users:** You can block incoming calls (INVITE requests) from unregistered users (pertaining to User-type IP Groups). By default, calls from unregistered users are not blocked. This is configured using the parameter SRD. The flowchart below depicts the process for blocking unregistered users. When the call is rejected, the device sends a SIP 500 "Server Internal Error" response to the remote end.

Figure 20-2: Blocking Incoming Calls from Unregistered Users



## 20.4 SBC Media Handling

Media behavior includes anything related to the establishment, management and termination of media sessions within the SIP protocol. Media sessions are created using the SIP "offer"/"answer" mechanism. If successful, the result is a bi-directional media (RTP) flow (e.g. audio, fax, modem, DTMF). Each offer/answer may create more than one media session of different types (e.g. audio and fax). In a SIP dialog, multiple offer/answer transactions may occur, each may change the media sessions characteristics (e.g. IP



address, port, coders, media types, and RTP mode). The media capabilities exchanged in an offer/answer transaction include the following:

- Media types (Audio, Secure Audio, Video, Fax, Text...)
- IP addresses and ports of the media flow
- Media flow mode (send receive, receive only, send only, inactive)
- Media coders (coders and their characteristics used in each media flow)
- Other (standard or proprietary) media and session characteristics

Even though the device usually does not change the negotiated media capabilities (mainly performed by the remote user agents), it does examine the media exchange to control negotiated media types (if necessary) and to know how to open the RTP media channels (IP addresses, coder type, payload type etc.). The device forwards multiple video streams and text, as is.

The device interworks (normalization) the media (RTP-to-RTP, SRTP-to-RTP, and SRTP-to-SRTP) between its SBC legs. It "re-builds" specific fields in the RTP header when forwarding media packets. The main fields include the sequence number, SSRC, and timestamp.

The device is aware and sometimes active in the offer/answer process due to the following:

- NAT traversal: the device changes the SDP address to be its own address, thereby, resolving NAT problems.
- Firewall and security:
  - RTP pin holes - only RTP packets related to a successful offer/answer negotiation traverse the device: When the device initializes, there are no RTP pin holes opened, this means that each RTP/RTCP packets destined to the device are discarded. Once an offer/answer transaction ends successfully, an RTP pin hole is opened and RTP/RTCP flows between the two remote user agents. Once a pin hole is opened, the payload type and RTP header version is validated for each packet. RTP pin holes close if one of the associated SIP dialogs is closed (may also be due to broken connection).
  - Late rogue detection - once a dialog is disconnected, the related pin holes also disconnect.
  - Deep Packet inspection of the RTP that flows through the opened pin holes.
- Adding of media functionality to SIP user agents:
  - Transcoding (for a description on the transcoding modes, see Transcoding Modes)
  - Broken connection

According to the above functionalities, the call can be configured to operate in one of the following modes:

- **Media Anchoring without Transcoding (Transparent):** RTP traverses the device with minimal RTP packet changes (no DSP resources needed). This is typically used to solve NAT, firewall, and security issues. In this mode, all the "audio" coders in the received offer are included in the SBC outgoing offer. The Coder Table configuration has no effect on the coders in the outgoing offer. For more information, see "Media Anchoring without Transcoding (Transparent)" on page 207.
- **Media Anchoring with Transcoding:** RTP traverses the device and each leg uses a different coder or coder parameters (DSP resources are required). For more information, see Media Anchoring with Transcoding.
- **No Media Anchoring:** The RTP packet flow does not traverse the device. Instead, the two SIP UA's establish a direct RTP/SRTP flow between one another (see "No Media Anchoring" on page 207).



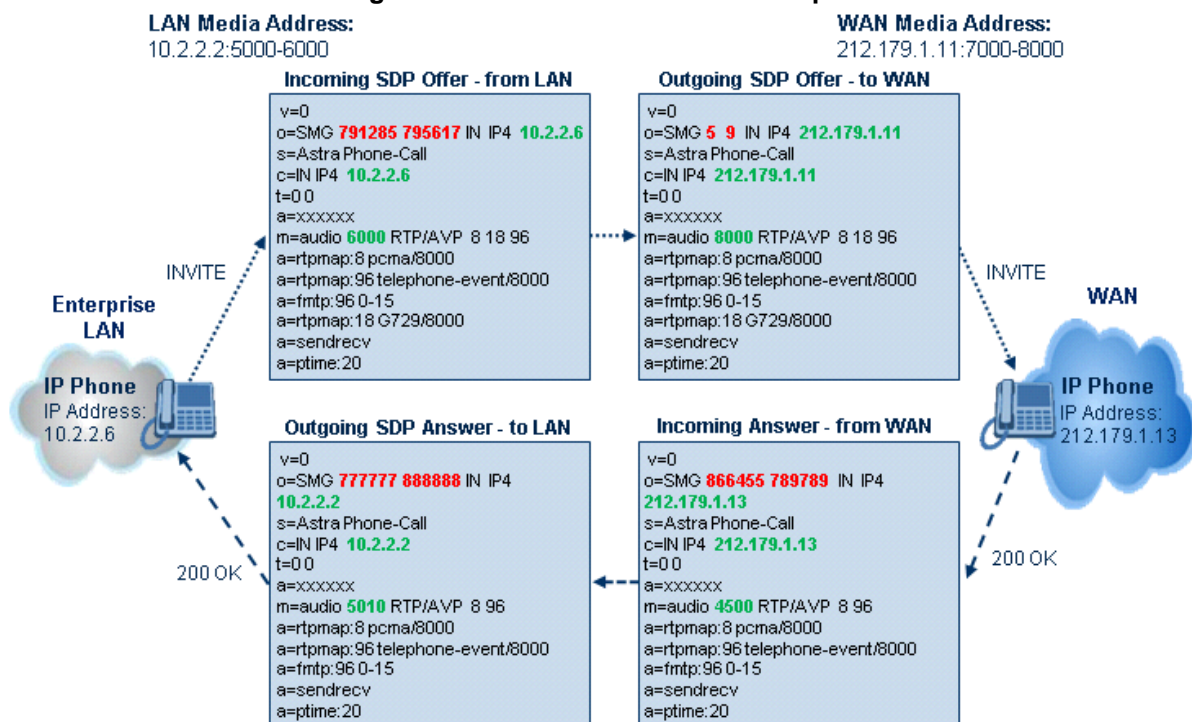
### 20.4.1 Media Anchoring without Transcoding (Transparent)

To direct the RTP to flow through the device (for NAT traversal, firewall and security), all IP address fields in the SDP are modified:

- Origin: IP address, session and version id
- Session connection attribute ('c=' field)
- Media connection attribute ('c=' field)
- Media port number
- RTCP media attribute IP address and port

Each SBC leg allocates and uses the device's local ports (e.g., for RTP/RTCP/fax). The local ports are allocated from a Media Realm associated with each leg. The legs are associated with a Media Realm as follows: If the leg's IP Group is configured with a Media Realm, then this is the associated Media Realm; otherwise, the leg's SRD Media Realm is the associated one. The figure below illustrates an example of SDP handling for a call between a LAN IP Phone 10.2.2.6 and a remote IP Phone 212.179.1.13 on the WAN.

Figure 20-3: SDP Offer/Answer Example



### 20.4.2 No Media Anchoring

The No Media Anchoring or Anti-Tromboning feature enables the use of SBC signaling capabilities without handling the RTP/SRTP (media) flow between remote SIP user agents (UA). The RTP packet flow does not traverse the device and instead, the two SIP UAs establish a direct RTP/SRTP flow (i.e., direct call) between one another. Signaling continues to traverse the device with minimal intermediation and involvement to enable certain SBC abilities such as routing.

By default, media packets traverse the device. This is done in order to:

- Solve NAT problems
- Enforce media security policy
- Perform media transcoding between the two legs



#### Media monitoring

However, since media packets traverse the SBC, media quality may degrade, for example, due to packet delay.

In some setups, specific calls do not require media anchoring, for example, when there is no need for NAT, security, or transcoding. This is typical for calls between users in the LAN:

- Internal LAN calls: When the SBC routes a call between two UAs within the same LAN, the SBC can forward the SDP directly between caller and callee, and direct the RTP to flow between the UAs without traversing the SBC.
- Internal LAN calls via WAN: In this setup, the SBC dynamically identifies that the call is between UAs located in the same network (i.e., LAN) and thereby, directs the RTP to flow between these UAs without traversing the SBC

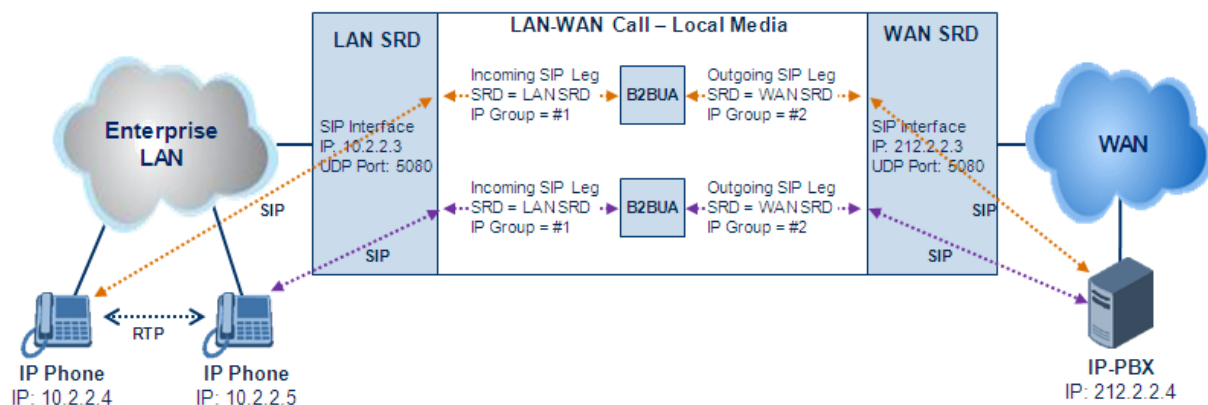
In contrast to the regular SBC implementation, the No Media Anchoring feature:

- Does not perform any manipulation on SDP data (offer/answer transaction) such as ports, IP address, coders
- Opening voice channels and allocation of IP media ports are not required

The No Media Anchoring feature is typically implemented in the following scenarios:

- SBC device is located within the LAN.
- Calls between two SIP UA's in the same LAN and signals are sent to a SIP proxy server (or hosted IP PBX) located in the WAN.

**Figure 20-4: SBC SIP Signaling without RTP Media Flow**



The benefits of implementing the No Media Anchoring include the following:

- Saves network bandwidth
- Reduces CPU usage (no RTP/SRTP handling)
- Avoids interference in SDP negotiation and header manipulation on RTP/SRTP

The No Media Anchoring process is as follows:

1. Identifies a No Media Anchoring call - according to configuration and the call's properties (such as source, destination, IP Group, and SRD).
2. Handles the identified No Media Anchoring call.

The No Media Anchoring feature is enabled using the SBCDirectMedia parameter. You can also enable No Media Anchoring per SRD (using the IntraSRDMediaAnchoring parameter), whereby calls between two UA's that pertain to the same SRD (source and destination) are handled as No Media Anchoring (direct media) calls.



**Notes:**

- No Media Anchoring can be used when the SBC does not do NAT traversal (for media) where all the users are in the same domain.
- No Media Anchoring calls cannot operate simultaneously with the following SBC features:
  - Force transcoding
  - Extension Coders
  - Extension of RFC 2833/Out-of-band DTMF/In-band DTMF
  - Extension of SRTP/RTPAll restriction features (Allowed Coders, restrict SRTP/SRT, restrict RFC 2833) can operate simultaneously. Once No Media Anchoring is enabled, the features listed above are disabled.
- The Coder Restriction feature operates simultaneously with No Media Anchoring calls. Restricted coders are removed from the SDP offer message.
- When two UA's pertain to the same SRD, the parameter IntraSRDMediaAnchoring is set to 1, and one of the UA's is defined as a foreign user (example, "follow me service") located in the WAN, while the other UA is located in the LAN: calls between these two UA's can't be established until IntraSRDMediaAnchoring is set to 0, as the device doesn't interfere in the SIP signaling. In other words, parameters such as IP addresses are not manipulated for calls between LAN and WAN (although required).
- When the parameter SBCDirectMedia is disabled, No Media Anchoring calls between two UA's belonging to separate SRD's cannot be configured. No Media Anchoring calls between two UA's belonging to the same SRD is configurable only (in this case).

### 20.4.3 Restricting Coders

The SBC Allowed Coders (coders restriction) feature determines the coders that can be used for a specific SBC leg. This provides greater control over bandwidth by enforcing the use of specific coders (*allowed coders groups*) while preventing the use of other coders. This is done by defining a group of allowed coders for the SBC leg, as described below:

1. Configure a Coders Group for allowed coders, using the AllowedCodersGroup parameter.
2. Select this Coders Group using the SBCAllowedCodersGroupID parameter of the IP Profile table.
3. Enable this feature by setting the SBCAllowedCodersMode parameter of the IP Profile table to **Restriction**.

Coders that are not listed (including unknown coders) in the Allowed Coders Group are removed from the SDP offer. Therefore, only coders common between the SDP offer and Allowed Coders Group are used. If the SDP offer does not list any of the Allowed Coders, the call is rejected.

**Notes:**

- For a list of supported coders, see Configuring Coders.
- Allowed Coder Groups are applicable only to audio media.



The Allowed Coders process is as follows:

- a. The device receives an incoming SIP message with SDP (offer) and checks the offered coders.
- b. The source (first) leg may have Allowed Coders (i.e. list of coders that can be used - enforced).
- c. The device checks for common coders between the SDP offered coders and the Allowed Coders Group list.

For example, assume the following:

- The SDP coder offer includes the following coders: G.729, G.711, and G.723.
- The source (first) leg includes the following Allowed Coders: G.711 and G.729.

The device selects the common coders, i.e., G.711 and G.729 (with changed preferred coder priority - highest for G.711). In other words, it removes the coders that are not in the Allowed Coders list and the order of priority is first according to the Allowed Coders list.

## 20.4.4 Prioritizing Coder List in SDP Offer

In addition to restricting the use of coders with Allowed coders, the device can prioritize the coders listed in the SDP offer. This feature is referred to as *Coder Preference*. This is done on both SBC legs:

- **Incoming SDP offer:** The device arranges the coder list according to the order in the Allowed Coders Group table. The coders listed higher up in the table take preference over ones listed lower down in the table. This feature is enabled by setting the 'Allowed Coders Mode' parameter in the IP Profile table to **Preference** or **Restriction and Preference**. If set to **Preference**, in addition to the Allowed coders that are listed first in the SDP offer, the original coders received in the SDP are retained and listed after the Allowed coders. Thus, this mode does not necessarily restrict coder use to Allowed coders, but uses (prefers) the Allowed coders whenever possible.
- **Outgoing SDP offer:** The coders are arranged in the SDP offer according to the above if only Allowed coders are used.

## 20.4.5 SRTP-RTP and SRTP-SRTP Transcoding

The device supports transcoding between SRTP and RTP. The device can also enforce specific SBC legs to use SRTP and/or RTP. The device's handling of SRTP/RTP is configured using the IP Profile parameter, `SBCMediaSecurityBehaviour`, which provides the following options:

- SBC passes the media as is, regardless of whether it's RTP or SRTP (default).
- SBC legs negotiate only SRTP media lines (m=); RTP media lines are removed from the incoming SDP offer\answer.
- SBC legs negotiate only RTP media lines; SRTP media lines are removed from the incoming offer\answer.
- Each SDP offer\answer is extended (if not already) to two media lines for RTP and SRTP.

If after SDP offer\answer negotiation, one SBC leg uses RTP while the other uses SRTP, then the device performs RTP-SRTP transcoding. To translate between RTP and SRTP, the following prerequisites must be met:

- At least one supported SDP "crypto" attribute.
- The `EnableMediaSecurity` parameter must be set to 1.

Channel resources are not required for transcoding between RTP and SRTP.

Transcoding where both legs are configured for SRTP is typically required to trans-encrypt and trans-decrypt. This is relevant when the MKI and Symmetric MKI parameters are enabled. In other words, both sides need to both encrypt and decrypt the outgoing and



incoming SRTP packets, respectively. Channel resources are not required for transcoding between SRTP and SRTP.

### 20.4.6 Multiple RTP Media Streams per Call Session

The device's SBC application supports multiple RTP media streams per SBC call session. Up to five different media types can be included in a session:

- Audio (m=audio)
- Video (m=video)
- Text (m=text)
- Fax (m=image)

Therefore, the device can provide transcoding of various attributes in the SDP offer/answer (e.g., codec, port, and packetization time) per media type. If the device is unable to perform transcoding (for example, does not support the codec), it relays the SBC dialog transparently.

## 20.5 Limiting SBC Call Duration

You can define a maximum allowed duration (in minutes) for SBC calls. If an established call reaches this user-defined limit, the device terminates the call. This feature ensures calls are properly terminated, allowing available resources for new calls. This feature is configured using the MaxCallDuration parameter.

## 20.6 SIP Authentication Server for SBC Users

The device can function as an authentication server for SIP SBC message requests, based on HTTP authentication DIGEST with MD5. Alternatively, such requests can be authenticated by an external, third-party server.

When functioning as an authentication server (set by the IP Group table parameter, AuthenticationMode), the device authenticates users belonging to a User-type IP Group. When the device receives an INVITE or REGISTER request from a client (e.g., SIP phone) for SIP message authorization, the device processes the authorization as follows:

1. The device verifies the type of incoming SIP method (e.g., INVITE) that must be challenged for authorization. This is configured using the IP Group table parameter, MethodList.
2. If the message is received without an Authorization header, the device "challenges" the client by sending a 401 or 407 SIP response. The client then resends the request with an Authorization header (containing the user name and password).
3. The device validates the SIP message according to the settings of the parameters, AuthNonceDuration, AuthChallengeMethod and AuthQOP.
  - If validation fails, the message is rejected and the device sends a 403 "Forbidden" response.
  - If validation succeeds, the device verifies identification of the SBC user. This is done by checking that the user name and password received from the user is the same username and password that appears in the device's database. The SBC users in the database are obtained from the User Information file. If the SIP SBC user is not successfully authenticated after three attempts, the device sends a 403 "Forbidden" response.
4. If the user is successfully identified, the SIP message request is processed.



## 20.7 Interworking SIP Signaling

The device supports interworking of SIP signaling messages to ensure interoperability between communicating SIP UAs or entities. This is critical in network environments where the UAs on opposing SBC legs have different SIP signaling support. For example, some UAs may support different versions of a SIP method while others may not even support a specific SIP method. The configuration method for assigning specific SIP message handling modes to UAs, includes configuring an IP Profile with the required interworking mode, and then assigning the IP Profile to the relevant IP Group.

This section describes some of the device's support for handling SIP methods to ensure interoperability.

### 20.7.1 Interworking SIP 3xx Redirect Responses

The device supports interworking of SIP 3xx redirect responses. By default, the device's handling of SIP 3xx responses is to send the Contact header unchanged. However, some SIP UAs may support different versions of the SIP 3xx standard while others may not even support SIP 3xx.

The handling of SIP 3xx can be configured for all calls, using the global parameter SBC3xxBehavior. For configuring different SIP 3xx handling options for different UAs (i.e., per IP Group), use the IP Profile table parameter, 'SBC Remote 3xx Behavior'.

#### 20.7.1.1 Resultant INVITE Traversing Device

The device can handle SIP 3xx responses so that the new INVITE message sent as a result of the 3xx traverses the device. The reasons for enforcing resultant INVITEs to traverse the device may vary:

- The user that receives the 3xx is unable to route to the 3xx contact (i.e., the user is on the LAN and the new contact is on the WAN). In such a scenario, the device enables the user to reach the WAN contact and overcome NAT problems.
- Enforce certain SBC policies (e.g., call admission control, header manipulation, and transcoding) on the resultant INVITE.

The device enforces this by modifying each Contact in the 3xx response as follows:

- Changes the host part to the device's IP address – this change causes the remote user agent to send the INVITE to the device.
- Adds a special prefix ("T~&R\_") to the Contact user part – to identify the new INVITE as a 3xx resultant INVITE.

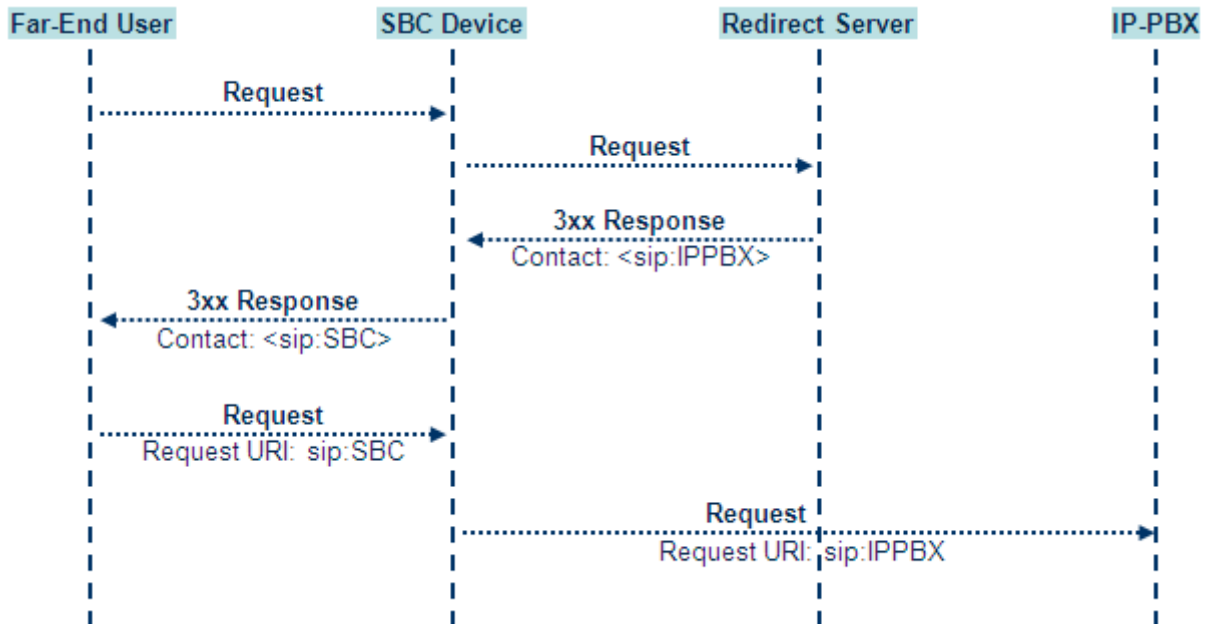
The SBC handling for the 3xx resultant INVITE is as follows:

1. The incoming INVITE is identified as a 3xx resultant INVITE according to the special prefix.
2. The device automatically replaces the SBC host part (in the Request-URI) with the host from the 3xx Contact.
3. The prefix ("T~&R\_") remains in the user part for the classification, manipulation, and routing mechanisms.
4. The classification, manipulation, and routing processes are done exactly like any other INVITE handling. The special prefix can be used for specific routing rules for 3xx resultant INVITEs.



- The prefix is removed before the resultant INVITE is sent to the destination.

**Figure 20-5: SIP 3xx Response Handling**



The process of this feature is described using an example:

- The device receives the Redirect server's SIP 3xx response (e.g., Contact: <sip:User@IPPBX:5060;transport=tcp;param=a;q=0.5>).
- The device replaces the Contact header value with the special prefix and database key value as user part, and with the device's URL as host part (e.g., Contact: <sip:Prefix\_Key\_User@SBC:5070;transport=udp;q=0.5>).
- The device sends this manipulated SIP 3xx response to the Far-End User (FEU).
- The FEU sends a new request with the Request-URI set to the value of the received 3xx response's Contact header (e.g., RequestURI: sip:Prefix\_Key\_User@SBC:5070;transport=udp).
- Upon receipt of the new request from the FEU, the device replaces the Request-URI with the new destination address (e.g., RequestURI: sip:Prefix\_User@IPPBX:5070;transport=tcp;param=a).
- The device removes the user prefix from the Request-URI, and then sends this Request-URI to the new destination (e.g., RequestURI: sip:User@IPPBX:5070;transport=tcp;param=a).

### 20.7.1.2 Local Handling of SIP 3xx

The device can handle SIP 3xx responses on behalf of the dialog-initiating UA and retry the request (e.g., INVITE) using one or more alternative URIs included in the 3xx response. The new request includes SIP headers from the initial request such as Diversion, History-Info, P-Asserted-Id, and Priority. The source and destination URIs can be manipulated using the regular manipulation mechanism.

The device sends the new request to the alternative destination according to the IP-to-IP Routing table rules. (where the 'Call Trigger' field is set to **3xx**). It is also possible to specify the IP Group that sent the 3xx request as matching criteria for the re-routing rule in this table ('ReRoute IP Group ID' field).



## 20.7.2 Interworking SIP Diversion and History-Info Headers

This device can be configured to interwork between the SIP Diversion and History-Info headers. This is important, for example, to networks that support the Diversion header but not the History-Info header, or vice versa. Therefore, mapping between these headers is crucial for preserving the information in the SIP dialog regarding how and why (e.g., call redirection) the call arrived at a certain SIP UA.

This feature is configured in the IP Profile table (IPProfile parameter) using the following new parameters:

- SBCDiversionMode - defines the device's handling of the Diversion header
- SBCHistoryInfoMode - defines the device's handling of the History-Info header

The handling of the SIP Diversion and History-Info headers is described in the table below:

**Table 20-1: Handling of SIP Diversion and History-Info Headers**

| Parameter Value                                                  | SIP Header Present in Received SIP Message                 |                                                               |                                                           |
|------------------------------------------------------------------|------------------------------------------------------------|---------------------------------------------------------------|-----------------------------------------------------------|
|                                                                  | Diversion                                                  | History-Info                                                  | Diversion and History-Info                                |
| <b>HistoryInfoMode = Add</b><br><b>DiversionMode = Remove</b>    | Diversion converted to History-Info.<br>Diversion removed. | Not present                                                   | Diversion removed.                                        |
| <b>HistoryInfoMode = Remove</b><br><b>DiversionMode = Add</b>    | Not present.                                               | History-Info converted to Diversion.<br>History-Info removed. | History-Info added to Diversion.<br>History-Info removed. |
| <b>HistoryInfoMode = Disable</b><br><b>DiversionMode = Add</b>   | Diversion converted to History-Info.                       | Not present.                                                  | Diversion added to History-Info.                          |
| <b>HistoryInfoMode = Disable</b><br><b>DiversionMode = Add</b>   | Not present.                                               | History-Info converted to Diversion.                          | History-Info added to Diversion.                          |
| <b>HistoryInfoMode = Add</b><br><b>DiversionMode = Add</b>       | Diversion converted to History-Info.                       | History-Info converted to Diversion.                          | Headers are synced and sent.                              |
| <b>HistoryInfoMode = Remove</b><br><b>DiversionMode = Remove</b> | Diversion removed.                                         | History-Info removed.                                         | Both removed.                                             |

## 20.7.3 Interworking SIP REFER Messages

The device supports interworking of SIP REFER messages. SIP UAs may support different versions of the REFER standard while others may not even support REFER.

This feature supports the following:

- Attended, unattended, and semi-attended call transfers
- Sending INVITE, REFER-notifications, BYE, PRACK and Session Timer on behalf of peer PBXs
- Advanced routing rules for the new, initiated INVITE
- Forwarding early media after REFER while attempting to avoid transcoding (by



sending session update)

- Interoperate with environments where different SIP UAs lack basic SIP functionality such as re-INVITE, UPDATE, PRACK, Delayed Offer, re-INVITE without SDP
- Session updates after connect to avoid transcoding

The handling of REFER can be configured for all calls, using the global parameter `SBCReferBehavior`. For configuring different REFER handling options for different UAs (i.e., IP Groups), use the IP Profile table parameter, 'SBC Remote Refer Behavior'.

- Local handling of REFER: This option is used for UAs that do not support REFER. Upon receipt of a REFER request, instead of forwarding it to the IP Group, the device handles it locally. It generates a new INVITE to the alternative destination according to the rules in the IP-to-IP Routing table (where the 'Call Trigger' field is set to **REFER**). It is also possible to specify the IP Group that sent the REFER request, as matching criteria for the re-routing rule in this table ('ReRoute IP Group ID' field).
- Transparent handling: The device forwards the REFER with the Refer-To header unchanged.
- Re-routing through SBC: The device changes the Refer-To header so that the re-routed INVITE is sent through the SBC application.
- IP Group Name = The device sets the host part in the REFER message to the name configured for the IP Group in the IP Group table.

## 20.7.4 Interworking SIP PRACK Messages

The device supports interworking of SIP Provisional Response ACKnowledgement (PRACK) messages (18x). While some UAs may not support PRACK (RFC 3262) others may require it. The device can be configured to resolve this interoperable issue and enable sessions between such endpoints. SIP PRACK handling is configured using the IP Profile parameter, 'SBC Prack Mode':

- Optional: PRACK is optional for these UAs. If required, the device performs the PRACK process on behalf of the destination UA.
- Mandatory: PRACK is required for these UAs. Calls from UAs that do not support PRACK are rejected. Calls destined to these UAs are also required to support PRACK.
- Transparent (default): The device does not intervene with the PRACK process and forwards the request as is.

## 20.7.5 Interworking SIP Session Timer

The device supports interworking of the SIP signaling keep-alive mechanism. The SIP standard provides a signaling keep-alive mechanism using re-INVITE and UPDATE messages. In certain setups, keep-alive may be required by some SIP UAs while for others it may not be supported. The device can resolve this mismatch by performing the keep-alive process on behalf of SIP UAs that do not support it.

For configuring the handling of session expires, use the IP Profile parameter, 'SBC Session Expires Mode'.



## 20.7.6 Interworking SIP Early Media

The device supports various interworking modes for SIP early media between SIP UAs (i.e., IP Groups):

- **Early Media Enabling:** The device supports the interworking of early media between SIP UAs that support early media and those that do not support receipt of early media. Early media can arrive in provisional responses to an INVITE request. The device forwards the request of early media for IP Groups that support this capability; otherwise, the device terminates it. Provisional responses whose SDP are suppressed are changed to a SIP 180 response. This feature is also supported for delayed offers. This is configured using the IP Profile parameter, 'SBC Remote Early Media Support'. The device refers to this parameter also for features that require early media such as playing ringback tone.
- **Early Media Response Type:** The device supports the interworking of different SIP provisional response types between UAs for forwarding the early media to the caller. This can support all early media response types (default), SIP 180 only, or SIP 183 only, and is configured by the IP Profile parameter, 'SBC Remote Early Media Response Type'.
- **Multiple 18x:** The device supports the interworking of different support for multiple 18x responses (including 180 Ringing, 181 Call is Being Forwarded, 182 Call Queued, and 183 Session Progress) that are forwarded to the caller. The UA can be configured as supporting only receipt of the first 18x response (i.e., the device forwards only this response to the caller), or receipt of multiple 18x responses (default). This is configured by the IP Profile parameter, 'SBC Remote Multiple 18x Support'.
- **Early Media RTP:** The device supports the interworking with remote clients that send 18x responses with early media and whose subsequent RTP is delayed, and with remote clients that do not support this and require RTP to immediately follow the 18x response. Some clients do not support 18x with early media, while others require 18x with early media (i.e., they cannot play ringback tone locally). These various interworking capabilities are configured by the IP Profile parameters, 'SBC Remote Early Media RTP', 'SBC Remote Supports RFC 3960', and 'SBC Remote Can Play Ringback'. See the flowcharts below for the device's handling of such scenarios:

**Figure 20-6: SBC Early Media RTP 18x without SDP**

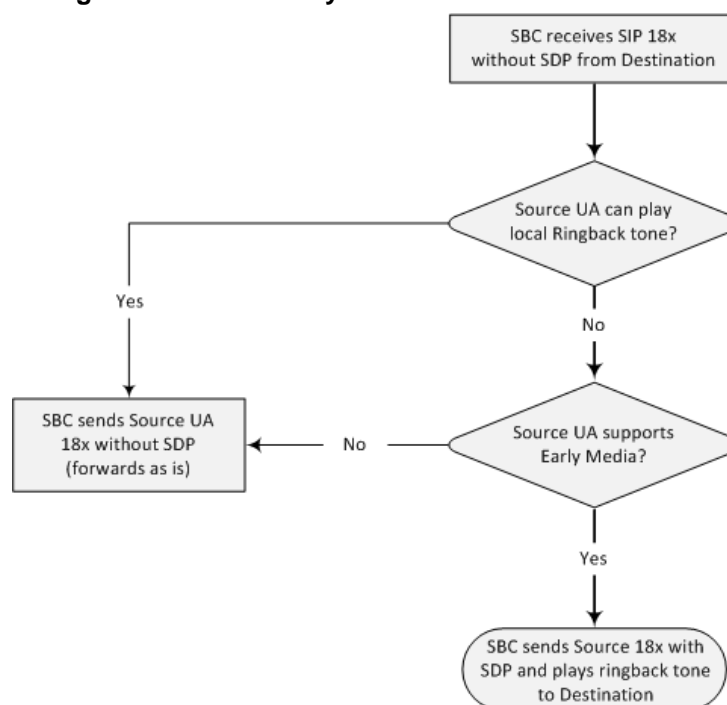
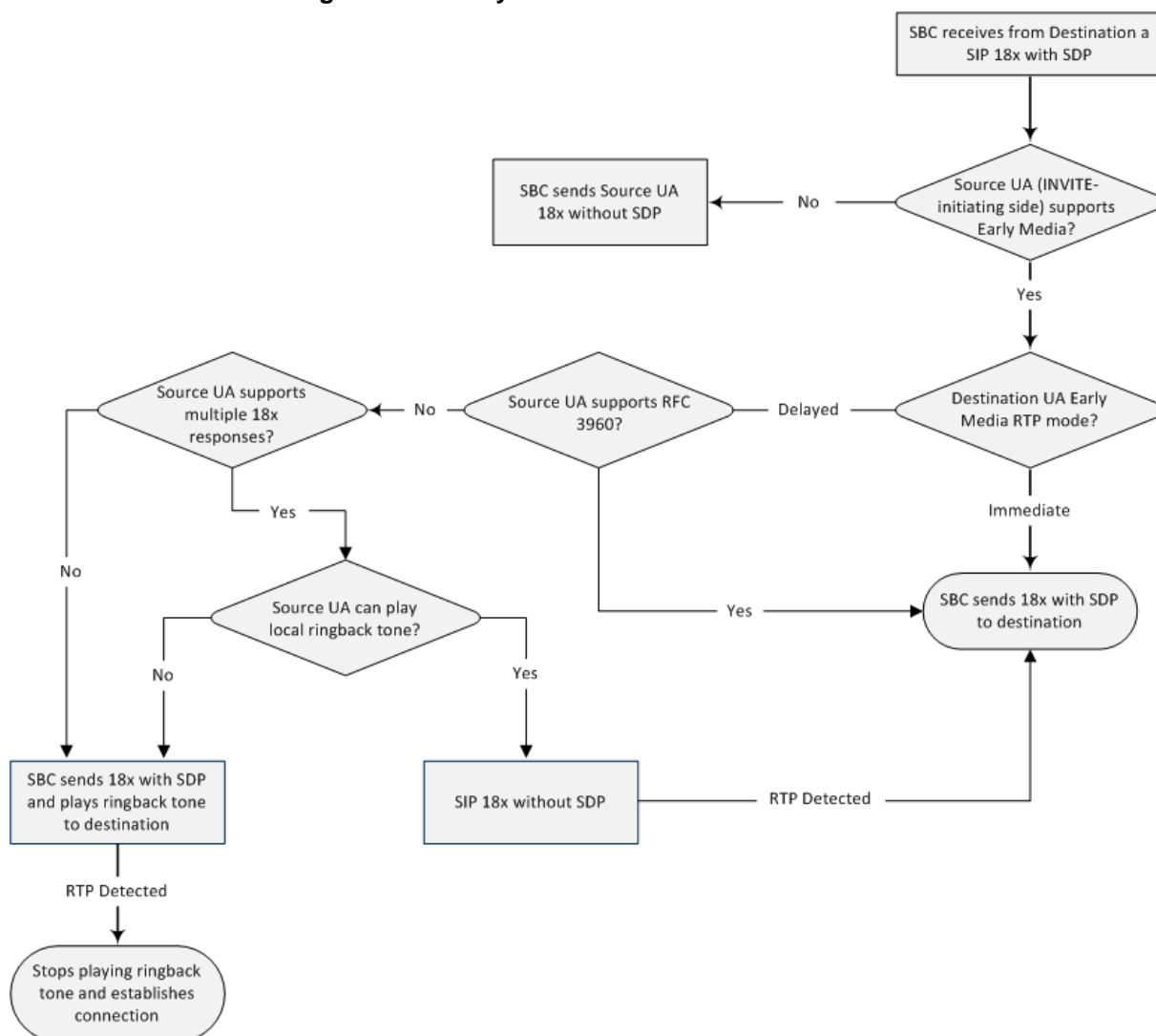




Figure 20-7: Early Media RTP - SIP 18x with SDP



### 20.7.7 Interworking SIP re-INVITE Messages

The device supports interworking of SIP re-INVITE messages. This enables communication between endpoints that generate re-INVITE requests and those that do not support the receipt of re-INVITES. The device does not forward re-INVITE requests to IP Groups that do not support it. Instead, it sends a SIP response to the re-INVITE request, which can either be a success or a failure, depending on whether the device can bridge the media between the endpoints. The device can also handle re-INVITES with or without an SDP body, enabling communication between endpoints that do not support re-INVITE requests without SDP, and those that require SDP. The device generates an SDP offer and adds it to the incoming re-INVITE request if it does not contain an SDP and only then forwards it to the destination endpoint. This interworking support is configured by the IP Profile parameter, 'SBC Remote Reinvite Support'.

### 20.7.8 Interworking SIP UPDATE Messages

The device supports interworking of the SIP UPDATED message. This enables communication between UAs that generate UPDATE requests and those that do not support the receipt of UPDATE requests. The device does not forward UPDATE requests



to IP Groups that do not support it. Instead, it sends a SIP response to the UPDATE request which can either be a success or a failure, depending on whether the device can bridge the media between the endpoints. The handling of UPDATE messages is configured by the IP Profile parameter 'SBC Remote Update Support'.

## 20.7.9 Interworking SIP re-INVITE to UPDATE

The device enables communication between endpoints (IP Groups) that do not support re-INVITE requests but support the UPDATE method, and vice versa. The device translates the re-INVITE request to the UPDATE request, and vice versa. Note that if a re-INVITE request arrives without SDP, the device generates the SDP and adds it to the outgoing UPDATE request. To enable this feature, each IP Group needs to be configured with its unique capabilities by associating it with a relevant IP Profile. For example, an IP Group that supports UPDATE requests but not re-INVITES would be configured as follows:

- SBCRemoteUpdateSupport = 2 (Supported)
- SBCRemoteReinviteSupport = 0 (Not Supported)

If a re-INVITE request needs to be forwarded to this IP Group, it is translated to an UPDATE request.

## 20.7.10 Interworking Delayed Offer

The device enables sessions between endpoints (IP Groups) that send INVITES without SDP (i.e., delayed media) and those that do not support the receipt of INVITES without SDP. The device creates an SDP and adds it to INVITES that arrive without SDP. Delayed offer is also supported when early media is present.

The interworking of delayed offer is configured using the IP Profile parameter 'SBC Remote Delayed Offer Support'.

## 20.7.11 Interworking Call Hold

The device supports the interworking of call hold / retrieve requests between IP entities supporting different call hold capabilities:

- Interworking SDP call hold formats. This is configured by the IP Profile parameter, 'SBC Remote Hold Format'.
- Interworking the play of the held tone for IP entities that cannot play held tones locally. This is configured by the IP Profile parameter, 'SBC Play Held Tone'.
- Interworking generation of held tone where the device generates the tone to the held party instead of the call hold initiator. This is configured by the IP Profile parameter, 'SBC Reliable Held Tone Source'.

For configuring IP Profiles, see Configuring IP Profiles [189](#).

# 20.8 Call Survivability

This section describes various call survivability features supported by the SBC device.

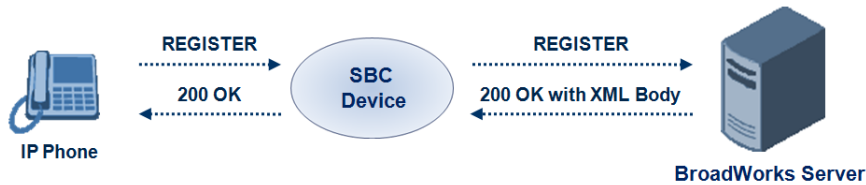
## 20.8.1 Auto-Provisioning of Subscriber-Specific Information for BroadWorks Server for Survivability

This feature enables SBC user registration for interoperability with BroadSoft BroadWorks server to provide call survivability in case of connectivity failure with the BroadWorks server, for example, due to a WAN failure. This feature enables local users to dial a local extension (or any other configured alias) that identifies another local user, in survivability mode. This feature is enabled using the SBCExtensionsProvisioningMode parameter.



In normal operation, when subscribers (such as IP phones) register to the BroadWorks server through the device, the device includes the SIP Allow-Events header in the sent REGISTER message. In response, the BroadWorks server sends the device a SIP 200 OK containing an XML body with subscriber information such as extension number, phone number, and URIs (aliases). The device forwards the 200 OK to the subscriber (without the XML body).

**Figure 20-8: Interoperability with BroadWorks Registration Process**



The device saves the users in its registration database with their phone numbers and extensions, enabling future routing to these destinations during survivability mode. When in survivability mode, the device routes the call to the Contact associated with the dialed phone number or extension number in the registration database.

Below is an example of an XML body received from the BroadWorks server:

```
<?xml version="1.0" encoding="utf-8"?>
<BroadsoftDocument version="1.0" content="subscriberData">
 <phoneNumbers>
 <phoneNumber>2403645317</phoneNumber>
 <phoneNumber>4482541321</phoneNumber>
 </phoneNumbers>
 <aliases>
 <alias>sip:bob@broadsoft.com</alias>
 <alias>sip:rhughes@broadsoft.com</alias>
 </aliases>
 <extensions>
 <extension>5317</extension>
 <extension>1321</extension>
 </extensions>
</BroadsoftDocument>
```

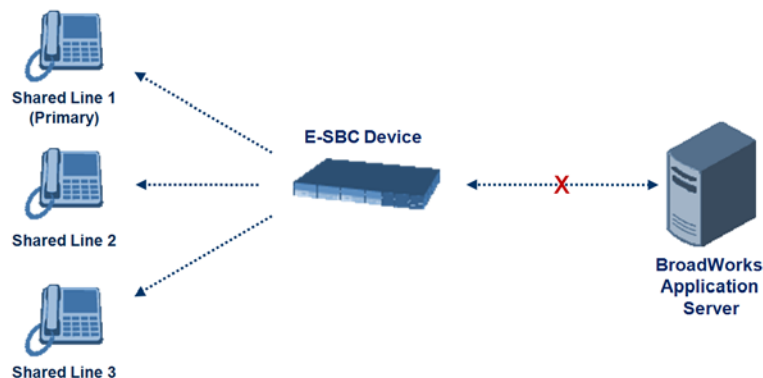
## 20.8.2 BroadSoft's Shared Phone Line Call Appearance for SBC Survivability

The device can provide redundancy for BroadSoft's Shared Call Appearance feature. When the BroadSoft application server switch (AS) fails or does not respond, or when the network connection between the device and the BroadSoft AS is down, the device manages the Shared Call Appearance feature for the SIP clients.



This feature is supported by configuring a primary extension and associating it with secondary extensions (i.e., *shared lines*) so that incoming calls to the primary extension also ring at the secondary extensions. The call is established with the first extension to answer the call, and consequently, the ringing at the other extensions stop. For example, assume primary extension number 600 is shared with secondary extensions 601 and 602. In the case of an incoming call to 600, all three phone extensions ring simultaneously (using the device's call forking feature as described in "SIP Forking Initiated by SIP Proxy Server" on page 224). Note that incoming calls specific to extensions 601 or 602 ring only at these specific extensions.

**Figure 20-9: Call Survivability for BroadSoft's Shared Line Appearance**



To configure this capability, you need to configure a shared-line, inbound manipulation rule for registration requests to change the destination number of the secondary extension numbers (e.g. 601 and 602) to the primary extension (e.g., 600). Call forking must also be enabled. The procedure below describes the main configuration required.



**Notes:**

- You can configure whether REGISTER messages from secondary lines are terminated on the device or forwarded transparently (as is), using the SBCSharedLineRegMode parameter.
- The device enables outgoing calls from all equipment that share the same line simultaneously (usually only one simultaneous call is allowed per a specific shared line).
- The LED indicator of a shared line may display the wrong current state.

➤ **To configure the Shared Line feature:**

1. In the IP Group table (see "Configuring IP Groups" on page 164), add a Server-type IP Group for the BroadWorks server.
2. In the IP Group table, add a User-type IP Group for the IP phone users and set the 'Enable SBC Client Forking' parameter to **Yes** so that the device forks incoming calls to all contacts under the same AOR that are registered in the device's registration database.
3. In the IP-to-IP Routing table (see "Configuring SBC IP-to-IP Routing" on page 236), add a rule for routing calls between the above configured IP Groups.
4. In the IP to IP Inbound Manipulation table (see "Configuring IP-to-IP Inbound Manipulations" on page 246), add a manipulation rule for the secondary extensions (e.g., 601 and 602) so that they also register in the device's database under the primary extension contact (e.g., 600):
  - Set the 'Manipulation Purpose' field to **Shared Line**.
  - Set the 'Source IP Group' field to the IP Group ID that you created for the users (e.g., 2).



- Set the 'Source Username Prefix' field to represent the secondary extensions (e.g., 601 and 602).
- Set the 'Manipulated URI' field to **Source** to manipulate the source URI.
- Set the 'Remove From Right' field to "1" to remove the last digit of the extensions (e.g., 601 is changed to 60).
- Set the 'Suffix to Add' field to "0" to add 0 to the end of the manipulated number (e.g., 60 is changed to 600).

### 20.8.3 Call Survivability for Call Centers

The device supports call survivability for call centers. When a communication failure (e.g., in the network) occurs with the remote voice application server responsible for handling the call center application (such as IVR), the device routes the incoming calls received from the customer (i.e., from the TDM gateway) to the call center agents.

In normal operation, the device registers the agents in its users registration database. Calls received from the TDM gateway are forwarded by the device to the application server, which processes the calls and sends them to specific call center agents, through the device. Upon a failure with the application server, the device routes the calls from the TDM Gateway to the agents. The device routes the call to the first available user it finds. If the call is not answered by the user, the device routes it to the next available user. The SBC can handle a sequence of up to five users, after which the session is timed out and the call is dropped.

Figure 20-10: Normal Operation in Call Center Application

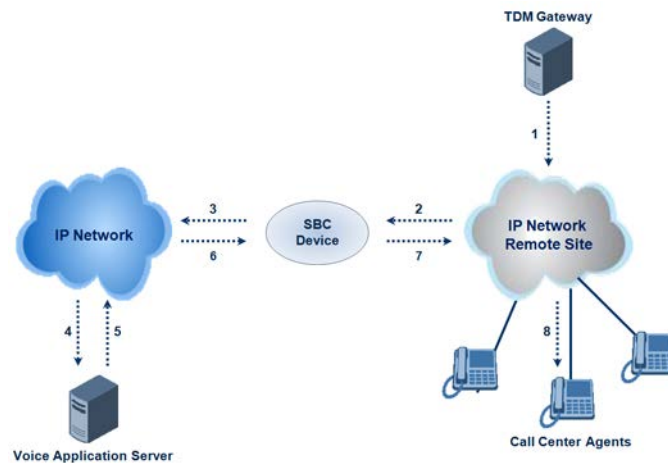
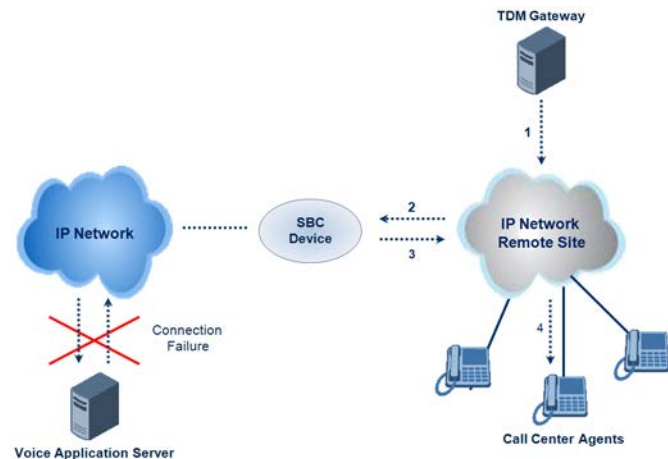


Figure 20-11: Call Survivability for Call Center



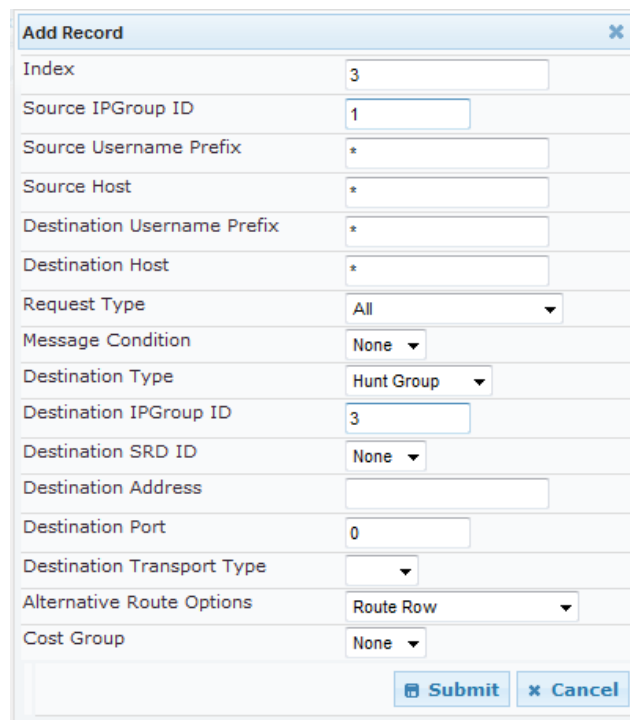


➤ **To configure call survivability for a call center application:**

1. In the IP Group table (see "Configuring IP Groups" on page 164), add IP Groups for the following entities:
  - TDM Gateway (Server-type IP Group). This entity forwards the customer calls through the device to the Application server.
  - Application server (Server-type IP Group). This entity processes the call and sends the call through the device to the specific call center agent located on a different network (remote).
  - Call center agents (User-type IP Group). You can configure multiple IP Groups to represent different groups of call center agents, for example, agents and managers.
2. In the Classification table (see "Configuring Classification Rules" on page 230), add rules to classify incoming calls that are received from the entities listed in Step 1, to IP Groups.
3. In the SBC IP-to-IP Routing table (see "Configuring SBC IP-to-IP Routing" on page 236), add the following IP-to-IP routing rules:
  - For normal operation:
    - ◆ Routing from TDM Gateway to Application server.
    - ◆ Routing from Application server to call center agents.
  - For call survivability mode: Routing from TDM Gateway to call center agents. This configuration is unique due to the following settings:
    - ◆ The 'Source IP Group ID' field is set to the IP Group of the TDM Gateway.
    - ◆ The 'Destination Type' field is set to **Hunt Group**, which is specifically used for call center survivability.
    - ◆ The 'Destination IP Group ID' field is set to the IP Group of the call center agents.

The figure below displays a routing rule example, assuming IP Group "1" represents the TDM Gateway and IP Group "3" represents the call center agents:

**Figure 20-12: Routing Rule Example for Call Center Survivability**



Add Record	
Index	3
Source IPGroup ID	1
Source Username Prefix	*
Source Host	*
Destination Username Prefix	*
Destination Host	*
Request Type	All
Message Condition	None
Destination Type	Hunt Group
Destination IPGroup ID	3
Destination SRD ID	None
Destination Address	
Destination Port	0
Destination Transport Type	
Alternative Route Options	Route Row
Cost Group	None
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	



## 20.8.4 Survivability Mode Display on Aastra IP Phones

If the SBC device is deployed in an Enterprise network with Aastra IP phones and connectivity with the WAN fails, the device provides call survivability by enabling communication between IP phone users within the LAN enterprise. In such a scenario, the device can be configured to notify the IP phones that it is currently operating in Survivability mode. When this occurs, the Aastra IP phones display the message, "StandAlone Mode" on their LCD screens. This feature is enabled by setting the `SBCEnableAASTRASurvivabilityNotice` parameter to 1.

When this feature is enabled and the SBC device is in Survivability mode, it responds to SIP REGISTER messages from the IP phones with a SIP 200 OK containing the following XML body:

```
Content-Type: application/xml
<?xml version="1.0" encoding="utf-8"?>
<LMIDocument version="1.0">
 <LocalModeStatus>
 <LocalModeActive>true</LocalModeActive>
 <LocalModeDisplay>StandAlone Mode</LocalModeDisplay>
 </LocalModeStatus>
</LMIDocument>
```

## 20.9 Call Forking

This section describes various Call Forking features supported by the device.

### 20.9.1 Initiating SIP Call Forking

The SBC device supports call forking of an incoming call to multiple SBC users (destinations). Call forking is supported by the device's capability of registering multiple SIP client user phone contacts (mobile and fixed-line extensions) under the same Address of Record (AOR) in its registration database. This feature can be implemented in the following example scenarios:

- An enterprise Help Desk, where incoming customer calls are simultaneously sent to multiple customer service agent extensions.
- An employee's phone devices, where the incoming call is simultaneously sent to multiple devices (e.g., to the employee's office phone and mobile SIP phone).
- An enterprise reception desk, where an incoming call is simultaneously sent to multiple receptionists.

The device supports various modes of call forking. For example, in Parallel call forking mode, the device sends the INVITE message simultaneously to all the users registered under the same AOR, resulting in the ringing of all extensions; the first extension to pick up the call receives the call, and all other extensions stop ringing. The Call Forking feature is configured by creating a User-type IP Group and configuring the IP Group table's parameter, 'SBC Client Forking Mode' (see [Configuring IP Groups](#) on page 164).

The device can also fork INVITE messages received for a Request-URI of a specific contact (user) registered in the database to all other users located under the same AOR as the specific contact. This is configured using the `SBCSendInviteToAllContacts` parameter.



## 20.9.2 SIP Forking Initiated by SIP Proxy Server

The device can handle SIP forking responses received from a proxy server in response to an INVITE forwarded by the device from a UA. In other words, received responses with a different SIP To header 'tag' parameter for the request forwarded by the device. This occurs in scenarios, for example, where a proxy server forks the INVITE request to several UAs, and therefore, the SBC device may receive several replies for a single request. Forked SIP responses may result in a single SDP offer with two or more SDP answers during call setup. The SBC handles this scenario by "hiding" the forked responses from the INVITE-initiating UA. This is achieved by marking the UA that responded first to the INVITE as the active UA, and only requests/responses from that UA are subsequently forwarded. All other requests/responses from other UAs are handled by the SBC (SDP offers from these users are answered with an 'inactive' media).

The SBC supports two forking modes, configured by the `SBCForkingHandlingMode` parameter:

- Latch On First - only the first received 18x response is forwarded to the INVITE initiating UA, and disregards any subsequently received 18x forking responses (with or without SDP).
- Sequential - all 18x responses are forwarded to the INVITE initiating UA, one at a time in a sequential manner. If 18x arrives with an offer only, only the first offer is forwarded to the INVITE initiating UA.

The SBC also supports media synchronization for call forking. If the active UA is the first one to send the final response (e.g., 200 OK) the call is established and all other final responses are acknowledged and a BYE is sent if needed. If another UA sends the first final response, then it is possible that the SDP answer that was forwarded to the INVITE-initiating UA is not relevant, and media synchronization is needed between the two UAs. Media synchronization is done by sending a re-INVITE request immediately after the call is established. The re-INVITE is sent without an offer to the INVITE-initiating UA. This causes the UA to send an offer which is forwarded to the UA that confirmed the call. The media synchronization process is enabled by the `EnableSBCMediaSync` parameter.

## 20.10 Alternative Routing on Detection of Failed SIP Response

The device can detect failure of a sent SIP response (e.g., TCP timeout, and UDP ICMP). In such a scenario, the device re-sends the response to an alternative destination. This support is in addition to alternative routing if the device detects failed SIP requests.

For example, assume the device sends a SIP 200 OK in response to a received INVITE request. If the device does not receive a SIP ACK in response to this, it sends a new 200 OK to the next alternative destination. This new destination can be the next given IP address resolved from a DNS from the Contact or Record-Route header in the request related to the response.



## 21 SBC Configuration

This section describes the configuration of the SBC application.



**Note:** For the SBC application, the following requirements must be met:

- The SBC application must be enabled (see "Enabling Applications" on page 157).
- The 'SBC' Software License Key must be installed on the device (see "Loading Software License Key" on page 320).

### 21.1 Configuring General Settings

The General Settings page allows you to configure general SBC parameters. For a description of these parameters, see "SBC Parameters" on page 453.

➤ **To configure general parameters:**

1. Open the General Settings page (**Configuration** tab > **VoIP** menu > **SBC** > **General Settings**).

**Figure 21-1: General Settings Page**

Transcoding Mode	Only If Required
SBC No Answer Timeout	600
SBC GRUU Mode	AsProxy
Minimum Session-Expires [sec]	90
BroadWorks Survivability Feature	Disable
Bye Authentication	Disable
SBC User Registration Time	0
SBC Proxy Registration Time	0
SBC Survivability Registration Time	0
SBC Forking Handling Mode	Latch On First
Allow Unclassified Calls	Reject
SBC Session-Expires [sec]	180
SBC Direct Media	Disable
<b>Server Authentication</b>	
Lifetime of the nonce in seconds	300
Authentication Challenge Method	0
Authentication Quality of Protection	2

2. Configure the parameters as required.
3. Click **Submit** to apply your changes.
4. To save the changes to flash memory, see "Saving Configuration" on page 308.



## 21.2 Configuring Admission Control

The Admission Control page allows you to define up to 100 rules for limiting the number of concurrent calls (SIP dialogs). These call limits can be applied per SRD, IP Group, SIP request type (e.g., INVITEs), SIP dialog direction (e.g., inbound), and/or per user (identified by its registered contact). This feature can be useful for implementing Service Level Agreements (SLA) policies.

The SIP dialog limits can be defined per SIP request type and direction. These relate to requests that initiate SIP dialogs and not the subsequent requests that can be of different type and direction. The SIP dialog-initiating request types can include SIP INVITEs, REGISTER, and/or SUBSCRIBE, or it can be configured to include the total number of all dialogs.

This feature also provides support for SIP-dialog rate control, using the "token bucket" mechanism. The token bucket is a control mechanism that dictates the rate of SIP-dialog setups based on the presence of tokens in the bucket – a logical container that holds aggregate SIP dialogs to be accepted or transmitted. Tokens in the bucket are removed ("cached in") for the ability to setup a dialog. Therefore, a flow can setup dialogs up to its peak burst rate if there are adequate tokens in the bucket and if the burst threshold is configured appropriately:

- Every SIP dialog setup request must attempt to take a token from the bucket.
- If there are no tokens, the request is dropped.
- New tokens are added to the bucket at a user-defined rate (token rate).
- If the bucket contains the maximum number of tokens, tokens to be added at that moment are dropped.

Requests that reach the user-defined call limit (maximum concurrent calls and/or call rate) are sent to an alternative route, if configured in the IP-to-IP Routing table for the SRD or IP Group. If no alternative routing rule is located, the device rejects the SIP request with a SIP 486 "Busy Here" response.



### Notes:

- The enforcement of a configured limitation for the incoming leg is performed immediately after the Classification process. If the call/request is rejected at this stage, no routing is performed. The enforcement for the outgoing leg is performed within each alternative route iteration. This is accessed from two places: one during initial classification/routing, and another during alternative routing process.
- The Admission Control table can also be configured using the table *ini* file parameter, SBCAdmissionControl.



➤ **To configure Admission Control rules:**

1. Open the Admission Control page (**Configuration** tab > **VoIP** menu > **SBC** > **Admission Control**).
2. Click the **Add** button; the following dialog box appears:

**Figure 21-2: Admission Control Page - Add Record Dialog Box**

Index	0
Limit Type	IP Group
IP Group ID	-1
SRD ID	-1
Request Type	All
Request Direction	Both
Limit	-1
Limit Per User	-1
Rate	0
Max Burst	0

3. Configure the rule as required. For a description of the parameters, see the table below.
4. Click **Submit** to apply your changes.

**Table 21-1: Admission Control Parameters**

Parameter	Description
Limit Type CLI: limit-type [SBCAdmissionControl_LimitType]	Defines the entity to which the rule applies. <ul style="list-style-type: none"> <li>▪ [0] IP Group (default)</li> <li>▪ [1] SRD</li> </ul>
IP Group ID [SBCAdmissionControl_IPGroupID]	Defines the IP Group to which you want to apply the rule. To apply the rule to all IP Groups, set this parameter to -1 (default). <b>Note:</b> This parameter is applicable only if 'Limit Type' is set to <b>IP Group</b> .
SRD ID [SBCAdmissionControl_SRID]	Defines the SRD to which you want to apply the rule. To apply the rule to all SRDs, set this parameter to -1 (default). <b>Note:</b> This parameter is applicable only if 'Limit Type' is set to <b>SRD</b> .
Request Type [SBCAdmissionControl_RequestType]	Defines the SIP dialog-initiating request type to which you want to apply the rule (not the subsequent requests that can be of different type and direction). <ul style="list-style-type: none"> <li>▪ [0] All = (Default) Includes the total number of all dialogs.</li> <li>▪ [1] INVITE</li> <li>▪ [2] SUBSCRIBE</li> </ul>



Parameter	Description
	<ul style="list-style-type: none"> <li>[3] Other</li> </ul>
Request Direction [SBCAdmissionControl_RequestDirection]	<p>Defines the direction of the SIP request to which the rule applies.</p> <ul style="list-style-type: none"> <li>[0] Both = (Default) Rule applies to inbound and outbound SIP dialogs.</li> <li>[1] Inbound = Rule applies only to inbound SIP dialogs.</li> <li>[2] Outbound = Rule applies only to outbound SIP dialogs.</li> </ul>
Limit [SBCAdmissionControl_Limit]	<p>Defines the maximum number of concurrent SIP dialogs per IP Group or SRD. You can also use the following special values:</p> <ul style="list-style-type: none"> <li>[0] 0 = Block all these dialogs.</li> <li>[-1] -1 = (Default) No limit.</li> </ul>
Limit Per User [SBCAdmissionControl_LimitPerUser]	<p>Defines the maximum number of concurrent SIP dialogs per user belonging to the specified IP Group or SRD. You can also use the following special values:</p> <ul style="list-style-type: none"> <li>[0] 0 = Block all these dialogs.</li> <li>[-1] -1 = (Default) No limit.</li> </ul>
Rate [SBCAdmissionControl_Rate]	<p>Defines the rate at which tokens are added to the token bucket per second (i.e., token rate). One token is added to the bucket every 1000 divided by the value of this parameter (in milliseconds).</p> <p>The default is 0 (i.e., unlimited rate).</p> <p><b>Note:</b> The token bucket feature is per IP Group, SRD, SIP request type, and SIP request direction.</p>
Max Burst [SBCAdmissionControl_MaxBurst]	<p>Defines the maximum number of tokens (SIP dialogs) that the bucket can hold. The device only accepts a SIP dialog if a token exists in the bucket. Once the SIP dialog is accepted, a token is removed from the bucket. If a SIP dialog is received by the device and the token bucket is empty, then the device rejects the SIP dialog. Alternatively, if the bucket is full, for example, 100 tokens, and 101 SIP dialogs arrive (before another token is added to the bucket, i.e., faster than that defined in the Rate field), then the device accepts the first 100 SIP dialogs and rejects the last one.</p> <p>Dropped requests are replied with the SIP 486 "Busy Here" response. Dropped requests are not counted in the bucket.</p> <p>The default is 0 (i.e., unlimited SIP dialogs).</p> <p><b>Note:</b> The token bucket feature is per IP Group, SRD, SIP request type, and SIP request direction.</p>

## 21.3 Configuring Allowed Coder Groups

The Allowed Coders Group page allows you to define up to five Allowed Coder Groups, each with up to 10 coders. Allowed Coder Groups determine the coders that can be used for a specific SBC leg. Therefore, the device can enforce the use of specific coders while preventing the use of other coders. Coders excluded from the Allowed Coders Group are removed from the SDP offer. Only common coders between SDP offered coders and coders configured in the Allowed Coder Groups are used. For more information, see "Restricting Coders" on page 209.

The order of appearance of coders in the Allowed Coder Group determines the coder priority (preference), whereby the first coder is given the highest priority. For more information, see "Prioritizing Coder List in SDP Offer" on page 210.



**Notes:**

- Each coder can appear only once per Allowed Coder Group.
- Allowed Coder Groups are applicable only to audio media.
- Allowed Coder Groups can be assigned to IP Profiles (see "Configuring IP Profiles" on page 189).
- The Allowed Coder Groups table can also be configured using the table ini file parameter, AllowedCodersGroup.

➤ **To configure Allowed Coder Groups:**

1. Open the Allowed Coders Group page (**Configuration** tab > **VoIP** menu > **SBC** > **Allowed Coders Group**).

**Figure 21-3: Allowed Coders Group Page**

2. From the 'Allowed Coders Group ID' drop-down list, select an ID for the Allowed Coder Group.
3. In the Coder Name table, select coders for the Allowed Coder Group.
4. Click **Submit** to apply your changes.
5. To save the changes to flash memory, see "Saving Configuration" on page 308.

## 21.4 Routing SBC

This section describes the configuration of the routing entities for the SBC application. These include the following:

- Classification rules - see "Configuring the Classification Rules" on page 230
- Condition rules - see "Configuring Condition Rules" on page 235
- IP-to-IP routing rules - see "Configuring SBC IP-to-IP Routing" on page 236
- Alternative routing reasons - see "Configuring Alternative Routing Reasons" on page 243



## 21.4.1 Configuring Classification Rules

The Classification table enables you to configure up to 100 Classification rules. Classification rules are used to classify incoming SIP dialog-initiating requests (e.g., INVITE messages) to source IP Groups from where the SIP dialog request originated. The identified IP Group is later used in the manipulation and routing processes.

Classification rules also enhance security by allowing you to create a SIP access list, whereby classified calls can be denied (i.e., blacklist) or allowed (i.e., whitelist).

The Classification table is used to classify incoming SIP dialog requests only if the other classification stages fail, as described below:

1. **Classification Stage 1 - Registered Users Database:** The device searches its registration database to check if the incoming SIP dialog arrived from a registered user:
  - Compares the SIP Contact header of the received SIP dialog to the Contact of the registered user.
  - Compares the URL in the SIP P-Asserted-Identity/From header to the registered address-of-record (AOR).

If this stage fails, the device proceeds to classification based on Proxy Set.

2. **Classification Stage 2 - Proxy Set:** If the database search fails, the device performs classification based on Proxy Set if the 'Classify By Proxy Set' parameter is enabled for the IP Group (see 'Configuring IP Groups' on page 164). If enabled, the device checks whether the INVITE's IP address (if host names, then according to the dynamically resolved IP address list) is defined for a Proxy Set ID (in the Proxy Set table). If a Proxy Set ID has such an IP address, the device classifies the INVITE to the IP Group that is associated with this Proxy Set. (The Proxy Set ID is assigned to the IP Group using the IP Group table's 'Proxy Set ID' parameter.)



**Note:** For security purposes, it is highly recommended to disable the Classify by Proxy Set feature so that the device can use the Classification table instead, for "strict" classification of incoming calls to IP Groups. In addition, in cases where multiple IP Groups are associated with the same Proxy Set ID, do **not** use the Classify by Proxy Set feature.

If this stage fails (or Classify by Proxy Set is disabled), the device proceeds to classification based on the Classification table.

3. **Classification Stage 3 - Classification Table:** If classification based on Proxy Set fails (or disabled), the device uses the Classification table to classify the SIP dialog to an IP Group. If it locates a classification rule whose characteristics (such as source IP address) match the incoming SIP dialog, then the SIP dialog is assigned to the associated IP Group. In addition, if the classification rule is defined as a whitelist, the SIP dialog is allowed and proceeds with the manipulation, routing and other SBC processes. If the classification rule is defined as a blacklist, the SIP dialog is denied.

If the classification process fails, the device rejects or allows the call, depending on the setting of the 'Unclassified Calls' parameter (on the General Settings page - **Configuration** tab > **VoIP** menu > **SBC** > **General Settings**). If this parameter is set to **Allow**, the incoming SIP dialog is assigned to an IP Group as follows:

1. The device checks on which SIP listening port (e.g., 5061) the incoming SIP dialog request arrived and the SIP Interface which is configured with this port (in the SIP Interface table).
2. The device checks the SRD that is associated with this SIP Interface (in the SIP Interface table) and then classifies the SIP dialog with the first IP Group that is associated with this SRD. For example, if IP Groups 3 and 4 use the same SRD, the device classifies the call to IP Group 3.

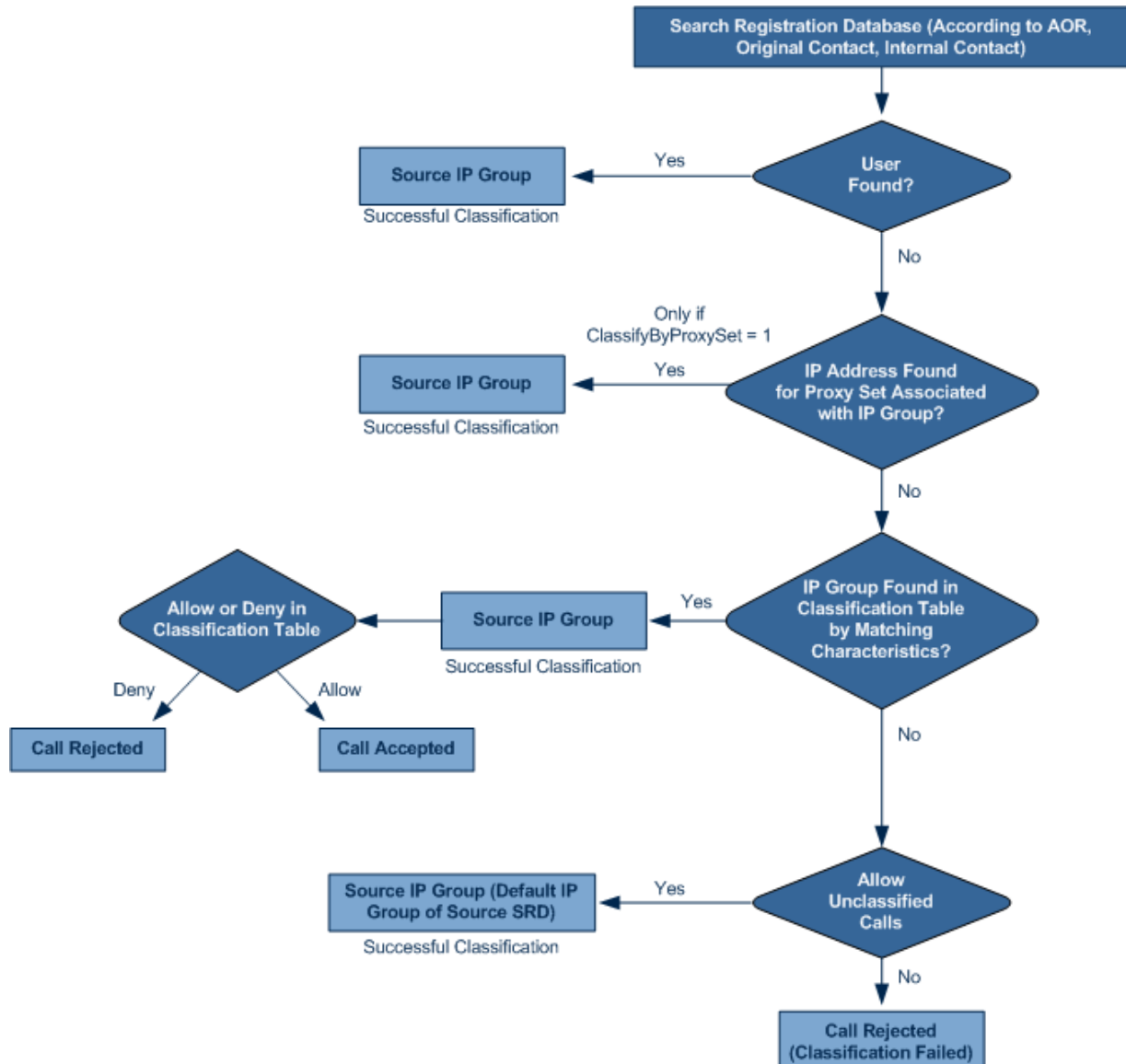




**Note:** If classification for a SIP request fails and the device is configured to reject unclassified calls, the device can send a specific SIP response code per SIP interface, configured by the 'Classification Failure Response Type' parameter in the SIP Interface table (see 'Configuring SIP Interface Table' on page 161).

The flowchart below illustrates the classification process:

**Figure 21-4: Classification Process (Identifying IP Group or Rejecting Call)**



**Notes:**

- Incoming REGISTER messages are saved in the device's registration database and sent to a destination only if they are associated with a source User-type IP Group.
- The Classification table can also be configured using the table ini file parameter, Classification.



The Classification table provides two configuration areas:

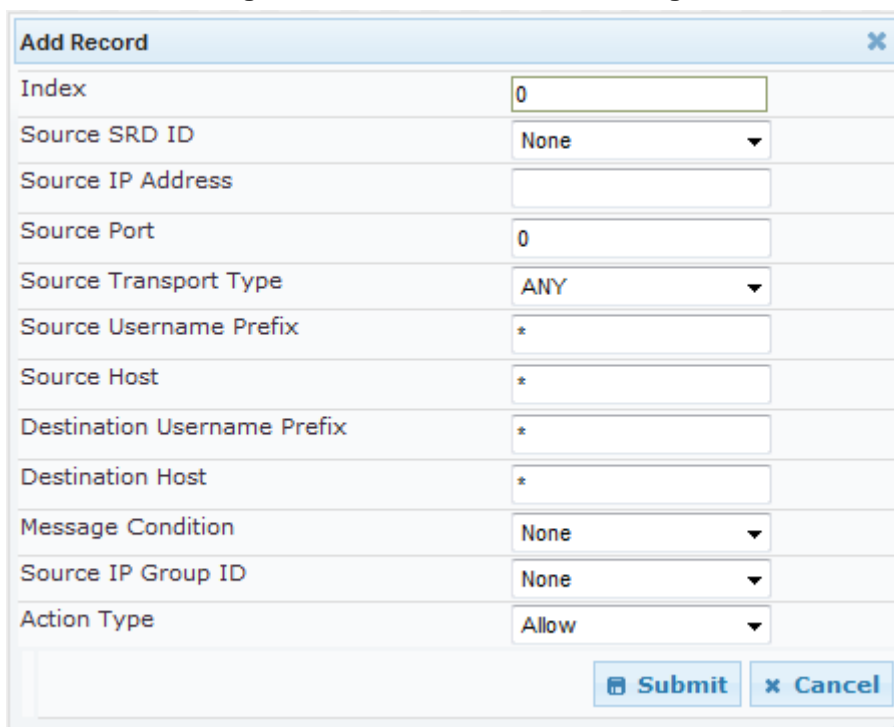
- Matching characteristics of incoming IP call, for example, source IP address.
- Operation - classifies call to an IP Group.

If the incoming call matches the characteristics of a rule, then the call is classified to the IP Group configured for that rule.

➤ **To configure classification rules:**

1. Open the Classification Table page (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **Classification Table**).
2. Click the **Add** button; the following appears:

**Figure 21-5: Classification Table Page**



3. Configure the rule as required. For a description of the parameters, see the table below.
4. Click **Submit** to apply your changes.

**Table 21-2: Classification Table Parameters**

Parameter	Description
Index	Defines the index number of the table row entry.
<b>Matching Characteristics</b>	
Source SRD ID [Classification_SrcSRDID]	<p>Defines the SRD ID of the incoming SIP dialog. The default is -1 (i.e., no SRD is assigned).</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>■ The SRDs are configured in the SRD table (see "Configuring SRD Table" on page 159).</li> <li>■ The SRDs are also associated with a port number as defined by the SIP Interface used by the SRD (see "Configuring SIP Interface Table" on page 161).</li> </ul>



Parameter	Description
Source IP Address [Classification_SrcAddress]	<p>Defines the source IP address (in dotted-decimal notation) of the incoming SIP dialog.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>If this parameter is not configured or is configured as an asterisk (*), then any source IP address is accepted.</li> <li>The IP address can include the "x" wildcard to represent single digits. For example: 10.8.8.xx represents all the addresses between 10.8.8.10 to 10.8.8.99.</li> <li>The IP address can include the asterisk (*) wildcard to represent any number between 0 and 255. For example, 10.8.8.* represents all addresses between 10.8.8.0 and 10.8.8.255.</li> </ul>
Source Port [Classification_SrcPort]	Defines the source port number of the incoming SIP dialog.
Source Transport Type [Classification_SrcTransportType]	Defines the source transport type (UDP, TCP, or TLS) of the incoming SIP dialog.
Source Username Prefix [Classification_SrcUsernamePrefix]	<p>Defines the prefix of the source URI user part of the incoming SIP dialog. The URI is typically located in the SIP From header. However, you can configure the SIP header from where the device obtains the source URI. This is done in the IP Group table, using the 'Source URI Input' parameter. For more information on how the device obtains this URI, see "SIP Dialog Initiation Process" on page 200.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For REGISTER requests, the source URL is obtained from the To header.</li> <li>The prefix can be a single digit or a range of digits. For available notations, see "Dialing Plan Notation for Routing and Manipulation" on page 385.</li> </ul>
Source Host [Classification_SrcHost]	<p>Defines the prefix of the source URI host name. The URI is typically located in the SIP From header. However, you can configure the SIP header from where the device obtains the source URI. This is done in the IP Group table, using the 'Source URI Input' parameter. For more information on how the device obtains this URI, see "SIP Dialog Initiation Process" on page 200.</p> <p>If this routing rule is not required, leave the field empty. The asterisk (*) symbol can be used to depict any source host prefix.</p> <p><b>Note:</b> For REGISTER requests, the source URL is obtained from the To header.</p>
Destination Username Prefix [Classification_DestUsernamePrefix]	<p>Defines the prefix of the destination Request-URI user part of the incoming SIP dialog.</p> <p><b>Note:</b> The prefix can be a single digit or a range of digits. For available notations, see "Dialing Plan Notation for Routing and Manipulation" on page 385.</p>
Destination Host [Classification_DestHost]	Defines the prefix of the destination Request-URI host name of the incoming SIP dialog request. If this routing rule is not required, leave the field empty. The asterisk (*) symbol can be used to depict any destination host prefix.
Message Condition [Classification_MessageCondition]	Assigns a Condition rule which can also be used to classify the



Parameter	Description
dition]	incoming SIP dialog. <b>Note:</b> Condition rules are configured in the Condition Table (see "Configuring Condition Rules" on page 235).
<b>Operation Rule</b>	
Source IP Group ID [Classification_SrcIPGroupID]	Defines an IP Group to which the incoming SIP dialog request is assigned if this SIP dialog matches the matching rule. The default is -1 (i.e., no IP Group is assigned). <b>Notes:</b> <ul style="list-style-type: none"> <li>The IP Group must be associated with the selected SRD.</li> <li>The IP Group is used for SBC routing and manipulations.</li> <li>To define IP Groups, see "Configuring IP Groups" on page 164.</li> </ul>
Action Type [Classification_ActionType]	Defines a whitelist or blacklist for incoming SIP dialog requests that match the characteristics of the classification rule. <ul style="list-style-type: none"> <li>[0] Deny = Blocks incoming SIP dialogs that match the characteristics of the Classification rule (blacklist).</li> <li>[1] Allow = Allows incoming SIP dialogs that match the characteristics of the Classification rule (whitelist) and assigns it to the associated IP Group. (default)</li> </ul>

### 21.4.1.1 Classification Based on URI of Selected Header Example

The following example describes how to configure classification of incoming calls to IP Groups, based on source URI in a specific SIP header.

This example assumes the following incoming INVITE message:

```
INVITE sip:8000@10.33.4.226 SIP/2.0
Via: SIP/2.0/UDP 10.33.4.226;branch=z9hG4bKVEBTDHSAHSUYRTEXEDEGJY
From: <sip:100@10.33.4.226>;tag=YSQQKXXREVDPTYPTNFMWG
To: <sip:8000@10.33.4.226>
Call-ID: FKPNOYRNKROIMEGBSSKS@10.33.4.226
CSeq: 1 INVITE
Contact: <sip:100@10.33.4.226>
Route: <sip:2000@10.10.10.10>,<sip:300@10.10.10.30>
Supported: em,100rel,timer,replaces
P-Caller-Party-ID: <sip:1111@10.33.38.1>
User-Agent: Sip Message Generator V1.0.0.5
Content-Length: 0
```

- In the Classification table, add the following classification rules:

Index	Source Username Prefix	Destination Username Prefix	Destination Host	Source IP Group ID
0	333	-	-	1
1	1111	2000	10.10.10.10	2



2. In the IP Group table, add the following IP Groups:

Index	Source URI Input	Destination URI Input
1	-	-
2	P-Called-Party-ID	Route

In this example, a match exists only for Classification Rule #1. This is because the source (1111) and destination (2000) username prefixes match those in the INVITE's P-Called-Party-ID header (i.e., "<sip:1111@10.33.38.1>") and Route header (i.e., "<sip:2000@10.10.10.10>"), respectively. These SIP headers were determined in IP Group ID 2.

## 21.4.2 Configuring Condition Rules

Condition rules define special conditions for the incoming SIP messages. Condition rules are configured using the same syntax as that used for message conditions in the Message Manipulations table (see Configuring SIP Message Manipulation on page 182).

Condition rules are used if assigned to any of the following:

- Classification rules in the Classification table (see Configuring Classification Rules on page 230). This enables you to use SIP message conditions as additional matching criteria for classifying incoming SIP dialogs to IP Groups, thereby increasing the strictness of the classification process.
- IP-to-IP routing rules in the IP-to-IP Routing table (see Configuring SBC IP-to-IP Routing on page 236): This enables you to use SIP message conditions as additional matching criteria for selecting the routing rule.

You can define simple Condition rules, for example, "header.to.host contains company" or complex rules using the "AND" or "OR" Boolean operands. You can also use regular expressions (regex), for example:

- "body.sdp regex pcmu" can be used to enable routing based on the offered codec (G.711 Mu) in the incoming SDP message.
- "body.sdp regex (AVP[0-9][\s]\*s8[\s][\n])" can be used to enable routing based on payload type 8 in the incoming SDP message.



### Notes:

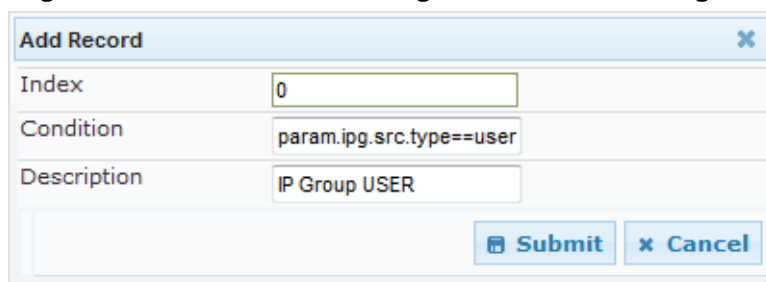
- For a detailed description of the syntax for configuring SIP message manipulation rules, refer to *SIP Message Manipulations Quick Reference Guide*.
- The Condition table can also be configured using the table ini file parameter, ConditionTable.



➤ **To configure Condition rules:**

1. Open the Condition Table page (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **Condition Table**).
2. Click the **Add** button; the following dialog box appears:

**Figure 21-6: Condition Table Page - Add Record Dialog Box**



The dialog box titled 'Add Record' contains three input fields: 'Index' with the value '0', 'Condition' with the value 'param.ipg.src.type==user', and 'Description' with the value 'IP Group USER'. At the bottom right are 'Submit' and 'Cancel' buttons.

3. Configure the rule as required. For a description of the parameters, see the table below.
4. Click **Submit**.

The figure below shows an example of the Condition table configured with the following rules:

- **Index 1:** Incoming SIP dialog that is classified as belonging to a User-type IP Group.
- **Index 2:** Incoming SIP dialog with a SIP Via header.
- **Index 3:** Incoming SIP dialog with 101 as the user part in the SIP From header.

**Figure 21-7: Condition Table Page**

Index	Condition	Description
0	param.ipg.src.type==user	IP Group USER
1	header.via.exists	Includes SIP Via header
2	header.from.url.user=='101'	101 user part of From header

**Table 21-3: Condition Table Parameters Description**

Parameter	Description
Condition [ConditionTable_Condition]	Defines the Condition rule of the SIP message. The valid value is a string. <b>Note:</b> User and host parts must be enclosed in single quotes.
Description [ConditionTable_Description]	Defines a brief description of the Condition rule.

## 21.4.3 Configuring SBC IP-to-IP Routing

The IP-to-IP Routing table enables you to configure up to 1,000 SBC IP-to-IP routing rules. This table provides enhanced IP-to-IP call routing capabilities for routing received SIP dialog messages (e.g., INVITE) to a destination IP address. The SIP message is routed according to a routing rule whose configured input characteristics (e.g., Source IP Group) match the incoming SIP message. If the characteristics of an incoming call does not match the first rule, the call characteristics is then compared to those of the second rule, and so on until a matching rule is located. If no rule is matched, the call is rejected.

The call can be routed to one of the following IP destinations:

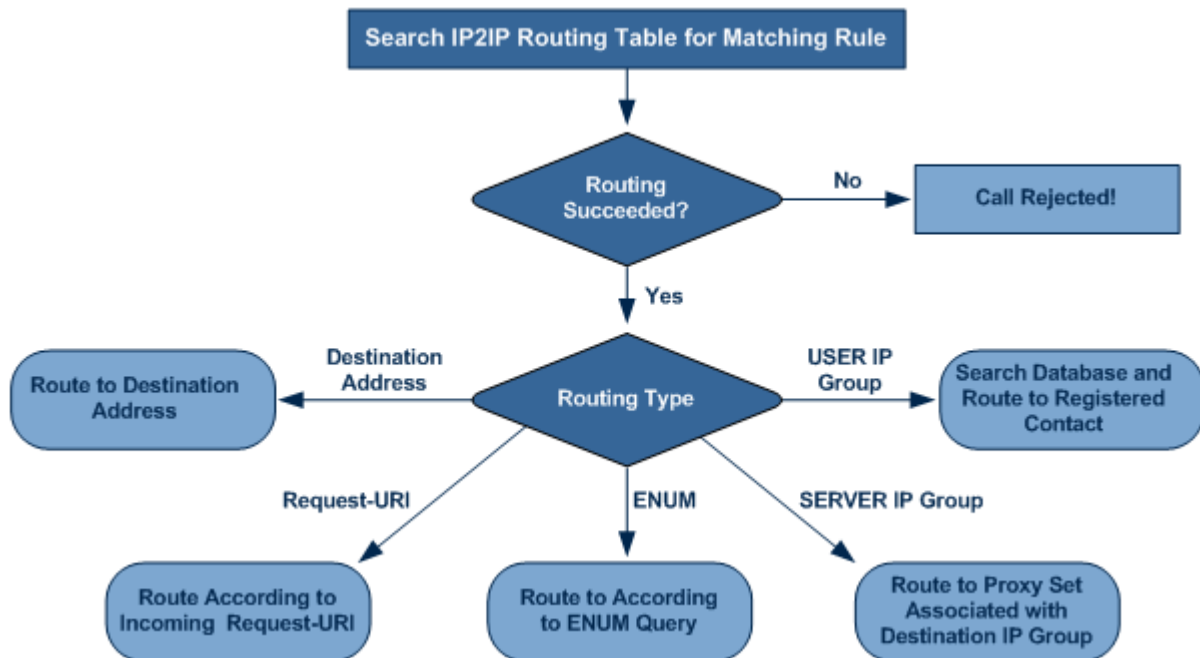
- IP Group - the destination is the address configured for the Proxy Set associated with the IP Group (allows redundancy/load balancing).
- Specified destination address (can be based on IP address, host name, port, transport



type, and/or SRD). Routing to a host name can be resolved using NAPTR/SRV/A-Record.

- Request-URI of incoming SIP dialog initiating requests.
- ENUM query.
- Hunt Group - used for call survivability (see "Call Survivability for Call Centers" on page 221).
- IP address (in dotted-decimal notation or FQDN - NAPTR/SRV/A-Record resolutions) according to a specified Dial Plan index listed in the loaded Dial Plan file.
- LDAP server or LDAP query result. For more information on LDAP-based routing, see "Routing Based on LDAP Active Directory Queries" on page 141.

**Figure 21-8: IP-to-IP Routing Types**



For all destination types listed above except destination IP Group, the IP Group can optionally be itself, configured to provide the destination SRD and/or IP Profile. If neither destination SRD nor destination IP Group is defined, the destination SRD is the source SRD and the destination IP Group is its default IP Group.

The IP-to-IP Routing table also provides the following features:

- **Alternative routing or load balancing:** In addition to the alternative routing/load balancing provided by the Proxy Set associated with the destination IP Group, the table allows the configuration of alternative routes whereby if a route fails, the next adjacent (below) rule in the table that is configured as 'Alt Route Ignore/Consider Inputs' are used. The alternative routes rules can be set to enforce the input matching criteria or to ignore any matching criteria. Alternative routing occurs upon one of the following conditions:
  - A request sent by the device is responded with one of the following:
    - ◆ SIP response code (i.e., 4xx, 5xx, and 6xx SIP responses) configured in the SBC Alternative Routing Reasons table (see "Configuring Alternative Routing Reasons" on page 243).
    - ◆ SIP 408 Timeout or no response (after timeout).
  - The DNS resolution includes IP addresses that the device has yet to try (for the current call).

Messages are re-routed with the same SIP Call-ID and CSeq header fields (increased by 1).



- **Re-routing of SIP requests:** This table enables you to configure "re-routing" rules of requests (e.g., INVITEs) that the device sends upon receipt of SIP 3xx responses or REFER messages. These rules are configured for destinations that do not support receipt of 3xx or REFER and where the device handles the requests locally (instead of forwarding the 3xx or REFER to the destination).
- **Least cost routing (LCR):** If the LCR feature is enabled, the device searches the routing table for matching routing rules and then selects the one with the lowest call cost. The call cost of the routing rule is done by assigning it a Cost Group. For configuring Cost Groups, see "Least Cost Routing" on page 149. If two routing rules have identical costs, then the rule appearing higher up in the table (i.e., first-matched rule) is used. If a selected route is unavailable, the device uses the next least-cost routing rule. However, even if a matched rule is not assigned a Cost Group, the device can select it as the preferred route over other matched routing rules with Cost Groups, according to the settings of the LCR parameter, LCRDefaultCost (see "Enabling LCR and Configuring Default LCR" on page 152).

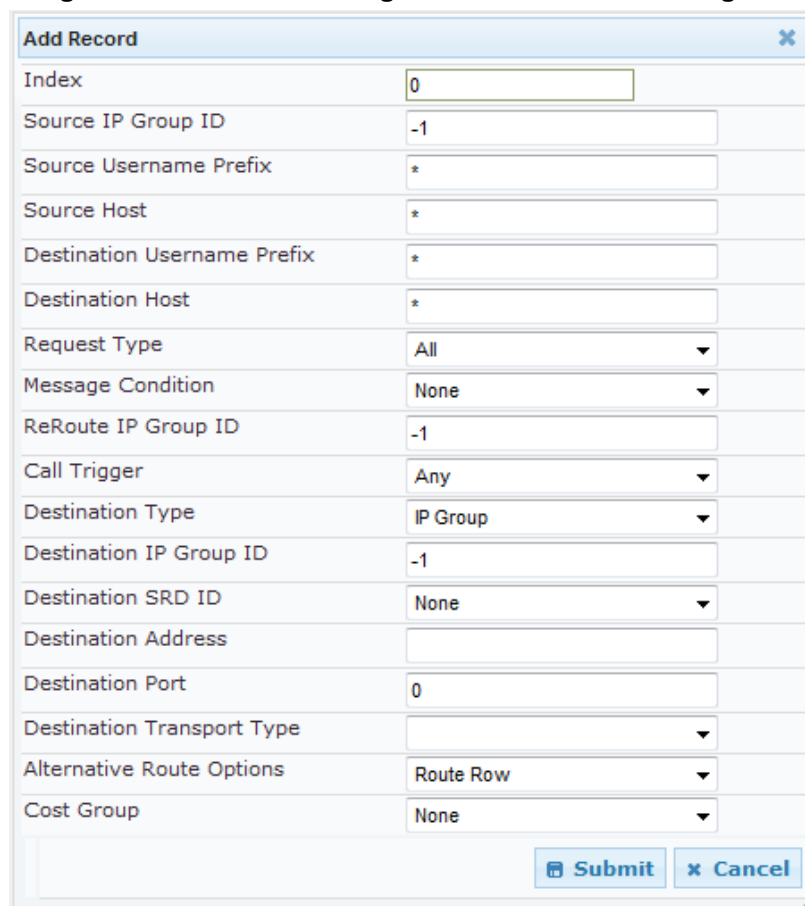


**Note:** The IP-to-IP Routing table can also be configured using the table ini file parameter, IP2IPRouting (see "SBC Parameters" on page 453).

➤ **To configure SBC IP-to-IP routing rules:**

1. Open the IP-to-IP Routing Table page (**Configuration** tab > **VoIP** menu > **SBC** submenu > **Routing SBC** submenu > **IP to IP Routing Table**).
2. Click the **Add** button; the following dialog box appears:

**Figure 21-9: IP-to-IP Routing Table - Add Record Dialog Box**



Index	0
Source IP Group ID	-1
Source Username Prefix	*
Source Host	*
Destination Username Prefix	*
Destination Host	*
Request Type	All
Message Condition	None
ReRoute IP Group ID	-1
Call Trigger	Any
Destination Type	IP Group
Destination IP Group ID	-1
Destination SRD ID	None
Destination Address	
Destination Port	0
Destination Transport Type	
Alternative Route Options	Route Row
Cost Group	None

Submit Cancel



3. Configure the rule as required. For a description of the parameters, see the table below.
4. Click **Submit**.

**Table 21-4: IP-to-IP Routing Table Parameters Description**

Parameter	Description
<b>Matching Characteristics</b>	
Source IP Group ID [IP2IPRouting_SrcIPGroupID]	Selects the IP Group from where the IP-to-IP call originated. Typically, the IP Group of an incoming SIP dialog is determined (or classified) using the 'Classification' table (see <a href="#">Configuring Classification Rules</a> on page 230). If not used (i.e., any IP Group), simply leave the field empty. The default is -1.
Source Username 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. For example, to denote any prefix, use the asterisk (*) symbol; to denote calls without a user part in the URI, use the \$ sign. For available notations, see "Dialing Plan Notation for Routing and Manipulation" on page 385. The default is * (i.e., any prefix).
Source Host [IP2IPRouting_SrcHost]	Defines the host part of the incoming SIP dialog's source URI (usually the From URI). If this rule is not required, leave the field empty. To denote any host name, use the asterisk (*) symbol (default).
Destination Username 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. For example, to denote any prefix, use the asterisk (*) symbol; to denote calls without a user part in the URI, use the \$ sign. For available notations, see "Dialing Plan Notation for Routing and Manipulation" on page 385. The default is * (i.e., any prefix).
Destination Host [IP2IPRouting_DestHost]	Defines the host part of the incoming SIP dialog's destination URI (usually the Request-URI). If this rule is not required, leave the field empty. The asterisk (*) symbol (default) can be used to denote any destination host.
Request Type [IP2IPRouting_RequestType]	Defines the SIP dialog request type of the incoming SIP dialog. <ul style="list-style-type: none"> <li>▪ [0] All (default)</li> <li>▪ [1] INVITE</li> <li>▪ [2] REGISTER</li> <li>▪ [3] SUBSCRIBE</li> <li>▪ [4] INVITE and REGISTER</li> <li>▪ [5] INVITE and SUBSCRIBE</li> <li>▪ [6] OPTIONS</li> </ul>
Message Condition [IP2IPRouting_MessageCondition]	Selects a Message Condition rule. To configure Message Condition rules, see "Configuring Condition Rules" on page 235.
ReRoute IP Group ID	Defines the IP Group that initiated (sent) the SIP redirect



Parameter	Description
[IP2IPRouting_ReRouteIPGroupID]	<p>response (e.g., 3xx) or REFER message. This field is typically used for re-routing requests (e.g., INVITEs) when interworking is required for SIP 3xx redirect responses or REFER messages (for more information, see "Interworking SIP 3xx Redirect Responses" on page 212 and "Interworking SIP REFER Messages" on page 214, respectively). This parameter functions together with the 'Call Trigger' field (see below).</p> <p>The default is -1 (i.e., not configured).</p>
Call Trigger [IP2IPRouting_Trigger]	<p>Defines the reason (i.e, trigger) for re-routing the SIP request:</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Any = (Default) This routing rule is used for all scenarios (re-routes and non-re-routes).</li> <li>▪ <b>[1]</b> 3xx = Re-routes the request if it was triggered as a result of a SIP 3xx response.</li> <li>▪ <b>[2]</b> REFER = Re-routes the INVITE if it was triggered as a result of a REFER request.</li> <li>▪ <b>[3]</b> 3xx or REFER = Applies to options <b>[1]</b> and <b>[2]</b>.</li> <li>▪ <b>[4]</b> 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.</li> </ul>
<b>Operation Routing Rule</b>	
Destination Type [IP2IPRouting_DestType]	<p>Determines the destination type to which the outgoing SIP dialog is sent.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> 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).</li> <li>▪ <b>[1]</b> 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'.</li> <li>▪ <b>[2]</b> 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.</li> <li>▪ <b>[3]</b> 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.</li> <li>▪ <b>[4]</b> Hunt Group = Used for call center survivability. For more information, see "Call Survivability for Call Centers" on page 221.</li> <li>▪ <b>[5]</b> 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: &lt;destination / called prefix number&gt;,0,&lt;IP destination&gt; Note that the second parameter "0" is ignored. An example of a configured Dial Plan (# 6) in the Dial Plan file is shown below:</li> </ul>



Parameter	Description
	<p><b>[ PLAN6 ]</b></p> <pre>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</pre> <p>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 <b>[PLAN1]</b>, "1" denotes <b>[PLAN2]</b>, and so on.</p> <ul style="list-style-type: none"> <li>▪ <b>[7]</b> LDAP = LDAP-based routing.</li> </ul>
Destination IP Group ID <b>[IP2IPRouting_DestIPGroupID]</b>	<p>Defines the IP Group ID to where you want to route the call. The SIP dialog messages are sent to the IP address defined for the Proxy Set associated with this IP Group. If you select an IP Group, it is unnecessary to configure a destination IP address (in the 'Destination Address' field). However, if both parameters are configured, then the IP Group takes precedence.</p> <p>If the destination IP Group is of USER type, the device searches for a match between the Request-URI (of the received SIP dialog) to an AOR registration record in the device's database. The SIP dialog is then sent to the IP address of the registered contact.</p> <p>The default is -1.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This parameter is only relevant if the parameter 'Destination Type' is set to 'IP Group'. However, regardless of the settings of the parameter 'Destination Type', the IP Group is still used - only for determining the IP Profile or outgoing SRD. If neither IP Group nor SRD are defined in this table, the destination SRD is determined according to the source SRD associated with the Source IP Group (configured in the IP Group table, see "Configuring IP Groups" on page 164). If this table does not define an IP Group but only an SRD, then the first IP Group associated with this SRD (in the IP Group table) is used.</li> <li>▪ If the selected destination IP Group ID is type SERVER, the request is routed according to the IP Group addresses.</li> <li>▪ If the selected destination IP Group ID is type USER, the request is routed according to the IP Group specific database (i.e., only to registered users of the selected database).</li> <li>▪ If the selected destination IP Group ID is ANY USER (<b>[-2]</b>), the request is routed according to the general database (i.e., any matching registered user).</li> </ul>
Destination SRD ID <b>[IP2IPRouting_DestSRDID]</b>	<p>Defines the SRD ID. The default is None.</p> <p><b>Note:</b> The destination IP Group must belong to the destination SRD if both are configured in this table.</p>
Destination Address <b>[IP2IPRouting_DestAddress]</b>	<p>Defines the destination to where the call is sent. This can be an IP address or a domain name (e.g., domain.com). If</p>



Parameter	Description
	<p>ENUM-based routing is used (i.e., the 'Destination Type' parameter is set to ENUM) this 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 Multiple Interface table. The ENUM reply includes a SIP URI (user@host) which is used as the destination Request-URI in this routing table.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable only if the 'Destination Type' parameter is set to Dest Address [1] or ENUM [3].</li> <li>When using domain names, enter a DNS server IP address or alternatively, define these names in the Internal DNS table (see Configuring the Internal SRV Table on page 106).</li> <li>To terminate SIP OPTIONS messages at the device (i.e., to handle them locally), set this parameter to "internal".</li> </ul>
Destination Port [IP2IPRouting_DestPort]	Defines the destination port to where the call is sent.
Destination Transport Type [IP2IPRouting_DestTransportType]	<p>Defines the transport layer type for sending the call:</p> <ul style="list-style-type: none"> <li><b>[-1]</b> Not Configured (default)</li> <li><b>[0]</b> UDP</li> <li><b>[1]</b> TCP</li> <li><b>[2]</b> TLS</li> </ul> <p><b>Note:</b> When this parameter is set to -1, the transport type is determined by the parameter SIPTransportType.</p>
Alternative Route Options [IP2IPRouting_AltRouteOptions]	<p>Determines whether this routing rule is the main routing rule or an alternative routing rule (to the rule defined directly above it in the table).</p> <ul style="list-style-type: none"> <li><b>[0]</b> Route Row (default) = Main routing rule - the device first attempts to route the call to this route if the incoming SIP dialog's input characteristics matches this rule.</li> <li><b>[1]</b> Alt Route Ignore Inputs = If the call cannot be routed to the main route (Route Row), the call is routed to this alternative route regardless of the incoming SIP dialog's input characteristics.</li> <li><b>[2]</b> Alt Route Consider Inputs = If the call cannot be routed to the main route (Route Row), the call is routed to this alternative route only if the incoming SIP dialog matches this routing rule's input characteristics.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>The alternative routing entry (<b>[1]</b> or <b>[2]</b>) must be defined in the next consecutive table entry index to the Route Row entry (i.e., directly below it). For example, if Index 4 is configured as a Route Row, Index 5 must be configured as the alternative route.</li> <li>For IP-to-IP alternative routing, configure alternative routing reasons upon receipt of 4xx, 5xx, and 6xx SIP responses (see Configuring Alternative Routing Reasons on page 243). However, if no response, ICMP, or a SIP 408 response is received, the device attempts to use the</li> </ul>



Parameter	Description
	<p>alternative route even if no entries are configured in the 'SBC Alternative Routing Reasons' table.</p> <ul style="list-style-type: none"> <li>Multiple alternative route entries can be configured (e.g., Index 1 is the main route - Route Row - and indices 2 through 4 are configured as alternative routes).</li> </ul>
Cost Group [IP2IPRouting_CostGroup]	<p>Assigns a Cost Group to the routing rule for determining the cost of the call. To configure Cost Groups, see "Configuring Cost Groups" on page 153.</p> <p>By default, no Cost Group is assigned to the rule.</p>

### 21.4.4 Configuring Alternative Routing Reasons

The SBC Alternative Routing Reasons page allows you to define up to five different call release (termination) reasons for call releases. If a call is released as a result of one of these reasons provided in SIP 4xx, 5xx, and 6xx response codes, the device attempts to locate an alternative route for the call. The call release reason type can be configured, for example, when there is no response to an INVITE message (after INVITE re-transmissions), where the device issues an internal 408 'No Response' implicit release reason.

Release reasons can also be configured to indicate that a route for an SRD or IP Group has reached its call admission control limit (i.e., maximum concurrent calls and/or call rate), as set in the Admission Control table (see "Configuring Admission Control" on page 226). In such a scenario, an alternative route configured in the IP-to-IP Routing table can be used.

Alternative routing rules are configured in the IP-to-IP Routing table where the 'Alternative Route Options' parameter is set to **Alt Route Ignore Inputs** or **Alt Route Consider Inputs**. For more information, see "Configuring SBC IP-to-IP Routing" on page 236.



#### Notes:

- Alternative routing occurs even if this table is not configured upon scenarios where no response, ICMP, or a SIP 408 response is received.
- SIP requests pertaining to an SRD or IP Group that reach the call limit (maximum concurrent calls and/or call rate) as defined in the Call Admission table are sent to an alternative route if configured in the IP-to-IP Routing table for the SRD or IP Group. If no alternative routing rule is located, the device automatically rejects the SIP request with a SIP 486 "Busy Here" response.
- The SBC Alternative Routing Reasons table can also be configured using the table ini file parameter, SBCAlternativeRoutingReasons.



➤ To configure SIP reason codes for alternative IP routing:

1. Open the SBC Alternative Routing Reasons page (**Configuration** tab > **VoIP** menu > **SBC** > **Routing SBC** > **Alternative Routing Reasons**).

Figure 21-10: Alternative Routing Reasons Page

SBC Alternative Routing Reasons	
Reason 1	401
Reason 2	
Reason 3	
Reason 4	
Reason 5	

2. Configure different call failure reasons that invoke alternative routing.
3. Click **Submit** to apply your changes.

## 21.5 SBC Manipulations

This section describes the configuration of the manipulation rules for the SBC application.

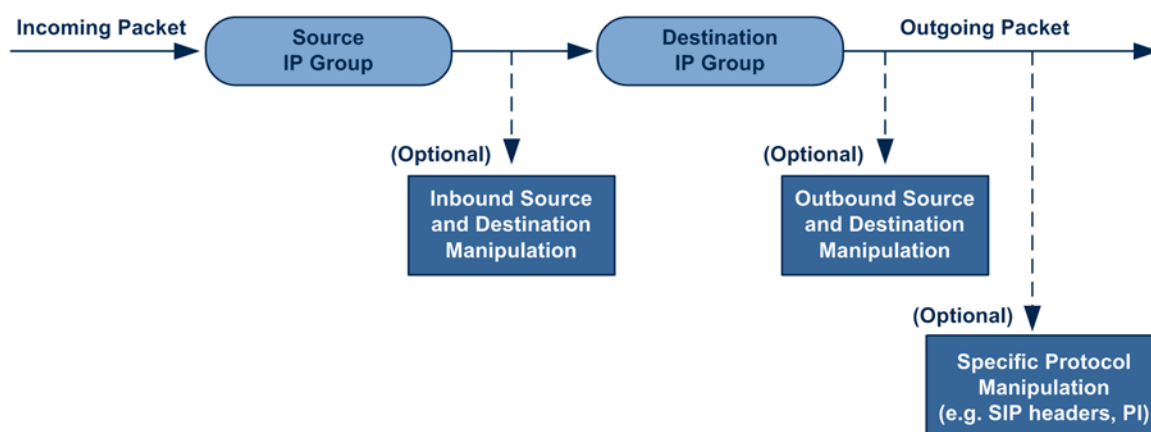


**Note:** For additional manipulation features, see the following:

- "Configuring SIP Message Policy Rules".
- "Configuring SIP Message Manipulation" on page 182.

The device supports SIP URI user part (source and destination) manipulations for inbound and outbound routing. These manipulations can be applied to a source IP group, source and destination host and user prefixes, and/or user-defined SIP request (e.g., INVITE, OPTIONS, SUBSCRIBE, and/or REGISTER). Since outbound manipulations are performed after routing, the outbound manipulation rule matching can also be done by destination IP Group. Manipulated destination user and host are performed on the following SIP headers: Request-URI, To, and Remote-Party-ID (if exists). Manipulated source user and host are performed on the following SIP headers: From, P-Asserted (if exists), P-Preferred (if exists), and Remote-Party-ID (if exists).

Figure 21-11: SIP URI Manipulation in IP-to-IP Routing





You can also restrict source user identity in outgoing SIP dialogs in the Outbound Manipulation table (using the column PrivacyRestrictionMode). The device identifies an incoming user as restricted if one of the following exists:

- From header user is 'anonymous'.
- P-Asserted-Identity and Privacy headers contain the value 'id'.

All restriction logic is done after the user number has been manipulated.

Host name (source and destination) manipulations are simply host name substitutions with the names defined for the source and destination IP Groups respectively (if any, in the IP Group table).

Below is an example of a call flow and consequent SIP URI manipulations:

■ **Incoming INVITE from LAN:**

```
INVITE sip:1000@10.2.2.3;user=phone;x=y;z=a SIP/2.0
Via: SIP/2.0/UDP 10.2.2.6;branch=z9hGLLLLLan
From: <sip:7000@10.2.2.6;user=phone;x=y;z=a>;tag=0lLAN;parameter1=abe
To: <sip:1000@10.2.2.3;user=phone>
Call-ID: USELLLLAN@10.2.2.3
CSeq: 1 INVITE
Contact: <sip:7000@10.2.2.3>
Supported: em,100rel,timer,replaces
Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK
User-Agent: Sip Message Generator V1.0.0.5
Content-Type: application/sdp
Content-Length: 155
v=0
o=SMG 791285 795617 IN IP4 10.2.2.6
s=Phone-Call
c=IN IP4 10.2.2.6
t=0 0
m=audio 6000 RTP/AVP 8
a=rtpmap:8 pcma/8000
a=sendrecv
a=ptime:20
```

■ **Outgoing INVITE to WAN:**

```
INVITE sip: 9721000@ITSP;user=phone;x=y;z=a SIP/2.0
Via: SIP/2.0/UDP 212.179.1.12;branch=z9hGWwan
From:
<sip:97000@IP_PBX;user=phone;x=y;z=a>;tag=OWan;parameter1=abe
To: <sip: 9721000@ ITSP;user=phone>
Call-ID: USEVWWAN@212.179.1.12
CSeq: 38 INVITE
Contact: <sip:7000@212.179.1.12>
Supported: em,100rel,timer,replaces
Allow:
REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER
User-Agent: Sip Message Generator V1.0.0.5
Content-Type: application/sdp
Content-Length: 155
v=0
o=SMG 5 9 IN IP4 212.179.1.11
s=Phone-Call
c=IN IP4 212.179.1.11
t=0 0
m=audio 8000 RTP/AVP 8
a=rtpmap:8 pcma/8000
```



```
a=sendrecv
a=ptime:20
```

The SIP message manipulations in the example above (contributing to typical topology hiding) are as follows:

- Inbound source SIP URI user name from "7000" to "97000":

```
From:<sip:7000@10.2.2.6;user=phone;x=y;z=a>;tag=01LAN;parameter1=abe
```

to

```
From:
<sip:97000@IP_PBX;user=phone;x=y;z=a>;tag=0Wan;parameter1=abe
```

- Source IP Group name (i.e., SIP URI host name) from "10.2.2.6" to "IP\_PBX":

```
From:<sip:7000@10.2.2.6;user=phone;x=y;z=a>;tag=01LAN;parameter1=abe
```

to

```
From:
<sip:97000@IP_PBX;user=phone;x=y;z=a>;tag=0Wan;parameter1=abe
```

- Inbound destination SIP URI user name from "1000" to "9721000":

```
INVITE sip:1000@10.2.2.3;user=phone;x=y;z=a SIP/2.0
```

```
To: <sip:1000@10.2.2.3;user=phone>
```

to

```
INVITE sip:9721000@ITSP;user=phone;x=y;z=a SIP/2.0
```

```
To: <sip:9721000@ITSP;user=phone>
```

- Destination IP Group name (SIP URI host name) from "10.2.2.3" to "ITSP":

```
INVITE sip:1000@10.2.2.3;user=phone;x=y;z=a SIP/2.0
```

```
To: <sip:1000@10.2.2.3;user=phone>
```

to

```
INVITE sip:9721000@ITSP;user=phone;x=y;z=a SIP/2.0
```

```
To: <sip:9721000@ITSP;user=phone>
```

## 21.5.1 Configuring IP-to-IP Inbound Manipulations

The IP to IP Inbound Manipulation table allows you to configure up to 100 manipulation rules for manipulating the source or destination SIP URI user part of inbound SIP dialog requests. You can apply these manipulations to different SIP dialog message types (e.g., INVITE or REGISTER) and SIP headers as follows:

- Manipulated destination URI user part are done on the following SIP headers: Request-URI, To, and Remote-Party-ID (if exists)
- Manipulated source URI user part are done on the following SIP headers: From, P-Asserted-Identity (if exists), P-Preferred-Identity (if exists), and Remote-Party-ID (if exists)

The IP to IP Inbound Manipulation table provides two configuration areas:

- Matching characteristics (*Rule*) of incoming call, for example, source host name.
- Manipulation operation (*Action*), for example, remove user-defined number of characters from the left of the SIP URI user part.

If the incoming call matches the characteristics of a rule, then its manipulation action is applied.



**Notes:**

- The IP Group table can be used to configure a host name that overwrites the received host name. This manipulation can be done for source or destination IP Groups (see "Configuring IP Groups" on page 164).
- The IP to IP Inbound Manipulation table can also be configured using the table ini file parameter, IPInboundManipulation.

➤ **To configure IP-to-IP inbound manipulation rules:**

1. Open the IP to IP Inbound Manipulation page (**Configuration** tab > **VoIP** menu > **SBC** > **Manipulations SBC** > **IP to IP Inbound**).
2. Click the **Add** button; the following dialog box appears:

**Figure 21-12: IP to IP Inbound Manipulation Page - Add Dialog Box**

3. Configure a rule as required. For a description of the parameters, see the table below.
4. Click **Submit**.

**Table 21-5: IP to IP Inbound Manipulation Parameters Description**

Parameter	Description
<b>Matching Characteristics (Rule)</b>	
Additional Manipulation [IPInboundManipulation_IsAdditionalManipulation]	<p>Determines whether additional SIP URI user part manipulation is done for the table entry rule listed directly above it.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> No = (Default) Regular manipulation rule (not done in addition to the rule above it).</li> <li>▪ <b>[1]</b> 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.</li> </ul> <p><b>Note:</b> Additional manipulation can only be done on a different SIP URI, source or destination, to the rule configured in the</p>



Parameter	Description
	row above as configured by the 'Manipulated URI' parameter (see below).
Manipulation Purpose [IPInboundManipulation_ManipulationPurpose]	<p>Defines the purpose of the manipulation:</p> <ul style="list-style-type: none"> <li><b>[0]</b> Normal = (Default) Inbound manipulations affect the routing input and source and/or destination number.</li> <li><b>[1]</b> Routing input only = Inbound manipulations affect the routing input only, retaining the original source and destination number.</li> <li><b>[2]</b> Shared Line = Used for the 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, see "BroadSoft's Shared Phone Line Call Appearance for SBC Survivability" on page <a href="#">219</a>.</li> </ul>
Source IP Group ID [IPInboundManipulation_SrcIpGroup]	<p>Defines the IP Group from where the incoming INVITE is received.</p> <p>For any IP Group, enter the value "-1".</p>
Source Username Prefix [IPInboundManipulation_SrcUsernamePrefix]	<p>Defines the prefix of the source SIP URI user name (usually in the From header).</p> <p>For any prefix, enter the asterisk "*" symbol (default).</p> <p><b>Note:</b> The prefix can be a single digit or a range of digits. For available notations, see "Dialing Plan Notation for Routing and Manipulation" on page <a href="#">385</a>.</p>
Source Host [IPInboundManipulation_SrcHost]	<p>Defines the source SIP URI host name - full name (usually in the From header). For any host name, enter the asterisk "*" symbol (default).</p>
Destination Username Prefix [IPInboundManipulation_DestinationUsernamePrefix]	<p>Defines the prefix of the destination SIP URI user name (usually in the Request-URI).</p> <p>For any prefix, enter the asterisk "*" symbol (default).</p> <p><b>Note:</b> The prefix can be a single digit or a range of digits. For available notations, see "Dialing Plan Notation for Routing and Manipulation" on page <a href="#">385</a>.</p>
Destination Host [IPInboundManipulation_DestinationHost]	<p>Defines the destination SIP URI host name - full name (usually in the Request URI).</p> <p>For any host name, enter the asterisk "*" symbol (default).</p>
Request Type [IPInboundManipulation_RequestType]	<p>Defines the SIP request type to which the manipulation rule is applied.</p> <ul style="list-style-type: none"> <li><b>[0]</b> All = (Default) All SIP messages.</li> <li><b>[1]</b> INVITE = All SIP messages except REGISTER and SUBSCRIBE.</li> <li><b>[2]</b> REGISTER = Only REGISTER messages.</li> <li><b>[3]</b> SUBSCRIBE = Only SUBSCRIBE messages.</li> <li><b>[4]</b> INVITE and REGISTER = All SIP messages except SUBSCRIBE.</li> <li><b>[5]</b> INVITE and SUBSCRIBE = All SIP messages except REGISTER.</li> </ul>
Manipulated URI [IPInboundManipulation_ManipulatedURI]	<p>Determines whether the source or destination SIP URI user part is manipulated.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Source = (Default) Manipulation is done on the source</li> </ul>



Parameter	Description
	SIP URI user part. <ul style="list-style-type: none"> <li>▪ <b>[1]</b> Destination = Manipulation is done on the destination SIP URI user part.</li> </ul>
<b>Operation Rule (Action)</b>	
Remove From Left <b>[IPInboundManipulation_RemoveFromLeft]</b>	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 <b>[IPInboundManipulation_RemoveFromRight]</b>	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". <b>Note:</b> If both 'Remove From Right' and 'Leave From Right' parameters are configured, the 'Remove From Right' setting is applied first.
Leave From Right <b>[IPInboundManipulation_LeaveFromRight]</b>	Defines the number of characters that you want retained from the right of the user name. <b>Note:</b> If both 'Remove From Right' and 'Leave From Right' parameters are configured, the 'Remove From Right' setting is applied first.
Prefix to Add <b>[IPInboundManipulation_Prefix2Add]</b>	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 <b>[IPInboundManipulation_Suffix2Add]</b>	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".

## 21.5.2 Configuring IP-to-IP Outbound Manipulations

The IP to IP Outbound Manipulation page allows you to configure up to 100 manipulation rules for manipulating SIP URI user part (source and destination) of outbound SIP dialog requests. Manipulation rules in the table are located according to the source IP Group, and source and destination host and user prefixes and can be applied to a user-defined SIP request type (e.g., INVITE, OPTIONS, SUBSCRIBE, and /or REGISTER). However, since outbound manipulations are done only after routing, the outbound manipulation rule matching can also be done by destination IP Group.

- Manipulated destination URI user part are performed on the following SIP headers: Request URI, To, and Remote-Party-ID (if exists).
- Manipulated source URI user part are performed on the following SIP headers: From, P-Asserted (if exists), P-Preferred (if exists), and Remote-Party-ID (if exists).

The IP to IP Outbound Manipulation table provides two configuration areas:

- Matching characteristics (*Rule*) of incoming call, for example, source host name.
- Manipulation operation (*Action*), for example, remove user-defined number of characters from the left of the SIP URI user part.

If the incoming call matches the characteristics of a rule, then its manipulation action is applied.




**Notes:**

- Manipulated destination SIP URI user names are done on the following SIP headers: Request URI, To, and Remote-Party-ID (if exists).
- Manipulated source SIP URI user names are done on the following SIP headers: From, P-Asserted (if exists), P-Preferred (if exists), and Remote-Party-ID (if exists)
- SIP URI host name (source and destination) manipulations can also be configured in the IP Group table. These manipulations are simply host name substitutions with the names defined for the source and destination IP Groups respectively.
- The IP to IP Outbound Manipulation table can also be configured using the table ini file parameter, IPOutboundManipulation.

➤ **To configure IP-to-IP outbound manipulation rules:**

1. Open the IP to IP Outbound Manipulation page (**Configuration** tab > **VoIP** menu > **SBC** > **Manipulations SBC** > **IP to IP Outbound**).
2. Click the **Add** button; the following dialog box appears:

**Figure 21-13: IP to IP Outbound Manipulation Page - Add Dialog Box**

Rule	Action
Index	<input type="text" value="0"/>
Additional Manipulation	<input type="text" value="No"/>
Source IP Group ID	<input type="text" value="-1"/>
Destination IP Group ID	<input type="text" value="-1"/>
Source Username Prefix	<input type="text" value="*"/>
Source Host	<input type="text" value="*"/>
Destination Username Prefix	<input type="text" value="*"/>
Destination Host	<input type="text" value="*"/>
Request Type	<input type="text" value="All"/>
ReRoute IP Group ID	<input type="text" value="-1"/>
Call Trigger	<input type="text" value="Any"/>
Manipulated URI	<input type="text" value="Source"/>
<input type="button" value="Submit"/> <input type="button" value="Cancel"/>	

3. Configure a rule as required. For a description of the parameters, see the table below.
4. Click **Submit**.



Table 21-6: IP to IP Outbound Manipulation Table Parameters Description

Parameter	Description
<b>Matching Characteristics (Rule)</b>	
Additional Manipulation [IPOutboundManipulation_Is AdditionalManipulation]	<p>Determines whether additional SIP URI user part manipulation is done for the table entry rule listed directly above it.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> No = (Default) Regular manipulation rule - not done in addition to the rule above it.</li> <li>▪ <b>[1]</b> Yes = If the previous table row entry rule matched the call, consider this row entry as a match as well and perform the manipulation specified by this rule.</li> </ul> <p><b>Note:</b> Additional manipulation can only be performed on a different SIP URI (either source or destination) to the rule configured in the row above (configured by the 'Manipulated URI' parameter).</p>
Source IP Group ID [IPOutboundManipulation_Sr cIPGroupID]	<p>Defines the IP Group from where the INVITE is received.</p> <p>For any Source IP Group, enter the value -1.</p>
Destination IP Group ID [IPOutboundManipulation_De stIPGroupID]	<p>Defines the IP Group to where the INVITE is to be sent.</p> <p>For any Destination IP Group, enter the value -1.</p>
Source Username Prefix [IPOutboundManipulation_Sr cUsernamePrefix]	<p>Defines the prefix of the source SIP URI user name (usually in the From header).</p> <p>For any prefix, enter the asterisk "*" symbol (default).</p> <p><b>Note:</b> The prefix can be a single digit or a range of digits. For available notations, see "Dialing Plan Notation for Routing and Manipulation" on page 385.</p>
Source Host [IPOutboundManipulation_Sr cHost]	<p>Defines the source SIP URI host name - full name (usually in the From header).</p> <p>For any host name, enter the asterisk "*" symbol (default).</p>
Destination Username Prefix [IPOutboundManipulation_De stUsernamePrefix]	<p>Defines the prefix of the destination SIP URI user name (usually in the Request-URI).</p> <p>For any prefix, enter the asterisk "*" symbol (default).</p> <p><b>Note:</b> The prefix can be a single digit or a range of digits. For available notations, see "Dialing Plan Notation for Routing and Manipulation" on page 385.</p>
Destination Host [IPOutboundManipulation_De stHost]	<p>Defines the destination SIP URI host name - full name (usually in the Request URI).</p> <p>For any host name, enter the asterisk "*" symbol (default).</p>
Request Type [IPOutboundManipulation_Re questType]	<p>Defines the SIP request type to which the manipulation rule is applied.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> All = (Default) all SIP messages.</li> <li>▪ <b>[1]</b> INVITE = All SIP messages except REGISTER and SUBSCRIBE.</li> <li>▪ <b>[2]</b> REGISTER = Only SIP REGISTER messages.</li> <li>▪ <b>[3]</b> SUBSCRIBE = Only SIP SUBSCRIBE messages.</li> <li>▪ <b>[4]</b> INVITE and REGISTER = All SIP messages except SUBSCRIBE.</li> <li>▪ <b>[5]</b> INVITE and SUBSCRIBE = All SIP messages except REGISTER.</li> </ul>



Parameter	Description
ReRoute IP Group ID [IPOutboundManipulation_ReRouteIPGroupID]	<p>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.</p> <p>The default is -1 (i.e., not configured).</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter functions together with the 'Call Trigger' parameter (see below).</li> <li>For more information on interworking of SIP 3xx redirect responses or REFER messages, see "Interworking SIP 3xx Redirect Responses" on page 212 and "Interworking SIP REFER Messages" on page 214, respectively.</li> </ul>
Call Trigger [IPOutboundManipulation_Tri gger]	<p>Defines the reason (i.e., trigger) for the re-routing of the SIP request:</p> <ul style="list-style-type: none"> <li><b>[0]</b> Any = (Default) Re-routed for all scenarios (re-routes and non-re-routes).</li> <li><b>[1]</b> 3xx = Re-routed if it triggered as a result of a SIP 3xx response.</li> <li><b>[2]</b> REFER = Re-routed if it triggered as a result of a REFER request.</li> <li><b>[3]</b> 3xx or REFER = Applies to options <b>[1]</b> and <b>[2]</b>.</li> <li><b>[4]</b> Initial only = Regular requests that the device forwards to a destination. In other words, re-routing of requests triggered by the receipt of REFER or 3xx does not apply.</li> </ul>
Manipulated URI [IPOutboundManipulation_Is AdditionalManipulation]	<p>Determines whether the source or destination SIP URI user part is manipulated.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Source = (Default) Manipulation is done on the source SIP URI user part.</li> <li><b>[1]</b> Destination = Manipulation is done on the destination SIP URI user part.</li> </ul>
<b>Operation Manipulation Rule (Action)</b>	
Remove From Left [IPOutboundManipulation_Re moveFromLeft]	<p>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".</p>
Remove From Right [IPOutboundManipulation_Re moveFromRight]	<p>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".</p>
Leave From Right [IPOutboundManipulation_Le aveFromRight]	<p>Defines the number of characters that you want retained from the right of the user name.</p>
Prefix to Add [IPOutboundManipulation_Pr efix2Add]	<p>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".</p>
Suffix to Add [IPOutboundManipulation_Su ffix2Add]	<p>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".</p>



Parameter	Description
Privacy Restriction Mode <b>[IPOutboundManipulation_PrivacyRestrictionMode]</b>	<p>Determines user privacy handling (i.e., restricting source user identity in outgoing SIP dialogs).</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Transparent = (Default) No intervention in SIP privacy.</li> <li>▪ <b>[1]</b> Don't change privacy = The user identity remains the same as in the incoming SIP dialog. If a restricted number exists, the restricted presentation is normalized as follows: <ul style="list-style-type: none"> <li>✓ From URL header: anonymous@anonymous.invalid.</li> <li>✓ If a P-Asserted-Identity header exists (either in the incoming SIP dialog or added by the device), a Privacy header is added with the value "id".</li> </ul> </li> <li>▪ <b>[2]</b> Restrict = The user identity is restricted (the restricted presentation is as mentioned above).</li> <li>▪ <b>[3]</b> Remove Restriction = The device attempts to reveal the user identity by setting user values in the From header and removing the privacy "id" value if the Privacy header exists.</li> </ul> <p>If the From header user is anonymous, the value is taken from the P-Preferred-Identity, P-Asserted-Identity, or Remote-Party-ID header (if exists).</p> <p>The device identifies an incoming user as restricted if one of the following exists:</p> <ul style="list-style-type: none"> <li>▪ From header user is anonymous.</li> <li>▪ P-Asserted-Identity and Privacy headers contain the value "id".</li> </ul> <p><b>Note:</b> All restriction logic is performed after the user number has been manipulated.</p>



## Reader's Notes



# Part VI

## Stand-Alone Survivability Application







## 22 SAS Overview

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:

- The SAS application is available only if the device is installed with the SAS Software License Key.
- Throughout this section, the term *user agent* (UA) refers to the enterprise's LAN phone user (i.e., SIP telephony entities such as IP phones).
- Throughout this section, the term *proxy* or *proxy server* refers to the enterprise's centralized IP Centrex or IP-PBX.
- Throughout this section, the term SAS refers to the SAS application running on the device.

### 22.1 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 258.
- **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 259.



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



## 22.1.1 SAS Outbound Mode

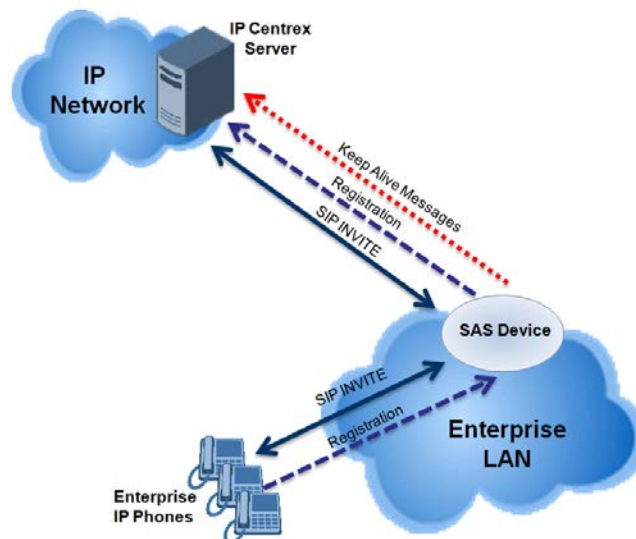
This section describes the SAS outbound mode, which includes the following states:

- Normal state (see "Normal State" on page 258)
- Emergency state (see "Emergency State" on page 258)

### 22.1.1.1 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 22-1: SAS Outbound Mode in Normal State (Example)**



### 22.1.1.2 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.

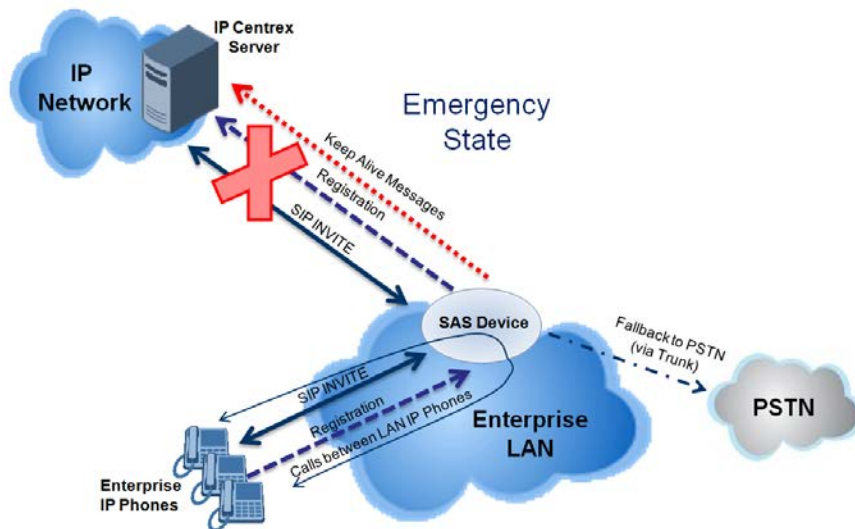
When the device receives calls, it searches its SAS registration database to locate the destination address (according to AOR or Contact). If the destination address is not found, SAS forwards the call to the default gateway. Typically, the default gateway is defined as the device itself (on which SAS 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 263.



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

**Figure 22-2: 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 260.

### 22.1.2 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.



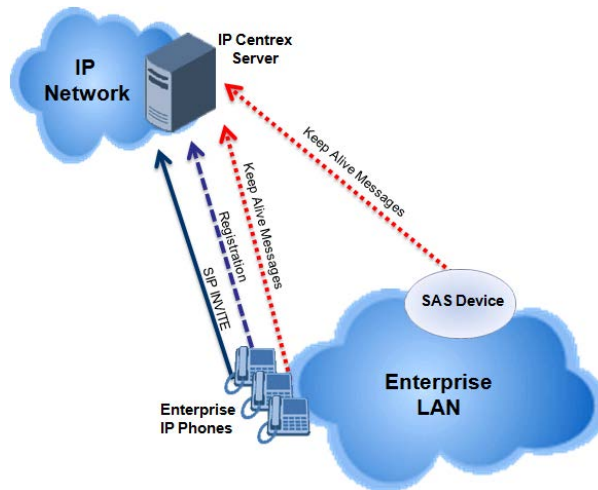
**Note:** In this SAS deployment, the UAs (e.g., IP phones) must support configuration for primary and secondary proxy servers (i.e., proxy redundancy), as well as homing. Homing allows the UAs to switch back to the primary server from the secondary proxy once the connection to the primary server returns (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.



### 22.1.2.1 Normal State

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

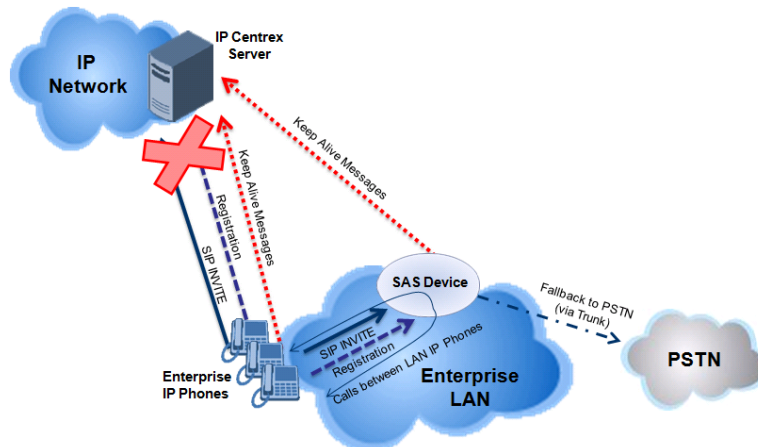
**Figure 22-3: SAS Redundant Mode in Normal State (Example)**



### 22.1.2.2 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 22-4: SAS Redundant Mode in Emergency State (Example)**



### 22.1.2.3 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).



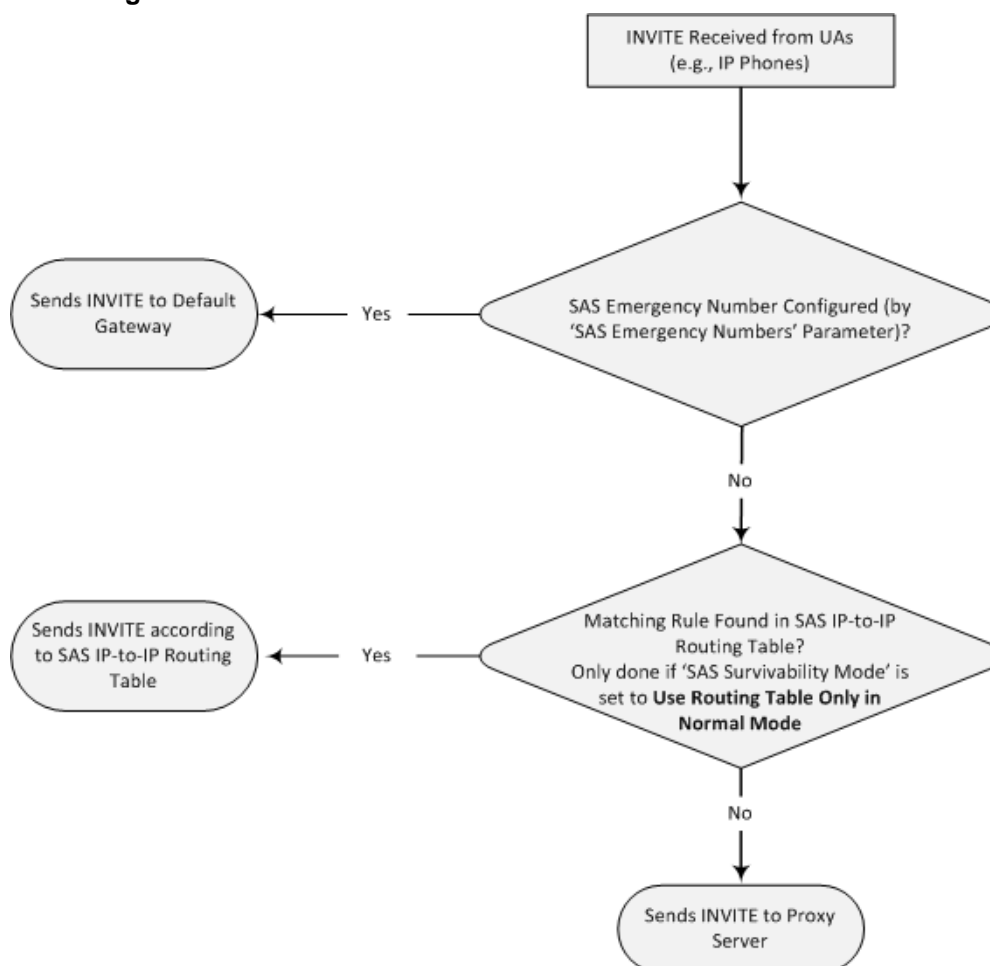
## 22.2 SAS Routing

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

### 22.2.1 SAS Routing in Normal State

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

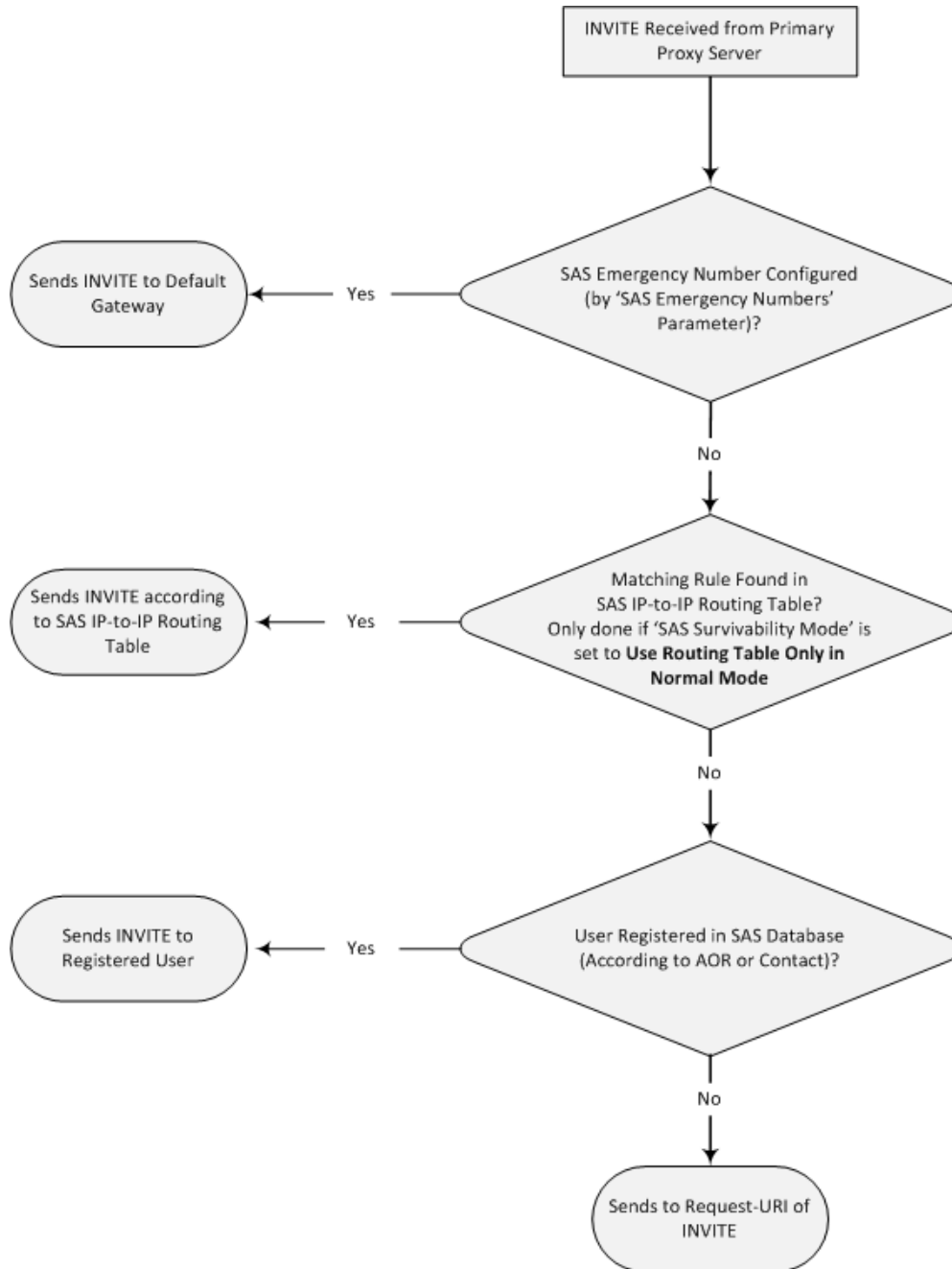
**Figure 22-5: Flowchart of INVITE from UA's in SAS Normal State**





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

**Figure 22-6: Flowchart of INVITE from Primary Proxy in SAS Normal State**

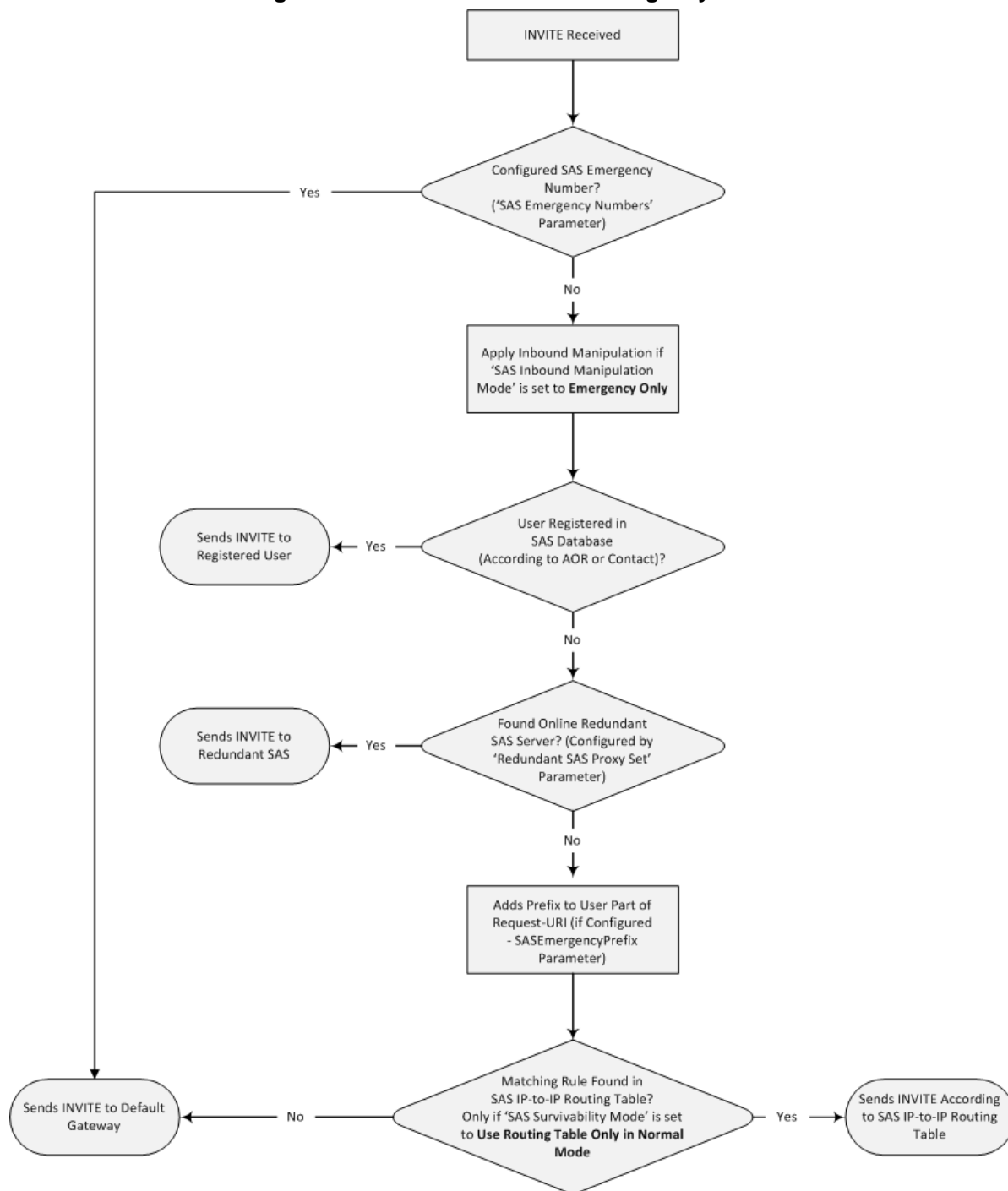




## 22.2.2 SAS Routing in Emergency State

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

**Figure 22-7: Flowchart for SAS Emergency State**





## Reader's Notes



## 23 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 265)
- SAS outbound mode (see "Configuring SAS Outbound Mode" on page 268)
- SAS redundant mode (see "Configuring SAS Redundant Mode" on page 269)
- Gateway and SAS applications deployed together (see "Configuring Gateway Application with SAS" on page 269)
- Optional, advanced SAS features (see "Advanced SAS Configuration" on page 273)

### 23.1 General SAS Configuration

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

#### 23.1.1 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 23-1: Enabling SAS Application**



3. Click **Submit**.
4. Save the changes to the flash memory with a device reset.



## 23.1.2 Configuring Common SAS Parameters

The procedure below describes how to configure SAS settings that are common to all SAS modes. This includes various SAS parameters as well as configuring the Proxy Set for the SAS proxy (if required). The SAS Proxy Set ID defines the address of the UAs' external proxy.

➤ **To configure common SAS settings:**

1. Open the SAS Configuration page (**Configuration** tab > **VoIP** menu > **SAS** > **Stand Alone Survivability**).
2. Define the port used for sending and receiving SAS messages. This can be any of the following port types:
  - UDP port - defined in the 'SAS Local SIP UDP Port' field
  - TCP port - defined in the 'SAS Local SIP TCP Port' field
  - TLS port - defined in the 'SAS Local SIP TLS Port' field



**Note:** This SAS port must be different than the device's local gateway port (i.e., that defined for the 'SIP UDP/TCP/TLS Local Port' parameter in the SIP General Parameters page - **Configuration** tab > **VoIP** menu > **SIP Definitions** > **General Parameters**).

3. In the 'SAS Default Gateway IP' field, define the IP address and port (in the format *x.x.x.x:port*) of the device (i.e., Gateway application). Note that the port of the device is defined by the parameter 'SIP UDP Local Port' (refer to the note in Step 2 above).
4. In the 'SAS Registration Time' field, define the value for the SIP Expires header, which is sent in the 200 OK response to an incoming REGISTER message when SAS is in emergency state.
5. 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 this parameter is set to '1-User Part Only', then upon receiving 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.



Figure 23-2: Configuring Common Settings

SAS Local SIP UDP Port	5080
SAS Default Gateway IP	
SAS Registration Time	20
SAS Local SIP TCP Port	5080
SAS Local SIP TLS Port	5081
SAS Proxy Set	2
SAS Emergency Numbers	
SAS Binding Mode	1-User Part Only
SAS Survivability Mode	Standard
Enable ENUM	Disable
Enable Record-Route	Disable
SAS Block Unregistered Users	Un-Block
Redundant SAS Proxy Set	-1
SAS Inbound Manipulation Mode	None

6. In the 'SAS Proxy Set' field, enter the Proxy Set used for SAS. The SAS Proxy Set must be defined only for 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.

If you define a SAS Proxy Set ID, you must configure the Proxy Set as described in Step 8 below.

7. Click **Submit** to apply your settings.
8. If you defined a SAS Proxy Set ID in Step 6 above, then you must configure the SAS Proxy Set ID:
- Open the Proxy Sets Table page (**Configuration** tab > **VoIP** menu > **Control Networks** > **Proxy Set Table**).
  - From the 'Proxy Set ID' drop-down list, select the required Proxy Set ID.



**Notes:**

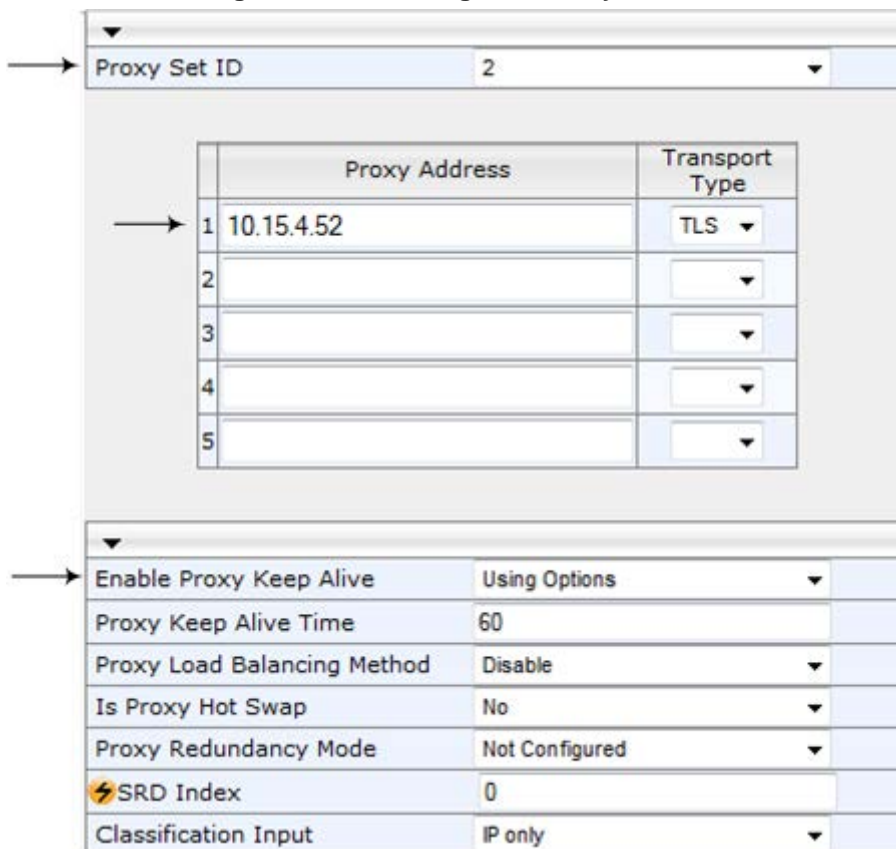
- The selected Proxy Set ID number must be the same as that specified in the 'SAS Proxy Set' field in the 'SAS Configuration' page (see Step 6).
- Do not use Proxy Set ID 0.

- In the 'Proxy Address' field, enter the IP address of the external proxy server.



- d. From the 'Enable Proxy Keep Alive' drop-down list, select **Using Options**. This instructs the device to send SIP OPTIONS messages to the proxy for the keep-alive mechanism.

**Figure 23-3: Defining SAS Proxy Server**



	Proxy Address	Transport Type
1	10.15.4.52	TLS
2		
3		
4		
5		

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

- e. Click **Submit** to apply your settings.

## 23.2 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 266.



**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**.



## 23.3 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 266.



**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**.

## 23.4 Configuring Gateway Application with SAS

If you want to run both the Gateway and SAS applications on the device, the configuration described in this section is required. The configuration steps depend on whether the Gateway application is operating with SAS in outbound mode or SAS in redundant mode.



**Note:** The Gateway application must use the same SAS operation mode as the SIP UAs. For example, if the UAs use the SAS application as a redundant proxy (i.e., SAS redundancy mode), then the Gateway application must do the same.



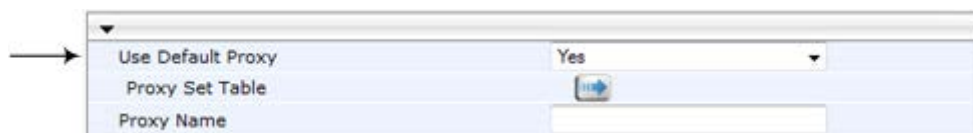
## 23.4.1 Gateway with SAS Outbound Mode

The procedure below describes how to configure the Gateway application with SAS outbound mode.

➤ **To configure Gateway application with SAS outbound mode:**

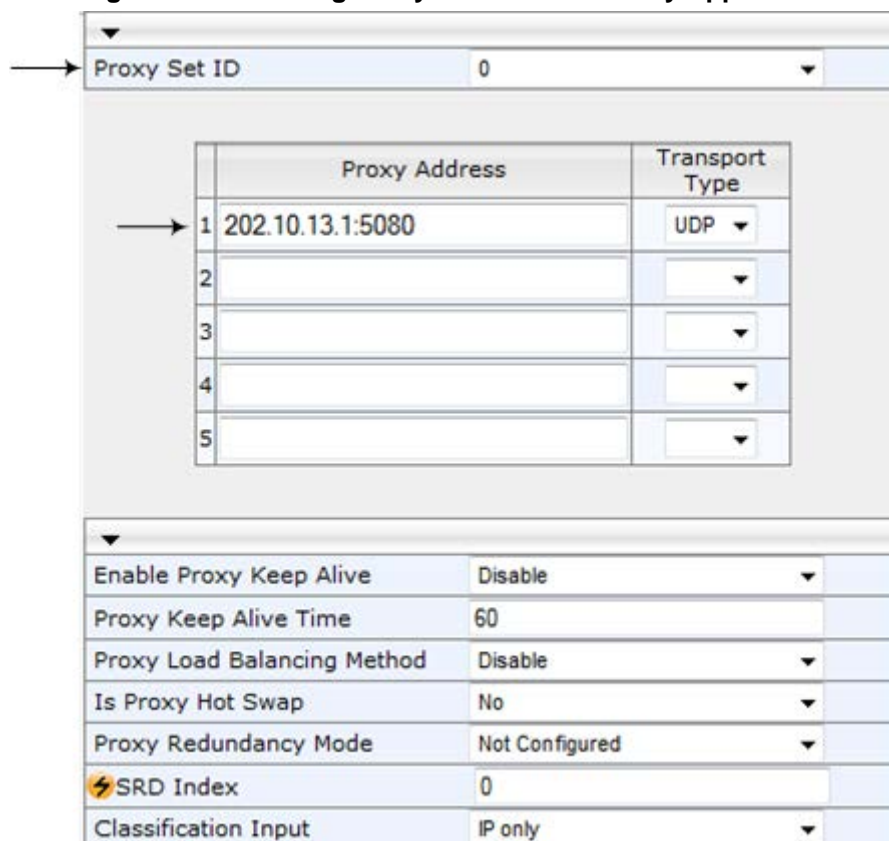
1. Define the proxy server address for the Gateway application:
  - a. Open the Proxy & Registration page (**Configuration** tab > **VoIP** menu > **SIP Definitions** submenu > **Proxy & Registration**).
  - b. From the 'Use Default Proxy' drop-down list, select **Yes**.

**Figure 23-4: Enabling Proxy Server for Gateway Application**



- c. Click **Submit**.
- d. Open the Proxy Sets Table page (**Configuration** tab > **VoIP** menu > **Control Network** submenu > **Proxy Sets** Table).
- e. From the 'Proxy Set ID' drop-down list, select **0**.
- f. In the first 'Proxy Address' field, enter the IP address and port of the device (in the format x.x.x.x:port). This is the port as defined in the 'SAS Local UDP/TCP/TLS Port' field (see "Configuring Common SAS Parameters" on page 266).

**Figure 23-5: Defining Proxy Server for Gateway Application**



	Proxy Address	Transport Type
1	202.10.13.1:5080	UDP
2		
3		
4		
5		

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

- g. Click **Submit**.



2. Disable use of user=phone in SIP URL:
  - 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**. This instructs the Gateway application not to use *user=phone* in the SIP URL and therefore, REGISTER and INVITE messages use SIP URI. (By default, REGISTER messages are sent with *sip uri* and INVITE messages with *tel uri*.)

**Figure 23-6: Disabling user=phone in SIP URL**

SIP General	
NAT IP Address	0.0.0.0
PRACK Mode	Supported
Channel Select Mode	Cyclic Ascending
Enable Early Media	Disable
183 Message Behavior	Progress
Session-Expires Time	0
Minimum Session-Expires	90
Session Expires Method	Re-INVITE
Asserted Identity Mode	Disabled
Fax Signaling Method	No Fax
Detect Fax on Answer Tone	Initiate T.38 on Preamble
SIP Transport Type	UDP
SIP UDP Local Port	5060
SIP TCP Local Port	5060
SIP TLS Local Port	5061
Enable SIPS	Disable
Enable TCP Connection Reuse	Enable
TCP Timeout	0
SIP Destination Port	5060
Use user=phone in SIP URL	No

- c. Click **Submit**.

## 23.4.2 Gateway with SAS Redundant Mode

The procedure below describes how to configure the Gateway application with SAS redundant mode.

### ➤ To configure Gateway application with SAS redundant mode:

1. Define the proxy servers for the Gateway application:
  - a. Open the Proxy & Registration page (**Configuration** tab > **VoIP** menu > **SIP Definitions** submenu > **Proxy & Registration**).
  - b. From the 'Use Default Proxy' drop-down list, select **Yes**.

**Figure 23-7: Enabling Proxy Server for Gateway Application**

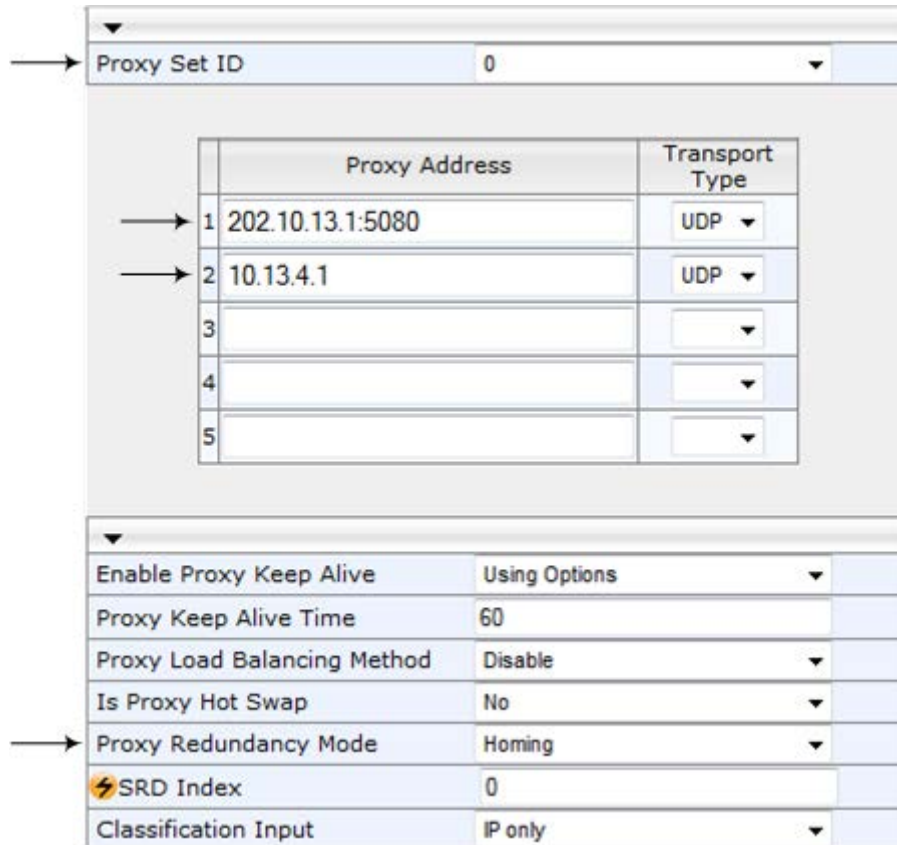
Use Default Proxy	Yes
Proxy Set Table	
Proxy Name	<input type="text"/>

- c. Click **Submit**.
- d. Open the Proxy Sets Table page (**Configuration** tab > **VoIP** menu > **Control Network** submenu > **Proxy Sets Table**).
- e. From the 'Proxy Set ID' drop-down list, select **0**.
- f. In the first 'Proxy Address' field, enter the IP address of the external proxy server.



- g. In the second 'Proxy Address' field, enter the IP address and port of the device (in the format *x.x.x.x:port*). This is the same port as defined in the 'SAS Local UDP/TCP/TLS Port' field (see "Configuring Common SAS Parameters" on page 266).
- h. From the 'Proxy Redundancy Mode' drop-down list, select **Homing**.

**Figure 23-8: Defining Proxy Servers for Gateway Application**



Proxy Set ID: 0

	Proxy Address	Transport Type
1	202.10.13.1:5080	UDP
2	10.13.4.1	UDP
3		
4		
5		

Enable Proxy Keep Alive	Using Options
Proxy Keep Alive Time	60
Proxy Load Balancing Method	Disable
Is Proxy Hot Swap	No
Proxy Redundancy Mode	Homing
SRD Index	0
Classification Input	IP only

- i. Click **Submit**.
2. Disable the use of *user=phone* in the SIP URL:
    - 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**. This instructs the Gateway application not to use *user=phone* in SIP URL and therefore, REGISTER and INVITE messages use SIP URI. (By default, REGISTER messages are sent with *sip uri* and INVITE messages with *tel uri*.)
    - c. Click **Submit**.



## 23.5 Advanced SAS Configuration

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

### 23.5.1 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:

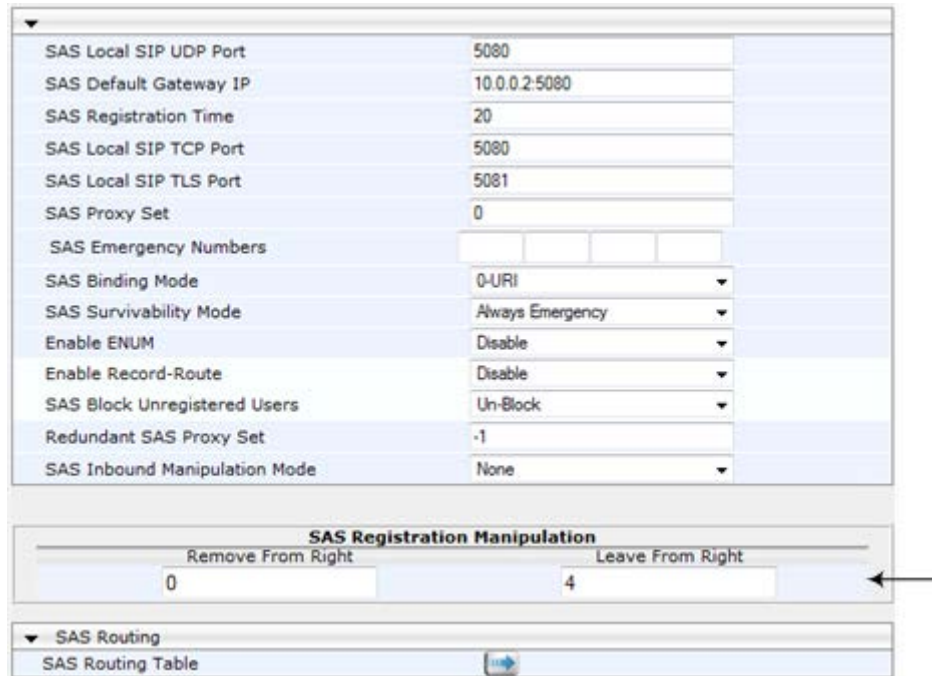
- **AOR:** 976653434@10.33.4.226
- **Associated AOR:** 3434@10.33.4.226 (after manipulation, in which only the four digits from the right of the URI user part are retained)
- **Contact:** 976653434@10.10.10.10

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 23-9: Manipulating User Part in Incoming REGISTER**



SAS Local SIP UDP Port	5080
SAS Default Gateway IP	10.0.0.2:5080
SAS Registration Time	20
SAS Local SIP TCP Port	5080
SAS Local SIP TLS Port	5081
SAS Proxy Set	0
SAS Emergency Numbers	
SAS Binding Mode	0-URI
SAS Survivability Mode	Always Emergency
Enable ENUM	Disable
Enable Record-Route	Disable
SAS Block Unregistered Users	Un-Block
Redundant SAS Proxy Set	-1
SAS Inbound Manipulation Mode	None

**SAS Registration Manipulation**

Remove From Right	Leave From Right
0	4

**SAS Routing**

SAS Routing Table	
-------------------	--

3. Click **Submit**.



**Notes:**

- 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 table ini file parameter, SASRegistrationManipulation.

## 23.5.2 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*.

**Table 23-1: SAS IP to IP Inbound Manipulation Parameters**

Parameter	Description
<b>Matching Characteristics (Rule)</b>	
Additional Manipulation <b>[IPInboundManipulation_IsAdditionalManipulation]</b>	<p>Determines whether additional SIP URI user part manipulation is done for the table entry rule listed directly above it.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> No = (Default) Regular manipulation rule (not done in addition to the rule above it).</li> <li>▪ <b>[1]</b> 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.</li> </ul> <p><b>Note:</b> 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).</p>
Manipulation Purpose <b>[IPInboundManipulation_ManipulationPurpose]</b>	<p>Defines the purpose of the manipulation:</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Normal = (Default) Inbound manipulations affect the routing input and source and/or destination number.</li> <li>▪ <b>[1]</b> Routing input only = Inbound manipulations affect the routing input only, retaining the original source and destination number.</li> <li>▪ <b>[2]</b> Shared Line = Used for the Shared-Line Appearance</li> </ul>



Parameter	Description
	feature. This manipulation is for registration requests to change the destination number of the secondary extension numbers to the primary extension. For more information, see "BroadSoft's Shared Phone Line Call Appearance for SBC Survivability" on page 219.
Source 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 [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). <b>Note:</b> The prefix can be a single digit or a range of digits. For available notations, see "Dialing Plan Notation for Routing and Manipulation" on page 385.
Source 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).
Destination Username Prefix [IPInboundManipulation_DestinationUsernamePrefix]	Defines the prefix of the destination SIP URI user name (usually in the Request-URI). For any prefix, enter the asterisk "*" symbol (default). <b>Note:</b> The prefix can be a single digit or a range of digits. For available notations, see "Dialing Plan Notation for Routing and Manipulation" on page 385.
Destination Host [IPInboundManipulation_DestinationHost]	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 [IPInboundManipulation_RequestType]	Defines the SIP request type to which the manipulation rule is applied. <ul style="list-style-type: none"> <li>[0] All = (Default) All SIP messages.</li> <li>[1] INVITE = All SIP messages except REGISTER and SUBSCRIBE.</li> <li>[2] REGISTER = Only REGISTER messages.</li> <li>[3] SUBSCRIBE = Only SUBSCRIBE messages.</li> <li>[4] INVITE and REGISTER = All SIP messages except SUBSCRIBE.</li> <li>[5] INVITE and SUBSCRIBE = All SIP messages except REGISTER.</li> </ul>
Manipulated URI [IPInboundManipulation_ManipulatedURI]	Determines whether the source or destination SIP URI user part is manipulated. <ul style="list-style-type: none"> <li>[0] Source = (Default) Manipulation is done on the source SIP URI user part.</li> <li>[1] Destination = Manipulation is done on the destination SIP URI user part.</li> </ul>
<b>Operation Rule (Action)</b>	
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".



Parameter	Description
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". <b>Note:</b> If both 'Remove From Right' and 'Leave From Right' parameters are configured, the 'Remove From Right' setting is applied first.
Leave From Right [IPInboundManipulation_LeaveFromRight]	Defines the number of characters that you want retained from the right of the user name. <b>Note:</b> If both 'Remove From Right' and 'Leave From Right' parameters are configured, the 'Remove From Right' setting is applied first.
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 [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".

### 23.5.3 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 page 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.



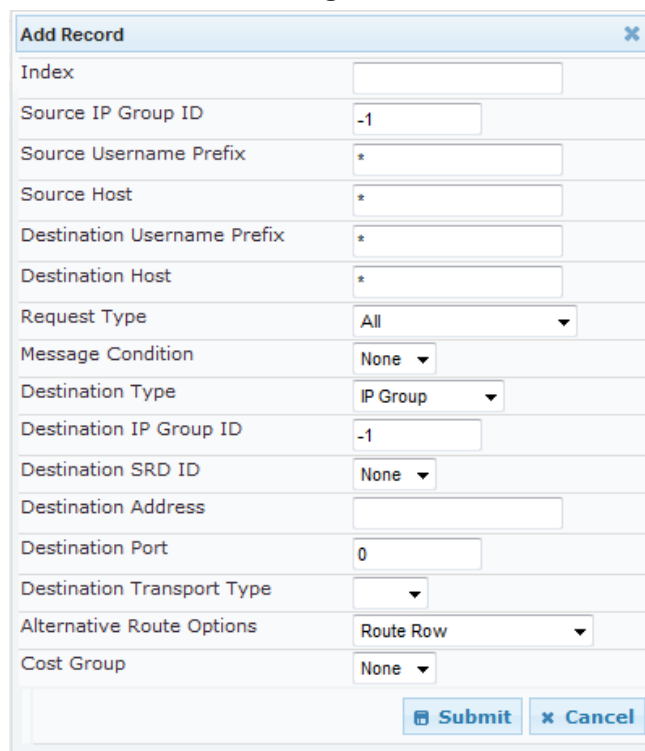
**Note:** The IP-to-IP Routing table can also be configured using the table *ini* file parameter, IP2IPRouting (see "Configuration Parameters Reference" on page 387).



➤ **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 23-10: Add Record Dialog Box of SAS IP2IP Routing Page**



The 'Add Record' dialog box contains the following fields and controls:

- Index: Text input field
- Source IP Group ID: Text input field with value -1
- Source Username Prefix: Text input field with asterisk (\*)
- Source Host: Text input field with asterisk (\*)
- Destination Username Prefix: Text input field with asterisk (\*)
- Destination Host: Text input field with asterisk (\*)
- Request Type: Dropdown menu with 'All' selected
- Message Condition: Dropdown menu with 'None' selected
- Destination Type: Dropdown menu with 'IP Group' selected
- Destination IP Group ID: Text input field with value -1
- Destination SRD ID: Dropdown menu with 'None' selected
- Destination Address: Text input field
- Destination Port: Text input field with value 0
- Destination Transport Type: Dropdown menu
- Alternative Route Options: Dropdown menu with 'Route Row' selected
- Cost Group: Dropdown menu with 'None' selected
- Buttons: 'Submit' and 'Cancel' at the bottom right.

3. Configure the rule according to the table below.
4. Click **Submit** to apply your changes.
5. To save the changes to flash memory, see "Saving Configuration" on page 308.



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

- 'Source IP Group ID'
- 'Destination IP Group ID'
- 'Destination SRD ID'
- 'Alternative Route Options'

**Table 23-2: SAS IP-to-IP Routing Table Parameters**

Parameter	Description
<b>Matching Characteristics</b>	
Source IP Group ID [IP2IPRouting_SrcIPGroupID]	Selects the IP Group from where the IP-to-IP call originated. Typically, the IP Group of an incoming SIP dialog is determined (or classified) using the 'Classification' table (see Configuring Classification Rules on page 230). If not used (i.e., any IP Group), simply leave the field empty.  The default is -1.



Parameter	Description
Source Username Prefix <b>[IP2IPRouting_SrcUsernamePrefix]</b>	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. For example, to denote any prefix, use the asterisk (*) symbol; to denote calls without a user part in the URI, use the \$ sign. For available notations, see "Dialing Plan Notation for Routing and Manipulation" on page 385. The default is * (i.e., any prefix).
Source Host <b>[IP2IPRouting_SrcHost]</b>	Defines the host part of the incoming SIP dialog's source URI (usually the From URI). If this rule is not required, leave the field empty. To denote any host name, use the asterisk (*) symbol (default).
Destination Username Prefix <b>[IP2IPRouting_DestUsernamePrefix]</b>	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. For example, to denote any prefix, use the asterisk (*) symbol; to denote calls without a user part in the URI, use the \$ sign. For available notations, see "Dialing Plan Notation for Routing and Manipulation" on page 385. The default is * (i.e., any prefix).
Destination Host <b>[IP2IPRouting_DestHost]</b>	Defines the host part of the incoming SIP dialog's destination URI (usually the Request-URI). If this rule is not required, leave the field empty. The asterisk (*) symbol (default) can be used to denote any destination host.
Request Type <b>[IP2IPRouting_RequestType]</b>	Defines the SIP dialog request type of the incoming SIP dialog. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> All (default)</li> <li>▪ <b>[1]</b> INVITE</li> <li>▪ <b>[2]</b> REGISTER</li> <li>▪ <b>[3]</b> SUBSCRIBE</li> <li>▪ <b>[4]</b> INVITE and REGISTER</li> <li>▪ <b>[5]</b> INVITE and SUBSCRIBE</li> <li>▪ <b>[6]</b> OPTIONS</li> </ul>
Message Condition <b>[IP2IPRouting_MessageCondition]</b>	Selects a Message Condition rule. To configure Message Condition rules, see "Configuring Condition Rules" on page 235.
ReRoute IP Group ID <b>[IP2IPRouting_ReRouteIPGroupID]</b>	Defines the IP Group that initiated (sent) the SIP redirect response (e.g., 3xx) or REFER message. This field is typically used for re-routing requests (e.g., INVITES) when interworking is required for SIP 3xx redirect responses or REFER messages (for more information, see "Interworking SIP 3xx Redirect Responses" on page 212 and "Interworking SIP REFER Messages" on page 214, respectively). This parameter functions together with the 'Call Trigger' field (see below). The default is -1 (i.e., not configured).
Call Trigger <b>[IP2IPRouting_Trigger]</b>	Defines the reason (i.e, trigger) for re-routing the SIP request: <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Any = (Default) This routing rule is used for all scenarios (re-routes and non-re-routes).</li> <li>▪ <b>[1]</b> 3xx = Re-routes the request if it was triggered as a result of a SIP 3xx response.</li> <li>▪ <b>[2]</b> REFER = Re-routes the INVITE if it was triggered as a result of a REFER request.</li> <li>▪ <b>[3]</b> 3xx or REFER = Applies to options <b>[1]</b> and <b>[2]</b>.</li> <li>▪ <b>[4]</b> Initial only = This routing rule is used for regular requests that</li> </ul>



Parameter	Description
	the device forwards to the destination. This rule is not used for re-routing of requests triggered by the receipt of REFER or 3xx.
<b>Operation Routing Rule</b>	
Destination Type [IP2IPRouting_DestType]	<p>Determines the destination type to which the outgoing SIP dialog is sent.</p> <ul style="list-style-type: none"> <li><b>[0]</b> 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).</li> <li><b>[1]</b> 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'.</li> <li><b>[2]</b> 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.</li> <li><b>[3]</b> 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.</li> <li><b>[4]</b> Hunt Group = Used for call center survivability. For more information, see "Call Survivability for Call Centers" on page 221.</li> <li><b>[5]</b> 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: &lt;destination / called prefix number&gt;,0,&lt;IP destination&gt;</li> </ul> <p>Note that the second parameter "0" is ignored. An example of a configured Dial Plan (# 6) in the Dial Plan file is shown below:</p> <pre>[ 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</pre> <p>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.</p> <ul style="list-style-type: none"> <li><b>[7]</b> LDAP = LDAP-based routing.</li> </ul>
Destination IP Group ID [IP2IPRouting_DestIPGroupID]	<p>Defines the IP Group ID to where you want to route the call. The SIP dialog messages are sent to the IP address defined for the Proxy Set associated with this IP Group. If you select an IP Group, it is unnecessary to configure a destination IP address (in the 'Destination Address' field). However, if both parameters are configured, then the IP Group takes precedence.</p> <p>If the destination IP Group is of USER type, the device searches for a match between the Request-URI (of the received SIP dialog) to an AOR registration record in the device's database. The SIP dialog is then sent to the IP address of the registered contact.</p> <p>The default is -1.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is only relevant if the parameter 'Destination Type' is set to 'IP Group'. However, regardless of the settings of the</li> </ul>



Parameter	Description
	<p>parameter 'Destination Type', the IP Group is still used - only for determining the IP Profile or outgoing SRD. If neither IP Group nor SRD are defined in this table, the destination SRD is determined according to the source SRD associated with the Source IP Group (configured in the IP Group table, see "Configuring IP Groups" on page 164). If this table does not define an IP Group but only an SRD, then the first IP Group associated with this SRD (in the IP Group table) is used.</p> <ul style="list-style-type: none"> <li>▪ If the selected destination IP Group ID is type SERVER, the request is routed according to the IP Group addresses.</li> <li>▪ If the selected destination IP Group ID is type USER, the request is routed according to the IP Group specific database (i.e., only to registered users of the selected database).</li> <li>▪ If the selected destination IP Group ID is ANY USER ([<b>-2</b>]), the request is routed according to the general database (i.e., any matching registered user).</li> </ul>
Destination SRD ID [IP2IPRouting_DestSRDID]	<p>Defines the SRD ID. The default is None.</p> <p><b>Note:</b> The destination IP Group must belong to the destination SRD if both are configured in this table.</p>
Destination Address [IP2IPRouting_DestAddresses]	<p>Defines the destination IP address (or domain name, e.g., domain.com) to where the call is sent.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This parameter is applicable only if the parameter 'Destination Type' is set to 'Dest Address' [<b>1</b>].</li> <li>▪ When using domain names, enter a DNS server IP address or alternatively, define these names in the 'Internal DNS Table' (see "Configuring the Internal SRV Table" on page 106).</li> </ul>
Destination Port [IP2IPRouting_DestPort]	<p>Defines the destination port to where the call is sent.</p>
Destination Transport Type [IP2IPRouting_DestTransportType]	<p>Defines the transport layer type for sending the call:</p> <ul style="list-style-type: none"> <li>▪ [<b>-1</b>] Not Configured (default)</li> <li>▪ [<b>0</b>] UDP</li> <li>▪ [<b>1</b>] TCP</li> <li>▪ [<b>2</b>] TLS</li> </ul> <p><b>Note:</b> When this parameter is set to -1, the transport type is determined by the parameter SIPTransportType.</p>
Alternative Route Options [IP2IPRouting_AltRouteOptions]	<p>Determines whether this routing rule is the main routing rule or an alternative routing rule (to the rule defined directly above it in the table).</p> <ul style="list-style-type: none"> <li>▪ [<b>0</b>] Route Row (default) = Main routing rule - the device first attempts to route the call to this route if the incoming SIP dialog's input characteristics matches this rule.</li> <li>▪ [<b>1</b>] Alt Route Ignore Inputs = If the call cannot be routed to the main route (Route Row), the call is routed to this alternative route regardless of the incoming SIP dialog's input characteristics.</li> <li>▪ [<b>2</b>] Alt Route Consider Inputs = If the call cannot be routed to the main route (Route Row), the call is routed to this alternative route only if the incoming SIP dialog matches this routing rule's input characteristics.</li> </ul>



Parameter	Description
	<p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>The alternative routing entry (<b>[1]</b> or <b>[2]</b>) must be defined in the next consecutive table entry index to the Route Row entry (i.e., directly below it). For example, if Index 4 is configured as a Route Row, Index 5 must be configured as the alternative route.</li> <li>For IP-to-IP alternative routing, configure alternative routing reasons upon receipt of 4xx, 5xx, and 6xx SIP responses (see <a href="#">Configuring Alternative Routing Reasons</a> on page 243). However, if no response, ICMP, or a SIP 408 response is received, the device attempts to use the alternative route even if no entries are configured in the 'SBC Alternative Routing Reasons' table.</li> <li>Multiple alternative route entries can be configured (e.g., Index 1 is the main route - Route Row - and indices 2 through 4 are configured as alternative routes).</li> </ul>
Cost Group <b>[IP2IPRouting_CostGroup]</b>	<p>Assigns a Cost Group to the routing rule for determining the cost of the call. To configure Cost Groups, see "Configuring Cost Groups" on page 153.</p> <p>By default, no Cost Group is assigned to the rule.</p>

## 23.5.4 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.

## 23.5.5 Configuring SAS Emergency Calls

You can configure SAS to route emergency calls (such as 911 in North America) directly to the PSTN through its . 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 263). 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).





**Note:** The port of the device is defined in the 'SIP UDP/TCP/TLS Local Port' field in the SIP General Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **General Parameters**).

3. In the 'SAS Emergency Numbers' field, enter an emergency number in each field box.

**Figure 23-11: Configuring SAS Emergency Numbers**

SAS Local SIP UDP Port	5080
SAS Default Gateway IP	10.13.4.12
SAS Registration Time	20
SAS Local SIP TCP Port	5080
SAS Local SIP TLS Port	5081
SAS Proxy Set	0
SAS Emergency Numbers	911
SAS Binding Mode	1-User Part Only
SAS Survivability Mode	Always Emergency
Enable ENUM	Disable
Enable Record-Route	Disable
SAS Block Unregistered Users	Block
Redundant SAS Proxy Set	-1
SAS Inbound Manipulation Mode	None

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

### 23.5.6 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.



## 23.5.7 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.

## 23.5.8 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`:

- **[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.

## 23.6 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, as described in "Viewing Registered Users" on page 345.



**Note:** You can increase the maximum number of registered SAS users, by implementing the SAS Cascading feature, as described in "SAS Cascading" on page 285.



## 24 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:

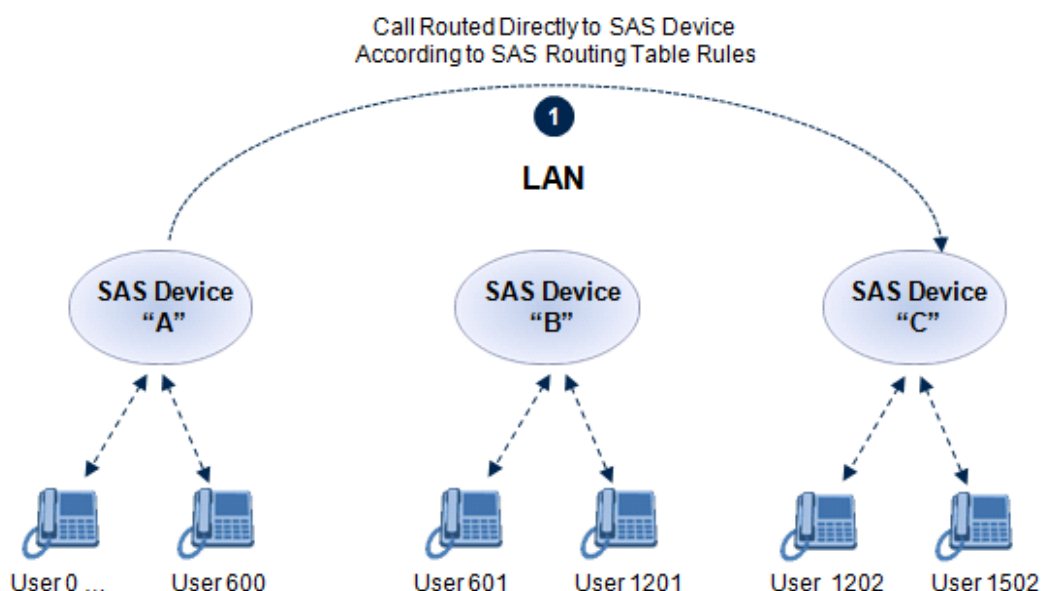
- **SAS Routing Table:** If users can be identified with unique phone extension numbers, then the SAS Routing table is used to configure SAS Cascading. This SAS Cascading method routes calls directly to the SAS Gateway (defined by IP address) to which the called SAS user is registered.

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 263). For a description on the SAS Routing table, see "SAS Routing Based on IP-to-IP Routing Table" on page 277.

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 24-1: SAS Cascading Using SAS Routing Table - Example**

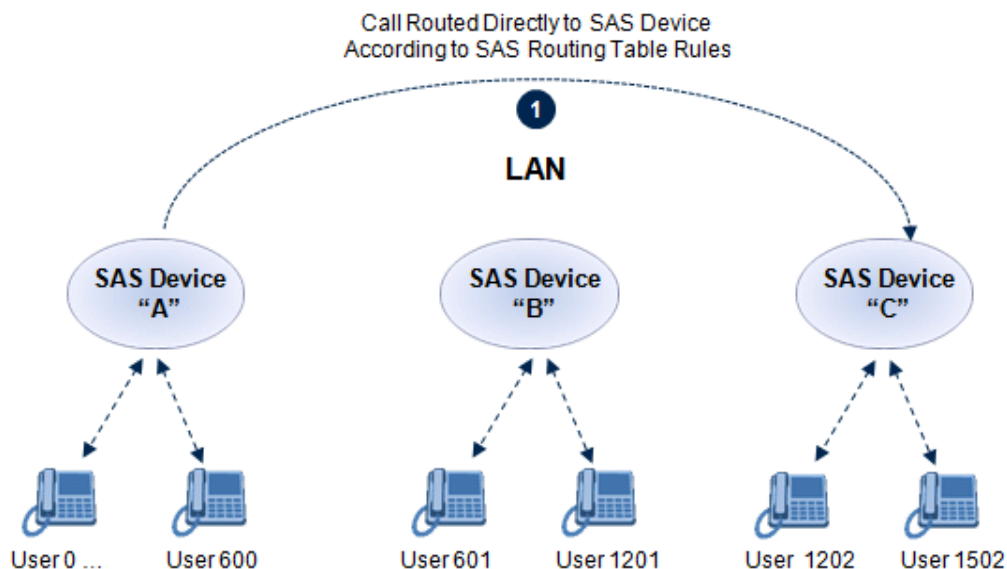


- SAS Redundancy mode:** If users cannot be distinguished (i.e., associated to a specific SAS gateway), then the SAS Redundancy feature is used to configure SAS Cascading. This mode routes the call in a loop fashion, from one SAS gateway to the next, until the user is located. Each SAS gateway serves 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 24-2: SAS Cascading Using SAS Redundancy Mode - Example**





# Part VII

## High Availability System





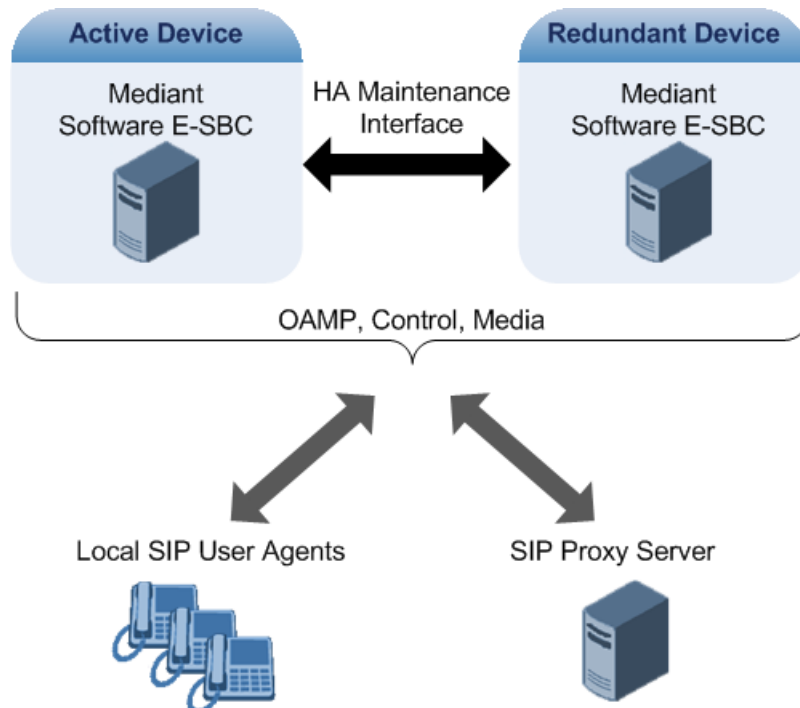


## 25 Overview

The device's High Availability (HA) feature provides 1+1 system redundancy using two Mediant Software E-SBC devices. If failure occurs in the active device, a switchover occurs to the redundant device which takes over the call handling process. Thus the continuity of call services is ensured. All active calls (signaling and media) are maintained upon switchover.

The figure below illustrates the Active-Redundant HA devices under normal operation. Communication between the two devices is through a Maintenance interface, having a unique IP address for each device. The devices have identical software and configuration including network interfaces (i.e., OAMP, Control, and Media), and have identical local-port cabling of these interfaces.

**Figure 3: Two Devices in HA State**



### 25.1 Connectivity and Synchronization between Devices

In HA mode, the Ethernet connectivity between the two devices is through a special LAN interface on each device, referred to as the *Maintenance* interface. Each device has its own Maintenance interface with a unique address, and each device knows the Maintenance address of the other. The Maintenance interface can use a dedicated Ethernet port group or share the same Ethernet port group with the other network interface types (i.e., OAMP, Media, and Control).

When only one of the devices is operational it is in HA stand-alone state. This means that the device has no connectivity to the second device. When the second device is powered up, it recognizes the active device through the Maintenance network and acquires the HA redundant state. It then begins synchronizing for HA with the active device through the Maintenance network. During synchronization, the active device sends the redundant device its current configuration settings, including auxiliary files. The active device also sends its software file (.cmp) if the redundant device is running a different software version. Once loaded to the redundant device, the redundant device reboots to apply the new configuration and/or software.



Thus, under normal operation, one of the devices is in active state while the other is in redundant state, where both devices share the same configuration and software. Any subsequent configuration update or software upgrade on the active device is also done on the redundant device.

In the active device, all logical interfaces (i.e., Media, Control, OAMP, and Maintenance) are active. In the redundant device, only the Maintenance interface is active, which is used for connectivity to the active device. Therefore, management is done only through the active device. Upon a failure in the active device, the redundant device becomes active and activates all its logical interfaces exactly as was used on the active device.

## 25.2 Device Switchover upon Failure

When a failure occurs in the active device, a switchover occurs to the redundant device making it the new active device. Whether a switchover is later done back to the repaired failed device, depends on whether you have enabled the Revertive mode:

- **Revertive mode enabled:** The Revertive mode specifies one of the device's as the "preferred" device between the two devices. This is done by assigning a priority level to each device (1 to 10, where 1 is the lowest). Whenever the device with higher priority recovers from a failure, it first becomes the redundant device but then initiates a switchover to become the active device once again; otherwise, after recovery, it becomes the redundant device and remains as redundant. If you change the priority level of the redundant device to one that is higher than the active device and then reset the redundant device, a switchover occurs to the redundant device making it the active device and the "preferred" device. If both devices are configured with the same priority level, then Revertive mode is irrelevant.
- **Revertive mode disabled:** A switchover is done only upon failure of the currently active device.

Failure detection by the devices is done by the constant keep-alive messages they send between themselves to verify connectivity. Upon detection of a failure in one of the devices, the following occurs:

- **Failure in active device:** The redundant device initiates a switchover. The failed device resets and the previously redundant device becomes the active device in stand-alone mode. If at a later stage this newly active device detects that the failed device has been repaired, the system returns to HA mode. If Revertive mode is enabled and the originally active device was configured with a higher priority, a switchover occurs to this device; otherwise, if it was configured with a lower priority (or Revertive mode was disabled), the repaired device is initialized as the redundant device.
- **Failure in redundant device:** The active device moves itself into stand-alone mode until the redundant device is returned to operation. If the failure in the redundant device is repaired after reset, it's initialized as the redundant device once again and the system returns to HA mode.

Connectivity failure triggering a switchover can include, for example, one of the following:

- **Loss of physical (link) connectivity:** If one or more physical network groups (i.e., Ethernet port pair) used for one or more network interfaces of the active device disconnects (i.e., no link) and these physical network groups are connected OK on the redundant device, then a switchover occurs to the redundant device.
- **Loss of network (logical) connectivity:** No network connectivity, verified by keep-alive packets between the devices. This applies only to the Maintenance interface.



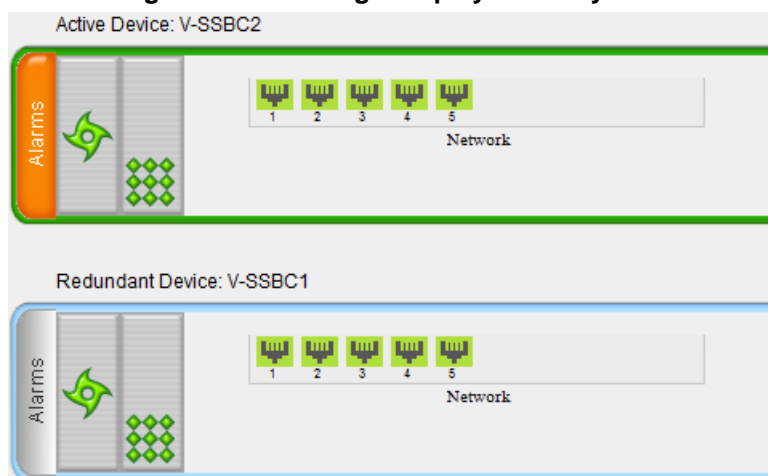
**Note:** Switchover triggered by loss of physical connectivity in one or more Ethernet port-group is not done if the active device has been set to a Revertive priority level of 10. In such a scenario, the device remains active despite the loss of connectivity in one or more of its Ethernet port groups.



## 25.3 HA Status

The device's Web Home page displays the status of the HA system. The Home page provides a graphical display of both the active and redundant devices:

**Figure 4: Home Page Display of HA System**



- Active device:
  - Color border: The active device is surrounded by a green border.
  - Title: The default title of the device is Active Device: "Device 1".
- Redundant device:
  - Color border: The redundant device is surrounded by a blue border.
  - Title: The default title of the device is Redundant Device: "Device 2".

The title of each device can be configured as described below:

➤ **To define a name for the device:**

1. Open the HA Settings page (**Configuration** tab > **System** menu > **HA Settings**).
2. In the 'HA Device Name' field, enter a name for the device, and then click **Submit**.

The Home page also displays the HA operational status of the device to which you are currently logged in. This is displayed in the 'High Availability' field under the General Information pane:

- "Not Operational": HA is not configured or the device is not installed with the HA Software License Key
- "Synchronizing": Redundant device is synchronizing with Active device
- "Operational": The device is in HA mode
- "Stand Alone": HA is configured but the Redundant device is missing and HA is currently unavailable
- "Not Available": HA is not configured correctly (error)



## Reader's Notes



## 26 HA Configuration

This section describes the configuration of the HA system.

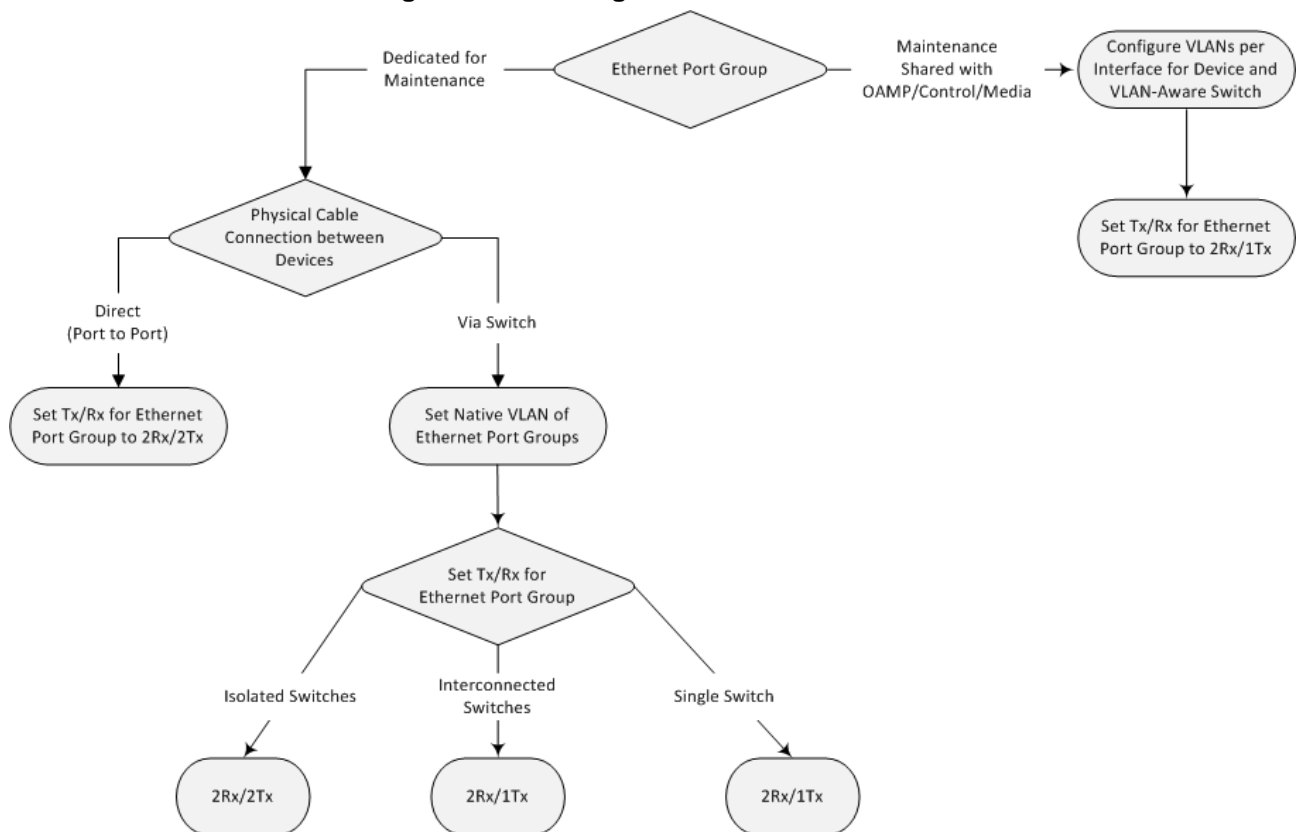
### 26.1 Initial HA Configuration

By default, HA is disabled on the device. When a device is loaded with valid HA configuration and it is the first device to be loaded, it becomes the active device. The second device that is loaded with HA configuration becomes the redundant (standby) device.

#### 26.1.1 Network Topology Types

The initial configuration of HA depends on how you want to deploy your HA system in the network. The flowchart below shows the different configuration setups according to network topology:

**Figure 5: HA Configuration Flowchart**



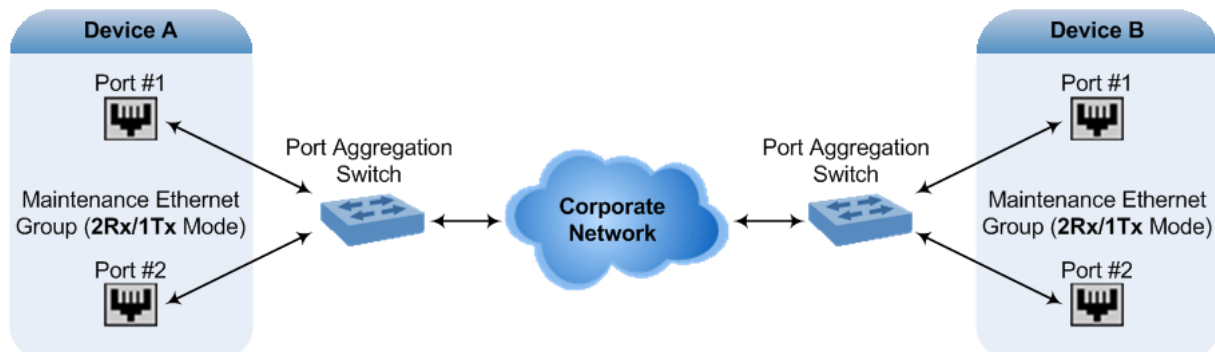
##### 26.1.1.1 Tx/Rx Port Settings

The required transmit (TX) / receive (Rx) mode that you need to configure for the port pair in the Ethernet Port Group used by the Maintenance interface depends on whether this Ethernet Port Group is shared or not with the other network interfaces (i.e., OAMP, and/or Control, and/or Media):



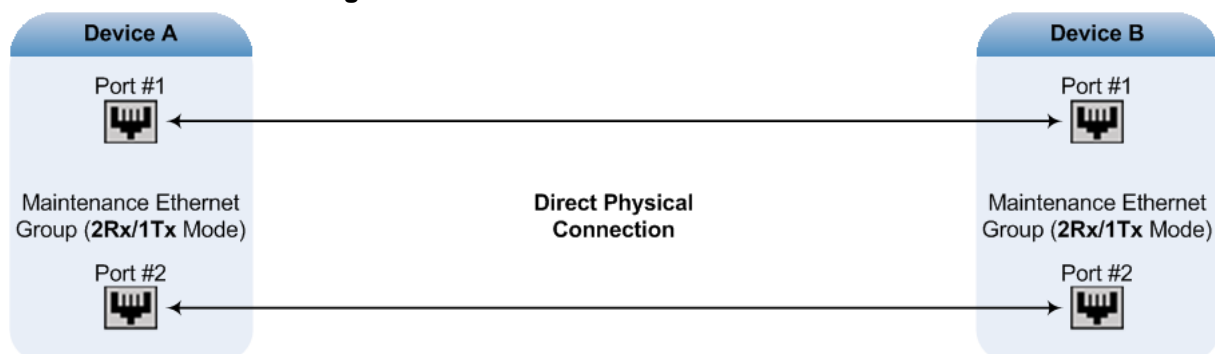
- For Geographical HA (both units are located far from each other), **2Rx/1Tx** port mode connected to a port aggregation switch is the recommended option:

**Figure 26-6: Rx/Tx Mode for Geographical HA**



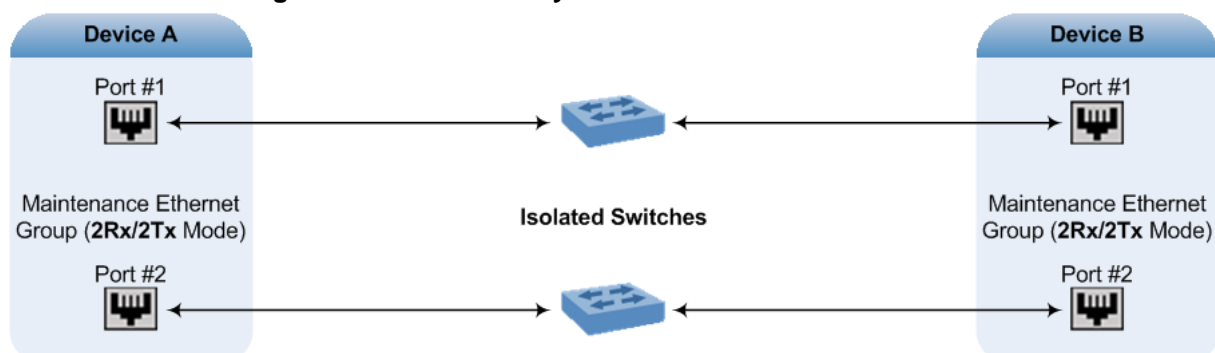
- If the Maintenance ports of both devices are connected directly to each other without intermediation of switches, configure the mode to **2RX/1TX**:

**Figure 26-7: Rx/Tx Mode for Direct Connection**



- If the two devices are connected through two (or more) isolated LAN switches (i.e., packets from one switch cannot traverse the second switch), configure the mode to **2RX/2TX**:

**Figure 26-8: Redundancy Mode for Two Isolated Switches**



**Notes:**



- When two LAN switches are used, the LAN switches must be in the same subnet (i.e., broadcast domain).
- To configure Tx/Rx modes of the Ethernet ports, see "Configuring Tx/Rx for Ethernet Port-Pair Groups" on page 88.



## 26.1.2 Configuring the HA Devices

This section describes how to initially configure the two devices comprising the HA system. This configuration is done in the following chronological order:

1. Configuring the first device for HA - see 'Step 1: Configure the First Device' on page 295
2. Configuring the second device for HA - see 'Step 2: Configure the Second Device' on page 297
3. Activating HA on the devices - see 'Step 3: Initialize HA on the Devices' on page 298



### Notes:

- The physical connections of the first and second devices to the network (i.e., Maintenance interface and OAMP, Control and Media interfaces) **must be identical**. This also means that the two devices must also use the same Ethernet Port Groups and the port numbers belonging to these Ethernet Port Groups. For example, if the first device uses Ethernet Port Group 1 (with ports 1 and 2), the second device must also use Ethernet Port Group 1 (with ports 1 and 2).
- Before configuring HA, determine the required network topology, as described in 'Network Topology Types' on page 293.
- For HA support, ensure that both devices are installed with a Software Feature Key that includes the HA feature.
- It is recommended to avoid using Spanning Tree Protocol (STP) on the Maintenance interface; the Ethernet connectivity of the Maintenance interface between the two devices should be constantly reliable without any disturbances.

### 26.1.2.1 Step 1: Configure the First Device

The first stage is to configure the first device for HA, as described in the procedure below:



**Note:** During this stage, ensure that the second device is powered off or disconnected from the network.

#### ➤ To configure the first device for HA:

1. Configure the network interfaces, including the default OAMP interface:
  - d. If you are already connected to the SBC via keyboard and monitor, change the OAMP parameters to suite your networking scheme, using CLI (refer to the *Installation Manual*).
  - e. Connect to the SBC's Web interface with the newly assigned OAMP IP address.
  - f. Open the Multiple Interface table (**Configuration** tab > **VoIP** menu > **Network** > **IP Settings**).
  - g. Configure the Control and Media network interfaces, as required.
  - h. Add the HA Maintenance interface (i.e., the **MAINTENANCE** Application Type).



### Notes:

- The used Ethernet Port Group, selected in the 'Underlying Interface' field, depends on the following:
  - ✓ **Dedicated Ethernet Port Group for Maintenance interface:** Use a different Ethernet Port Group for the Maintenance interface than for the other network interfaces.
  - ✓ **Shared Ethernet Port Group for Maintenance and OAMP/Control/Media interfaces:** Use the same Ethernet Port Group for all these interfaces.
- If you are using an Ethernet Port Group that is shared between the Maintenance interface and the other network interfaces, assign them different VLANs. Ensure that you also configure these VLANs on the third-party, VLAN-aware switch to which the Ethernet Port Group is connected.



The Multiple Interface table below shows an example where the Maintenance interface is assigned to Ethernet Port Group 2 ("GROUP\_2") and the other interfaces to Ethernet Port Group 1 ("GROUP\_1"):

**Figure 9: Multiple Interface Table with Maintenance Interface**

Index	Application Type	Interface Mode	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name	Primary DNS Server IP Address	Secondary DNS Server IP Address	Underlying
0	OAMP + Media + Control	IPv4 Manual	10.8.244.80	16	10.8.0.1	1	Voice	0.0.0.0	0.0.0.0	GROUP_1
1	MAINTENANCE	IPv4 Manual	10.3.0.51	16	10.3.0.1	2	Unknown	0.0.0.0	0.0.0.0	GROUP_2

2. If the Maintenance interface uses a dedicated Ethernet Port Group and the connection is through a switch, the packets of both interfaces should generally be untagged. In such a scenario, set the Native VLAN ID of each Ethernet Port Group so that it is the same as the VLAN ID set for each interface assigned to that Ethernet Port Group. The Native VLAN ID is configured in the Physical Ports Settings page (see 'Configuring Physical Ethernet Ports' on page 87). The figure below shows an example whereby the Native VLAN IDs of the Ethernet Port Groups are set to the same VLAN IDs of the interfaces using these Ethernet Port Groups:

**Figure 10: Native VLAN for Ethernet Port Groups of Maintenance and Other Interfaces**

OAMP, Control, Media

Index	Port	Mode	Native Vlan	Speed&Duplex	Description	Group Member	Group Status
1	GE_1	Enable	1	Auto Negotiation	User Port #0	GROUP_1	Active
2	GE_2	Enable	1	Auto Negotiation	User Port #1	GROUP_1	Redundant
3	GE_3	Enable	2	Auto Negotiation	User Port #2	GROUP_2	Active
4	GE_4	Enable	2	Auto Negotiation	User Port #3	GROUP_2	Redundant

Maintenance

3. Set the Ethernet port Tx / Rx mode of the Ethernet Port Group used by the Maintenance interface. This is configured in the Ethernet Group Settings page (see "Configuring Tx/Rx for Ethernet Port-Pair Groups" on page 88). The port mode depends on the type of Maintenance connection between the devices, as described in 'Tx/Rx Port Settings' on page 293.
4. Configure the HA parameters in the HA Settings page (**Configuration** tab > **System** menu > **HA Settings**):

**Figure 11: HA Settings Page**

HA Settings	
HA Remote Address	10.31.4.61
HA Revertive	Disable
HA Priority	5
Redundant HA Priority	5



- a. In the 'HA Remote Address' field, enter the Maintenance IP address of the **second** device.
  - b. (Optional) Enable the Revertive mode by setting the 'HA Revertive' parameter to **Enable** and then setting the priority level of this device in the 'HA Priority' field.
5. Burn the configuration to flash **without** a reset.
6. Power down the device.
7. Continue to 'Step 2: Configure the Second Device' on page 297 for configuring the second device.

### 26.1.2.2 Step 2: Configure the Second Device

Once you have configured the first device for HA, you can configure the second device for HA. As the configuration of the second device is similar to the first device, the procedure below briefly describes each procedural step. For detailed configuration such as the path to the Web configuration pages, refer to the section on configuring the first device ('Step 1: Configure the First Device' on page 295).



**Note:** During this stage, ensure that the first device is powered off or disconnected from the network.

➤ **To configure the second device for HA:**

1. Connect to the device in the same way as you did with the first device.
2. Configure the **same** OAMP, Media, and Control interfaces as you configured for the first device.
3. Configure a Maintenance interface for this device. The IP address must be different to that configured for the Maintenance interface of the first device. However, the Maintenance interfaces of the devices must be in the same subnet.
4. Configure the **same** Native VLAN IDs of the Ethernet Port Groups and VLAN IDs of the network interfaces as you configured for the first device.
5. Configure the **same** Ethernet port Tx / Rx mode of the Ethernet Port Group used by the Maintenance interface as you configured for the first device.
6. Configure the HA parameters in the HA Settings page (**Configuration** tab > **System** menu > **HA Settings**):
  - a. In the 'HA Remote Address' field, enter the Maintenance IP address of the **first** device.
  - b. (Optional) Enable the Revertive mode by setting the 'HA Revertive' parameter to **Enable** and then setting the priority level of this second device in the 'Redundant HA Priority' field.
7. Burn the configuration to flash **without** a reset.
8. Power down the device.
9. Continue to 'Step 3: Initialize HA on the Devices' on page 298 for completing the HA configuration.



### 26.1.2.3 Step 3: Initialize HA on the Devices

Once you have configured both devices for HA as described in the previous sections, follow the procedure below to complete and initialize HA so that the devices become operational in HA. This last stage applies to both devices.

➤ **To initialize the devices for HA:**

1. Cable the devices to the network.



**Note:** You must connect both ports (two) in the Ethernet Port Group of the Maintenance interface to the network (i.e., two network cables are used). This provides 1+1 Maintenance port redundancy.

2. Power up the devices; the redundant device synchronizes with the active device and updates its configuration according to the active device. The synchronization status is indicated as follows:

- Active device: The Web interface's Home page displays the HA status as "Synchronizing".

When synchronization completes successfully, the redundant device resets to apply the received configuration and software.

When both devices become operational in HA, the HA status is indicated as follows:

- Both devices: The Web interface's Home page displays the HA status as "Operational".

3. Access the active device with its OAMP IP address and configure the device as required. For information on configuration done after HA is operational, see 'Configuration while HA State is Operational' on page 298.

## 26.2 Configuration while HA is Operational

When the devices are operating in HA state, subsequent configuration is as follows:

- All configuration, including HA is done on the active device **only**.
- Non-HA configuration on the active device is automatically updated on the redundant device (through the Maintenance interface).
- HA-related configuration on the active device is automatically updated on the redundant device:
  - Maintenance interface:
    - ◆ Modified Maintenance interface address of the active device: this address is set as the new 'HA Remote Address' value on the redundant device.
    - ◆ Modified 'HA Remote Address' value on the active device: this address is set as the new Maintenance interface address on the redundant device. This requires a device reset.
    - ◆ Modifications on all other Maintenance interface parameters (e.g., Default Gateway and VLAN ID): updated to the Maintenance interface on the redundant device.
  - 'HA Revertive' mode (this requires a device reset).



- 'HA Priority' parameter is set for the active device.
- Modified 'Redundant HA Priority' value is set for the redundant device. This requires a device reset.



**Note:** If the HA system is already in Revertive mode and you want to change the priority of the device, to ensure that system service is maintained and traffic is not disrupted, it is recommended to set the higher priority to the redundant device and then reset it. After it synchronizes with the active device, it initiates a switchover and becomes the new active device (the former active device resets and becomes the new redundant device).

## 26.3 Configuring Firewall Allowed Rules

If you add firewall rules in the Firewall Settings page (see "Configuring Firewall Settings" on page 115) that block specified traffic, you also need to add rules that ensure traffic related to the HA feature is allowed. These allowed HA rules include the following:

- Keep-alive packets between the HA devices (e.g., rules #1 and #2 in the figure below).
- HA control and data packets between the HA devices (e.g., rules #3 and #4 in the figure below).
- HA control and data packets between the HA devices after switchover (e.g., rules #5 and #6 in the figure below). These rules are the same as rules #3 and #4 respectively, but are required as the TCP source and destination port IDs are not symmetric.
- HTTP protocol for file transferring (e.g., Rule #7 in the figure below).
- HTTP protocol for file transferring after switchover (e.g., Rule #8 - same as Rule #7 - in the figure below).

The figure below displays an example of the required firewall rules. In this example, 10.31.4.61 is the Maintenance interface of the redundant device and 10.31.4.62 is the Maintenance interface of the active device. "HA\_IF" is the name of the Maintenance interface.

**Figure 12: Allowed Firewall Rules for HA**

Edit Rule	Rule Status	Source IP	Source Port	Prefix Length	Local Port Range	Protocol	Use Specific Interface	Interface Name	Packet Size	Byte rate	Burst Bytes	Action Upon Match	Match Count
0	<input type="radio"/> Active	0.0.0.0	0	0	80-80	tcp	Enable	O+M+C	0	0	0	ALLOW	248
1	<input type="radio"/> Active	10.31.4.61	669	32	669-669	udp	Enable	HA_IF	0	0	0	ALLOW	921
2	<input type="radio"/> Active	10.31.4.62	669	32	669-669	udp	Enable	HA_IF	0	0	0	ALLOW	0
3	<input type="radio"/> Active	10.31.4.61	0	32	2442-2442	TCP	Enable	HA_IF	0	0	0	ALLOW	57
4	<input type="radio"/> Active	10.31.4.62	2442	32	0-65535	TCP	Enable	HA_IF	0	0	0	ALLOW	0
5	<input type="radio"/> Active	10.31.4.61	2442	32	0-65535	TCP	Enable	HA_IF	0	0	0	ALLOW	0
6	<input type="radio"/> Active	10.31.4.62	0	32	2442-2442	TCP	Enable	HA_IF	0	0	0	ALLOW	0
7	<input type="radio"/> Active	10.31.4.61	80	32	0-65535	TCP	Enable	HA_IF	0	0	0	ALLOW	0
8	<input type="radio"/> Active	10.31.4.62	80	32	0-65535	TCP	Enable	HA_IF	0	0	0	ALLOW	0
9	<input checked="" type="radio"/> Not Active	0.0.0.0	0	0	65535	Any	Disable	None	0	0	0	Block	0



## Reader's Notes



## 27 HA Maintenance

This section describes HA maintenance procedures.

### 27.1 Maintenance of Redundant Device

The only interface that is operational on the redundant device is the Maintenance interface. For maintenance, there are several protocols available for this interface (unlike the active device which uses the logical OAMP / management interface for these protocols):

- **Syslog:** To receive Syslog messages from the redundant device, ensure that there is a valid VLAN and route configured from the maintenance network to where the Syslog server is located on the network.
- **Telnet:** A Telnet server is always available on the redundant device (even if disabled by configuration).

### 27.2 Replacing a Failed Device

If you need to replace a non-functional device with a new one, the new device must be configured exactly as the second device, as described in 'Configuring the HA Devices' on page 295.

### 27.3 Forcing a Switchover

If required, you can force a switchover between active and redundant SBCs. For more information, see "High Availability Maintenance" on page 309.

### 27.4 Software Upgrade

The following types of software upgrades are available on the HA system:

- **Software Upgrade with Device Reset:** Both active and redundant devices burn and reboot with the new software version. This method is quick and simple, but it disrupts traffic (i.e., traffic affecting).
- **Hitless Software Upgrade:** This method maintains service (i.e., not traffic affecting) and is as follows:
  - a. The redundant device burns and resets with the new software version.
  - b. A switchover is done between the active and redundant devices, whereby the redundant device becomes the active one.
  - c. The previously active device burns and resets with the new software version.
  - d. The previously active device switches over to become the active device.

For more information on upgrading the software, see "Software Upgrade Wizard" on page 320.



## Reader's Notes



# Part VIII

## Maintenance







## 28 Basic Maintenance

The Maintenance Actions page allows you to perform the following:

- Reset the device - see "Resetting the Device" on page 305
- Lock and unlock the device - see "Locking and Unlocking the Device" on page 307
- Save configuration to the device's flash memory - see "Saving Configuration" on page 308

➤ To access the Maintenance Actions page, do one of the following:

- On the toolbar, click the **Device Actions** button, and then from the drop-down menu, choose **Reset**.
- On the Navigation bar, click the **Maintenance** tab, and then in the Navigation tree, select the **Maintenance** menu and choose **Maintenance Actions**.

Figure 28-1: Maintenance Actions Page

▼ Reset Configuration	
Reset Board	<input type="button" value="Reset"/>
Burn To FLASH	Yes <input type="button" value="v"/>
Graceful Option	No <input type="button" value="v"/>
▼ LOCK / UNLOCK	
Lock	<input type="button" value="LOCK"/>
Graceful Option	No <input type="button" value="v"/>
Current Admin State	UNLOCKED
▼ Save Configuration	
Burn To FLASH	<input type="button" value="BURN"/>

### 28.1 Resetting the Device

The Maintenance Actions page allows you to remotely reset the device. In addition, before resetting the device, you can choose the following options:

- Save the device's current configuration to the device's flash memory (non-volatile).
- Perform a graceful shutdown, whereby device reset starts only after a user-defined time (i.e., timeout) or after no more active traffic exists (the earliest thereof).



#### Notes:

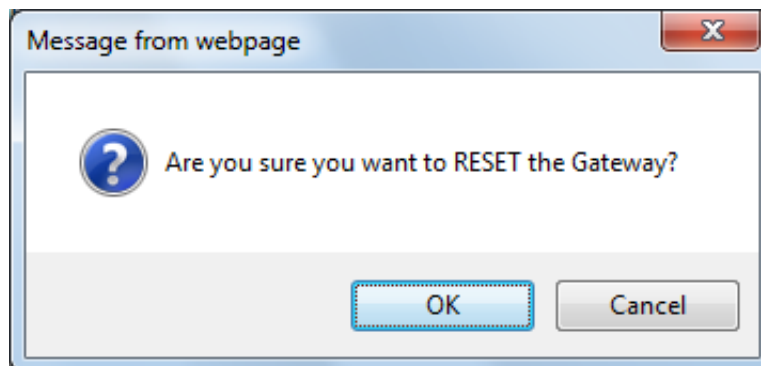
- Throughout the Web interface, parameters displayed with a lightning ⚡ symbol are not applied on-the-fly and require that you reset the device for them to take effect.
- When you modify parameters that require a device reset, once you click the **Submit** button in the relevant page, the toolbar displays "Reset" (see "Toolbar Description" on page 32) to indicate that a device reset is required.
- After you reset the device, the Web GUI is displayed in Basic view (see "Displaying Navigation Tree in Basic and Full View" on page 33).



➤ **To reset the device:**

1. Open the Maintenance Actions page (see "Basic Maintenance" on page 305).
2. Under the 'Reset Configuration' group, from the 'Burn To FLASH' drop-down list, select one of the following options:
  - **Yes:** The device's current configuration is saved (*burned*) to the flash memory prior to reset (default).
  - **No:** Resets the device without saving the current configuration to flash (discards all unsaved modifications).
3. Under the 'Reset Configuration' group, from the 'Graceful Option' drop-down list, select one of the following options:
  - **Yes:** Reset starts only after the user-defined time in the 'Shutdown Timeout' field (see Step 4) expires or after no more active traffic exists (the earliest thereof). In addition, no new traffic is accepted.
  - **No:** Reset starts regardless of traffic, and any existing traffic is terminated at once.
4. In the 'Shutdown Timeout' field (relevant only if the 'Graceful Option' in the previous step is set to **Yes**), enter the time after which the device resets. Note that if no traffic exists and the time has not yet expired, the device resets.
5. Click the **Reset** button; a confirmation message box appears, requesting you to confirm.

**Figure 28-2: Reset Confirmation Message Box**



6. Click **OK** to confirm device reset; if the parameter 'Graceful Option' is set to **Yes** (in Step 3), the reset is delayed and a screen displaying the number of remaining calls and time is displayed. When the device begins to reset, a message appears notifying you of this.

## 28.2 Remotely Resetting Device using SIP NOTIFY

The device can be remotely reset upon the receipt of a SIP NOTIFY that includes an Event header set to 'check-sync;reboot=true', as shown in the example below:

```
NOTIFY sip:<user>@<dsthost> SIP/2.0
To: sip:<user>@<dsthost>
From: sip:sipsak@<srchost>
CSeq: 10 NOTIFY
Call-ID: 1234@<srchost>
Event: check-sync;reboot=true
```



➤ **To enable remote reset upon receipt of SIP NOTIFY:**

1. Open the Advanced Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Advanced Parameters**).
2. Under the Misc Parameters group, set the 'SIP Remote Rest' parameter to **Enable**.
3. Click **Submit**.



**Note:** This SIP Event header value is proprietary to AudioCodes.

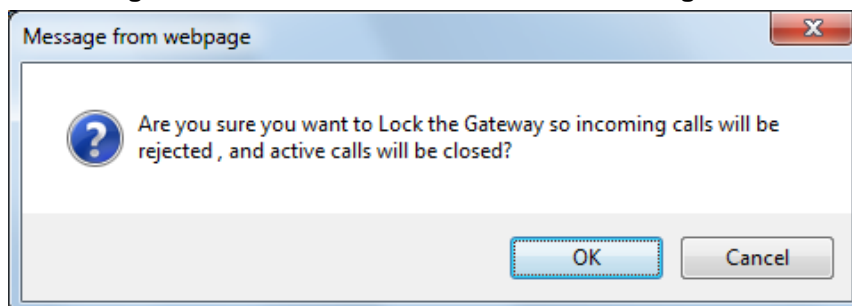
## 28.3 Locking and Unlocking the Device

The Lock and Unlock option allows you to lock the device so that it doesn't accept any new calls and maintains only the current calls. This is useful when, for example, you are uploading new software files to the device and you don't want any traffic to interfere with the process.

➤ **To lock the device:**

1. Open the Maintenance Actions page (see "Basic Maintenance" on page 305).
  2. Under the 'LOCK / UNLOCK' group, from the 'Graceful Option' drop-down list, select one of the following options:
    - **Yes:** The device is 'locked' only after the user-defined time in the 'Lock Timeout' field (see Step 3) expires or no more active traffic exists (the earliest thereof). In addition, no new traffic is accepted.
    - **No:** The device is 'locked' regardless of traffic. Any existing traffic is terminated immediately.
- Note:** These options are only available if the current status of the device is in the Unlock state.
3. In the 'Lock Timeout' field (relevant only if the parameter 'Graceful Option' in the previous step is set to **Yes**), enter the time (in seconds) after which the device locks. Note that if no traffic exists and the time has not yet expired, the device locks.
  4. Click the **LOCK** button; a confirmation message box appears requesting you to confirm device Lock.

**Figure 28-3: Device Lock Confirmation Message Box**



5. Click **OK** to confirm device Lock; if 'Graceful Option' is set to **Yes**, the lock is delayed and a screen displaying the number of remaining calls and time is displayed. Otherwise, the lock process begins immediately. The 'Current Admin State' field displays the current state - "LOCKED" or "UNLOCKED".



➤ **To unlock the device:**

1. Open the Maintenance Actions page (see "Maintenance Actions" on page 305).
2. Under the 'LOCK / UNLOCK' group, click the **UNLOCK** button. Unlock starts immediately and the device accepts new incoming calls.



**Note:** The Home page's General Information pane displays whether the device is locked or unlocked (see "Viewing the Home Page" on page 44).

## 28.4 Saving Configuration

The Maintenance Actions page allows you to save (*burn*) the current parameter configuration (including loaded auxiliary files) to the device's *non-volatile* memory (i.e., flash). The parameter modifications that you make throughout the Web interface's pages are temporarily saved (to the *volatile* memory - RAM) when you click the **Submit** button on these pages. Parameter settings that are saved only to the device's RAM revert to their previous settings after a hardware/software reset (or power failure). Therefore, to ensure that your configuration changes are retained, you must save them to the device's flash memory using the burn option described below.

➤ **To save the changes to the non-volatile flash memory :**

1. Open the Maintenance Actions page (see "Basic Maintenance" on page 305).
2. Under the 'Save Configuration' group, click the **BURN** button; a confirmation message appears when the configuration successfully saves.



**Notes:**

- Saving configuration to the *non-volatile* memory may disrupt current traffic on the device. To avoid this, disable all new traffic before saving, by performing a graceful lock (see "Locking and Unlocking the Device" on page 307).
- Throughout the Web interface, parameters displayed with the lightning ⚡ symbol are not applied on-the-fly and require that you reset the device for them to take effect (see "Resetting the Device" on page 305).
- The Home page's General Information pane displays whether the device is currently "burning" the configuration (see "Viewing the Home Page" on page 44).



## 29 High Availability Maintenance

The High Availability Maintenance page allows you to perform a switch-over between the Active and Redundant SBCs. It also allows you to reset the Redundant SBC.

**Notes:**

- When performing a switchover or a reset on a Redundant SBC, the HA mode becomes temporarily unavailable.
- This page can also be accessed from the toolbar's **Device Actions** drop-down menu options - **Switch Over** and **Reset Redundant** (refer to "Toolbar Description" on page 32).

➤ **To perform a switch-over:**

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

**Equation 1: High Availability Maintenance Page**

▼ Switch Over	
Switch Between Active And Redundant Boards	<b>Switch Over</b>
▼ Redundant Options	
Reset The Redundant Board	<b>Reset</b>

2. Under the 'Switch Over' group, click **Switch Over**; a confirmation box appears requesting you to confirm.
3. Click **OK**.

➤ **To reset the Redundant SBC:**

1. Under the 'Redundant Options' group, click **Reset**; a confirmation box appears requesting you to confirm.
2. Click **OK**.



## Reader's Notes



## 30 Software Upgrade

The **Software Update** menu allows you to do the following:

- Load Auxiliary Files (see "Loading Auxiliary Files" on page 311)
- Load Software License Key (see "Loading Software License Key" on page 320)
- Upgrade Device using Software Upgrade Wizard (see "Software Upgrade Wizard" on page 320)
- Load / save Configuration File (see "Backing Up and Loading Configuration File" on page 324)

### 30.1 Loading Auxiliary Files

Various Auxiliary files can be installed on the device. These Auxiliary files provide the device with additional configuration settings. The table below lists the different types of Auxiliary files:

**Table 30-1: Auxiliary Files**

File	Description
INI	Configures the device. The Web interface enables practically full device provisioning. However, some features may only be configured by ini file or you may wish to configure your device using the ini file. For more information on using the ini file to configure the device, see "INI File-Based Management" on page 71.
Call Progress Tones	Region-specific, telephone exchange-dependent file that contains the Call Progress Tones (CPT) levels and frequencies for the device. The default CPT file is U.S.A. For more information, see "Call Progress Tones File" on page 312.
Dial Plan	Provides dialing plans, for example, for obtaining the destination IP address for outbound IP routing. For more information, see "Dial Plan File" on page 315.
User Info	The User Information file maps PBX extensions to IP numbers. This file can be used to represent PBX extensions as IP phones in the global 'IP world'. For more information, see "User Information File" on page 316.

The Auxiliary files can be loaded to the device using one of the following methods:

- Web interface.
- TFTP: This is done by specifying the name of the Auxiliary file in an *ini* file (see Auxiliary and Configuration Files Parameters) and then loading the *ini* file to the device. The Auxiliary files listed in the *ini* file are then automatically loaded through TFTP during device startup. If the *ini* file does not contain a specific auxiliary file type, the device uses the last auxiliary file of that type that was stored on its non-volatile memory.




**Notes:**

- You can schedule automatic loading of updated auxiliary files using HTTP/HTTPS. For more information on automatic updates, see 'Automatic Update' on page 327.
- When loading an *ini* file using this Web page, parameters that are excluded from the loaded *ini* file retain their current settings (*incremental*).
- Saving an auxiliary file to flash memory may disrupt traffic on the device. To avoid this, disable all traffic on the device by performing a graceful lock as described in "Locking and Unlocking the Device" on page 307.
- For deleting auxiliary files, see "Viewing Device Information" on page 337.

The procedure below describes how to load Auxiliary files using the Web interface.

➤ **To load auxiliary files to the device using the Web interface:**

1. Open the Load Auxiliary Files page (**Maintenance** tab > **Software Update** menu > **Load Auxiliary Files**).



**Note:** The appearance of certain file load fields depends on the installed Software License Key.

2. Click the **Browse** button corresponding to the file type that you want to load, navigate to the folder in which the file is located, and then click **Open**; the name and path of the file appear in the field next to the **Browse** button.
3. Click the **Load File** button corresponding to the file you want to load.
4. Repeat steps 2 through 3 for each file you want to load.
5. Save the loaded auxiliary files to flash memory, see "Saving Configuration" on page 308 and reset the device (if you have loaded a Call Progress Tones file), see "Resetting the Device" on page 305.

### 30.1.1 Call Progress Tones File

The Call Progress Tones (CPT) auxiliary file includes the definitions of the Call Progress Tones (levels and frequencies) that are detected / generated by the device.

You can use one of the supplied auxiliary files (.dat file format) or create your own file. To create your own file, it's recommended to modify the supplied *usa\_tone.ini* file (in any standard text editor) to suit your specific requirements and then convert the modified *ini* file into binary format, using AudioCodes DConvert utility. For a description on converting a CPT *ini* file into a binary *dat* file, refer to the *DConvert Utility User's Guide*.



**Note:** Only the *dat* file format can be loaded to the device.

You can create up to 32 different Call Progress Tones, each with frequency and format attributes. The frequency attribute can be single or dual-frequency (in the range of 300 to 1980 Hz) or an Amplitude Modulated (AM). Up to 64 different frequencies are supported. Only eight AM tones, in the range of 1 to 128 kHz, can be configured (the detection range



is limited to 1 to 50 kHz). Note that when a tone is composed of a single frequency, the second frequency field must be set to zero.

The format attribute can be one of the following:

- **Continuous:** A steady non-interrupted sound (e.g., a dial tone). Only the 'First Signal On time' should be specified. All other on and off periods must be set to zero. In this case, the parameter specifies the detection period. For example, if it equals 300, the tone is detected after 3 seconds (300 x 10 msec). The minimum detection time is 100 msec.
- **Cadence:** A repeating sequence of on and off sounds. Up to four different sets of on/off periods can be specified.
- **Burst:** A single sound followed by silence. Only the 'First Signal On time' and 'First Signal Off time' should be specified. All other on and off periods must be set to zero. The burst tone is detected after the off time is completed.

You can specify several tones of the same type. These additional tones are used only for tone detection. Generation of a specific tone conforms to the first definition of the specific tone. For example, you can define an additional dial tone by appending the second dial tone's definition lines to the first tone definition in the *ini* file. The device reports dial tone detection if either of the two tones is detected.

The Call Progress Tones section of the *ini* file comprises the following segments:

- **[NUMBER OF CALL PROGRESS TONES]:** Contains the following key:  
'Number of Call Progress Tones' defining the number of Call Progress Tones that are defined in the file.
- **[CALL PROGRESS TONE #X]:** containing the Xth tone definition, starting from 0 and not exceeding the number of Call Progress Tones less 1 defined in the first section (e.g., if 10 tones, then it is 0 to 9), using the following keys:
  - **Tone Type:** Call Progress Tone types:
    - ◆ [1] Dial Tone
    - ◆ [2] Ringback Tone
    - ◆ [3] Busy Tone
    - ◆ [4] Congestion Tone
    - ◆ [6] Warning Tone
    - ◆ [7] Reorder Tone
    - ◆ [17] Call Waiting Ringback Tone - heard by the calling party
    - ◆ [18] Comfort Tone
    - ◆ [23] Hold Tone
    - ◆ [46] Beep Tone
  - **Tone Modulation Type:** Amplitude Modulated (1) or regular (0)
  - **Tone Form:** The tone's format can be one of the following:
    - ◆ Continuous (1)
    - ◆ Cadence (2)
    - ◆ Burst (3)
  - **Low Freq [Hz]:** Frequency (in Hz) of the lower tone component in case of dual frequency tone, or the frequency of the tone in case of single tone. This is not relevant to AM tones.
  - **High Freq [Hz]:** Frequency (in Hz) of the higher tone component in case of dual frequency tone, or zero (0) in case of single tone (not relevant to AM tones).
  - **Low Freq Level [-dBm]:** Generation level 0 dBm to -31 dBm in dBm (not relevant to AM tones).
  - **High Freq Level:** Generation level of 0 to -31 dBm. The value should be set to 32 in the case of a single tone (not relevant to AM tones).



- **First Signal On Time [10 msec]:** 'Signal On' period (in 10 msec units) for the first cadence on-off cycle. For continuous tones, this parameter defines the detection period. For burst tones, it defines the tone's duration.
- **First Signal Off Time [10 msec]:** 'Signal Off' period (in 10 msec units) for the first cadence on-off cycle (for cadence tones). For burst tones, this parameter defines the off time required after the burst tone ends and the tone detection is reported. For continuous tones, this parameter is ignored.
- **Second Signal On Time [10 msec]:** 'Signal On' period (in 10 msec units) for the second cadence on-off cycle. Can be omitted if there isn't a second cadence.
- **Second Signal Off Time [10 msec]:** 'Signal Off' period (in 10 msec units) for the second cadence on-off cycle. Can be omitted if there isn't a second cadence.
- **Third Signal On Time [10 msec]:** 'Signal On' period (in 10 msec units) for the third cadence on-off cycle. Can be omitted if there isn't a third cadence.
- **Third Signal Off Time [10 msec]:** 'Signal Off' period (in 10 msec units) for the third cadence on-off cycle. Can be omitted if there isn't a third cadence.
- **Fourth Signal On Time [10 msec]:** 'Signal On' period (in 10 msec units) for the fourth cadence on-off cycle. Can be omitted if there isn't a fourth cadence.
- **Fourth Signal Off Time [10 msec]:** 'Signal Off' period (in 10 msec units) for the fourth cadence on-off cycle. Can be omitted if there isn't a fourth cadence.
- **Carrier Freq [Hz]:** Frequency of the carrier signal for AM tones.
- **Modulation Freq [Hz]:** Frequency of the modulated signal for AM tones (valid range from 1 to 128 Hz).
- **Signal Level [-dBm]:** Level of the tone for AM tones.
- **AM Factor [steps of 0.02]:** Amplitude modulation factor (valid range from 1 to 50). Recommended values from 10 to 25.


**Notes:**

- When the same frequency is used for a continuous tone and a cadence tone, the 'Signal On Time' parameter of the continuous tone must have a value that is greater than the 'Signal On Time' parameter of the cadence tone. Otherwise, the continuous tone is detected instead of the cadence tone.
- The tones frequency must differ by at least 40 Hz between defined tones.

For example, to configure the dial tone to 440 Hz only, enter the following text:

```
[NUMBER OF CALL PROGRESS TONES]
Number of Call Progress Tones=1
#Dial Tone
[CALL PROGRESS TONE #0]
Tone Type=1
Tone Form =1 (continuous)
Low Freq [Hz]=440
High Freq [Hz]=0
Low Freq Level [-dBm]=10 (-10 dBm)
High Freq Level [-dBm]=32 (use 32 only if a single tone is
required)
First Signal On Time [10msec]=300; the dial tone is detected after
3 sec
First Signal Off Time [10msec]=0
Second Signal On Time [10msec]=0
Second Signal Off Time [10msec]=0
```



## 30.1.2 Dial Plan File

The Dial Plan file can be used for various digit mapping features, as described in this section.

### 30.1.2.1 Creating a Dial Plan File

Creating a Dial Plan file is similar between all Dial Plan features. The main difference is the syntax used in the Dial Plan file and the method for selecting the Dial Plan index to use for the specific feature.

The Dial Plan file is a text-based file that can contain up to eight Dial Plans (Dial Plan indices) and up to 8,000 rules (lines). The general syntax rules for the Dial Plan file are as follows (syntax specific to the feature is described in the respective section):

- Each Dial Plan index must begin with a Dial Plan name enclosed in square brackets "[...]" on a new line.
- Each line under the Dial Plan index defines a rule.
- Empty lines are ignored.
- Lines beginning with a semicolon ";" are ignored. The semicolon can be used for comments.

➤ **To create a Dial Plan file:**

1. Create a new file using a text-based editor (such as Notepad) and configure your Dial Plans, as required.
2. Save the file with the *ini* file extension name (e.g., mydialplanfile.ini).
3. Convert the *ini* file to a *dat* binary file, using AudioCodes DConvert utility. For more information, refer to *DConvert Utility User's Guide*.
4. Install the converted file on the device, as described in "Loading Auxiliary Files" on page 311.
5. Select the Dial Plan index that you want to use. This depends on the feature and is described in the respective section.

### 30.1.2.2 Obtaining IP Destination from Dial Plan File

You can use a Dial Plan index listed in a loaded Dial Plan file for determining the IP destination of SBC calls. This enables the mapping of called numbers to IP addresses (in dotted-decimal notation) or FQDNs (up to 15 characters).

➤ **To configure routing to an IP destination based on Dial Plan:**

1. Create the Dial Plan file. The syntax of the Dial Plan index for this feature is as follows:

```
<destination / called prefix number>,0,<IP destination>
```

Note that the second parameter "0" is not used and 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
10.33.8.52
201,0,10.33.8.52
300,0,itsp.com ; called prefix 300 is routed to itsp.com
```

2. Convert the file to a loadable file and then load it to the device.



3. Assign the Dial Plan index to the required routing rule:
  - a. Open the SBC IP-to-IP Routing table.
  - b. Set the 'Destination Type' field to Dial Plan.
  - c. In the 'Destination Address' field, enter the required Dial Plan index, where "0" denotes [PLAN1] in the Dial Plan file, "1" denotes [PLAN2], and so on.

### 30.1.3 User Information File

This section describes the various uses of the User Info file.

You can load the User Info file using any of the following methods:

- Web interface (see 'Loading Auxiliary Files' on page 311)
- *ini* file - using the `UserInfoFileName` parameter, e.g., `UserInfoFileName = 'UserInformationFile.txt'` (see 'Auxiliary and Configuration File Name Parameters' on page 470)
- Automatic update mechanism - using the `UserInfoFileURL` parameter, e.g., `UserInfoFileUrl = 'http://192.168.0.250/Audiocodes/ UserInformationFile.txt'` (see 'Automatic Update Mechanism' on page 327)

#### 30.1.3.1 User Information File for SBC User Database

You can create a User Info table of SBC users from a loaded User Info file.

The device can use the SBC User Info for the following:

- Registering each user to an external registrar server.
- Authenticating (for any SIP request and as a client) each user if challenged by an external server.
- Authenticating as a server incoming user requests (for SBC security).

If the device registers on behalf of users and the users do not perform registration, any SIP request destined to the user is routed to the Proxy Set associated with the user's IP Group.

The User Info file is a text-based file that you can create using any text-based program such as Notepad. To add SBC users to this file, use the following syntax:

```
[SBC]
FORMAT LocalUser,UserName,Password,IPGroupID
john,john_user,john_pass,2
sue,sue_user,sue_pass,1
```

where:

- *LocalUser* is the user and is used as the Request-URI user part for the AOR in the database
- *UserName* is the user's authentication username
- *Password* is the user's authentication password
- *IPGroupID* is the IP Group ID to which the user belongs and is used as the Request-URI source host part for the AOR in the database



#### Notes:

- To enable the User Info table, see 'Enabling the User Info Table' on page 317.
- To modify the Use Info table, you need to load a new User Info file containing your modifications.



### 30.1.3.2 Enabling the User Info Table

The procedure below describes how to load a User Info file to the device and enable the use of the User Info table:

➤ **To enable the User Info table:**

1. Open the Advanced Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Advanced Parameters**).
2. Set the 'Enable User-Information Usage' parameter to **Enable**.

## 30.2 Software License Key

The device is shipped with a pre-installed Software License Key, which determines the device's supported features, capabilities, and available resources. You can upgrade or change your device's supported features by purchasing and installing a new Software License Key to match your requirements.



**Notes:**

- The device is shipped by default with a pre-installed Software License Key that enables only one call session. Once you have installed the Mediant Software E-SBC on your hosted platform, you need to load a Software License Key file, supplied in the package, to enable the call capacity and features that you ordered. If you did not receive this Software License Key file with your installation disk, contact your AudioCodes sales representative to obtain it, as described in 'Obtaining the Software License Key File' below.
- The availability of certain Web pages depends on the installed Software License Key.

### 30.2.1 Obtaining the Software License Key File

Before you can install a new Software License Key, you need to obtain a Software License Key file for your device with the required features from your AudioCodes representative. The Software License Key is an encrypted key in string format that is associated with the device's serial number ("S/N") and supplied in a text-based file.

If you need a Software License Key for more than one device, the Software License Key file can include multiple Software License Keys (see figure below). In such cases, each Software License Key in the file is associated with a unique serial number identifying the specific device. When loading such a Software License Key file, the device installs only the Software License Key that is associated with its serial number.

**Figure 4: Software License Key File with Multiple S/N Lines**





➤ **To obtain a Software License Key:**

1. Make a note of the serial number of the device:
  - a. Open the Device Information page (**Status & Diagnostics** tab > **System Status** menu > **Device Information**).
  - b. The serial number is displayed in the "Serial Number" field.
2. If you need a Software License Key for more than one device, repeat Step 1 for each device.
3. Request the required Software License Key from your AudioCodes representative and provide them with the serial number of the device(s).
4. When you receive the new Software License Key file, check the file as follows:
5. Open the file with any text-based program such as Notepad.
  - a. Verify that the first line displays "[LicenseKeys]".
  - b. Verify that the file contains one or more lines in the following format:  
 "S/N<serial number> = <Software License Key string>".  
 For example: "S/N370604 = jCx6r5tovCIKaBBbhPtT53Yj..."
  - c. Verify that the "S/N" value reflects the serial number of your device. If you have multiple Software License Keys, ensure that each "S/N" value corresponds to a device.



**Warning:** Do not modify the contents of the Software License Key file.

6. Install the Software License Key on the device as described in 'Installing the Software License Key' on page 318.

## 30.2.2 Installing the Software License Key

Once you have received your Software License Key file from your AudioCodes representative, you can install it on the device using one of the following management tools:

- Web interface - see 'Installing Software License Key using Web Interface' on page 319
- AudioCodes EMS - refer to the EMS User's Manual or EMS Product Description



**Notes:**

- For the High Availability (HA) system, the Software License Key includes the HA feature and is installed on both devices - active and redundant. If the redundant device's Software License Key is missing or invalid, the system is moved to mismatch configuration mode (alerted by SNMP).
- When you install a new Software License Key, it is loaded to the device's non-volatile flash memory and overwrites the previously installed Software License Key.

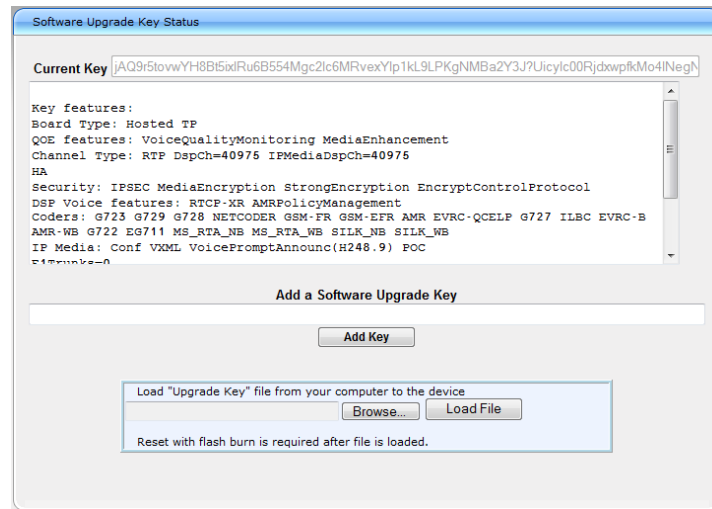


### 30.2.2.1 Installing Software License Key using Web Interface

The procedure below describes how to install the Software License Key using the Web interface.

➤ **To install the Software License Key using the Web interface:**

1. Open the Software Upgrade Key Status page (**Maintenance** tab > **Software Update** menu > **Software Upgrade Key**).



2. As a precaution, backup the Software License Key currently installed on the device. If the new Software License Key does not comply with your requirements, you can re-load this backup to restore the device's original capabilities.
  - a. In the 'Current Key' field, select the entire text string and copy it to any standard text file (e.g., Notepad).
  - b. Save the text file with any file name and file extension (e.g., key.txt) to a folder on your computer.
3. Depending on whether you are loading a Software License Key file with a single Software License Key (i.e., one "S/N") or with multiple Software License Keys (i.e., more than one "S/N"), do one of the following:
  - **Loading a File with a Single Software License Key:**
    - a. Open the Software License Key file using a text-based program such as Notepad.
    - b. Copy-and-paste the string from the file to the 'Add a Software Upgrade Key' field.
    - c. Click the **Add Key** button.
  - **Loading a File with Multiple Software License Keys:**
    - a. In the 'Load Upgrade Key file ...' field, click the **Browse** button and navigate to the folder in which the Software License Key file is located on your computer.
    - b. Click **Load File**; the new key is installed on the device.

If the Software License Key is valid, it is burned to the device's flash memory and displayed in the 'Current Key' field.



4. Verify that the Software License Key was successfully installed, by doing one of the following:
  - In the Software License Key Status page, check that the listed features and capabilities activated by the installed Software License Key match those that were ordered.
  - Access the Syslog server and ensure that the following message appears in the Syslog server:  
"S/N\_\_\_ Key Was Updated. The Board Needs to be Reloaded with ini file\n"
5. Reset the device; the new capabilities and resources enabled by the Software License Key are active.



**Note:** If the Syslog server indicates that the Software License Key was unsuccessfully loaded (i.e., the "SN\_" line is blank), do the following preliminary troubleshooting procedures:

1. Open the Software License Key file and check that the "S/N" line appears. If it does not appear, contact AudioCodes.
2. Verify that you have loaded the correct file. Open the file and ensure that the first line displays "[LicenseKeys]".
3. Verify that the content of the file has not been altered.

## 30.3 Software Upgrade Wizard

The Software Upgrade Wizard allows you to upgrade the device's firmware. The firmware file has the .cmp file extension name. The wizard also enables you to load an *ini* file and/or auxiliary files (typically loaded using the Load Auxiliary File page described in "Loading Auxiliary Files" on page 311). However, it is mandatory when using the wizard to first load a .cmp file to the device. You can then choose to also load an *ini* file and/or auxiliary files, but this cannot be done without first loading a .cmp file. For the *ini* and each auxiliary file type, you can choose to load a new file or not load a file but use the existing file (i.e., maintain existing configuration) running on the device.

The wizard also allows you to perform Hitless Upgrade (non-traffic affecting upgrade), whereby the upgrade process begins only after all current calls have been terminated. For a description of this process, see Software Upgrade on page 302.



**Warning:** The Software Upgrade Wizard requires the device to be reset at the end of the process, which may disrupt traffic. To avoid this, disable all traffic on the device before initiating the wizard by performing a graceful lock (see "Basic Maintenance" on page 305).



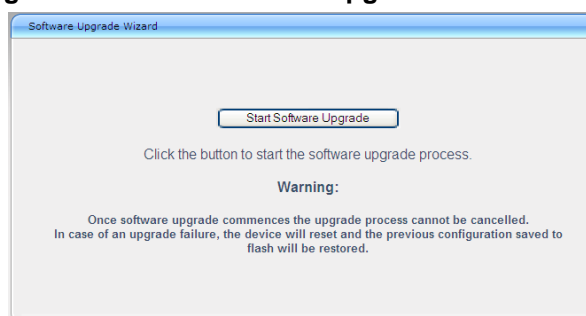
**Notes:**

- When upgrading from Version 6.4 to 6.6 using the Web interface, the Software Upgrade Wizard is not supported. To do so, back up the current configuration (ini file), install the 6.6 version from the installation CD, and then restore configuration. Refer to the *Installation Manual* for more information.
- When upgrading to a new software version, ensure that you have installed the new Software License Key.
- You can get the latest software files from AudioCodes Web site at <http://www.audiocodes.com/downloads>.
- Before upgrading the device, it is recommended that you save a copy of the device's configuration settings (i.e., *ini* file) to your computer. If an upgrade failure occurs, you can then restore your configuration settings by uploading the backup file to the device. For saving and restoring configuration, see "Backing Up and Loading Configuration File" on page 324.
- If you wish to also load an *ini* or auxiliary file, it is mandatory to first load a .cmp file.
- When you activate the wizard, the rest of the Web interface is unavailable. After the files are successfully loaded, access to the full Web interface is restored.
- If you upgraded your .cmp and the "SW version mismatch" message appears in the Syslog or Web interface, then your Software License Key does not support the new .cmp file version. If this occurs, contact AudioCodes support for assistance.
- If you use the wizard to load an *ini* file, parameters excluded from the *ini* file are assigned default values (according to the .cmp file running on the device) thereby, overriding values previously defined for these parameters.
- You can schedule automatic loading of these files using HTTP/HTTPS (see 'Automatic Update' on page 327).

➤ **To load files using the Software Upgrade Wizard:**

1. Stop all traffic on the device using the Graceful Lock feature (refer to the warning bulletin above).
2. Open the Software Upgrade wizard, by performing one of the following:
  - Select the **Maintenance** tab, click the **Software Update** menu, and then click **Software Upgrade Wizard**.
  - On the toolbar, click **Device Actions**, and then choose **Software Upgrade Wizard**.


**Figure 30-5: Start Software Upgrade Wizard Screen**





3. Click the **Start Software Upgrade** button; the wizard starts, requesting you to browse to a .cmp file for uploading.




**Note:** At this stage, you can quit the Software Update Wizard, by clicking **Cancel** , without requiring a device reset. However, once you start uploading a cmp file, the process must be completed with a device reset. If you choose to quit the process in any of the subsequent pages, the device resets.

4. Click the **Browse** button, navigate to the .cmp file, and then click **Load File**; a progress bar appears displaying the status of the loading process. When the .cmp file is successfully loaded to the device, a message appears notifying you of this.
5. If your device is in HA mode, select one of the following options:
  - Hitless Upgrade: (Default) To perform a Hitless Upgrade (non-traffic effecting upgrade), whereby the upgrade process begins only after all current calls have been terminated.
  - System Reset Upgrade: Both SBCs immediately reset with the newly loaded .cmp file.






**Note:** If you select Hitless Upgrade, you can upload only a .cmp file (auxiliary files and ini files cannot be uploaded as well).



6. If you want to load **only** a .cmp file, then click the **Reset**  button to reset the device with the newly loaded .cmp file, utilizing the existing configuration (*ini*) and auxiliary files. To load additional files, skip to the next Step.



**Note:** Device reset may take a few minutes depending on cmp file version (this may even take up to 10 minutes).

7. Click the **Next**  button; the wizard page for loading an *ini* file appears. You can now perform one of the following:
  - Load a new *ini* file: Click **Browse**, navigate to the *ini* file, and then click **Send File**; the *ini* file is loaded to the device and you're notified as to a successful loading.
  - Retain the existing configuration (*ini* file): Do not select an *ini* file, and ensure that the 'Use existing configuration' check box is selected (default).
  - Return the device's configuration settings to factory defaults: Do not select an *ini* file, and clear the 'Use existing configuration' check box.
8. Click the **Next**  button to progress to the relevant wizard pages for loading the desired auxiliary files. To return to the previous wizard page, click the **Back**  button. As you navigate between wizard pages, the relevant file type corresponding to the Wizard page is highlighted in the left pane.



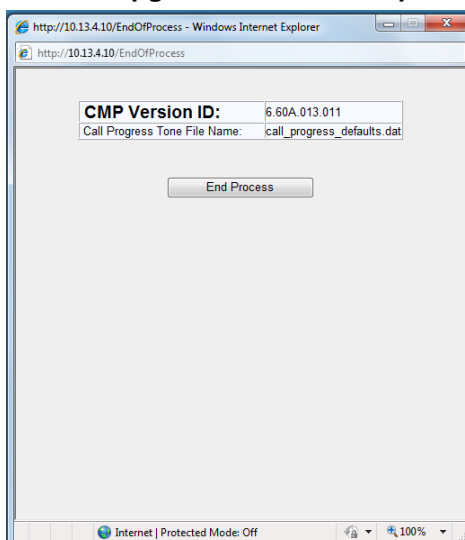
9. When you have completed loading all the desired files, click the **Next**  button until the last wizard page appears ("FINISH" is highlighted in the left pane).
10. Click the **Reset**  button to complete the upgrade process; the device 'burns' the newly loaded files to flash memory and then resets the device.



**Note:** Device reset may take a few minutes (depending on .cmp file version, this may even take up to 30 minutes).

After the device resets, the End of Process wizard page appears displaying the new .cmp and auxiliary files loaded to the device.

**Figure 30-6: Software Upgrade Process Completed Successfully**



11. Click **End Process** to close the wizard; the Web Login dialog box appears.
12. Enter your login user name and password, and then click **OK**; a message box appears informing you of the new .cmp file.
13. Click **OK**; the Web interface becomes active, reflecting the upgraded device.



## 30.4 Backing Up and Loading Configuration File

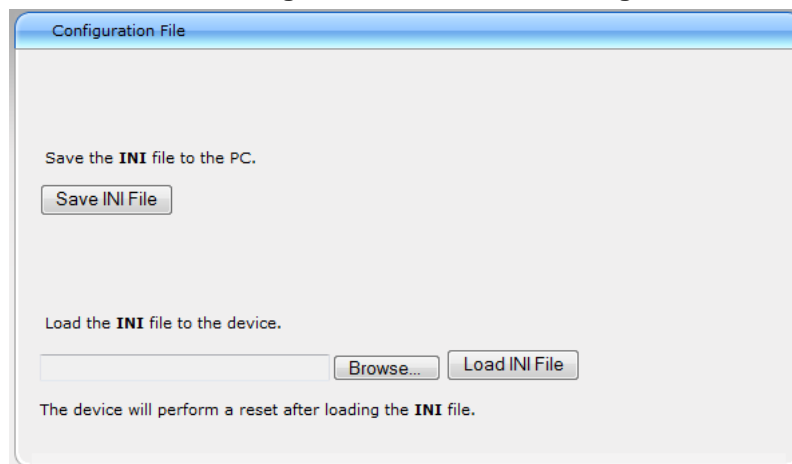
You can save a copy/backup of the device's current configuration settings as an *ini* file to a folder on your computer, using the Configuration File page. The saved *ini* file includes only parameters that were modified and parameters with other than default values. The Configuration File page also allows you to load an *ini* file to the device. If the device has "lost" its configuration, you can restore the device's configuration by loading the previously saved *ini* file or by simply loading a newly created *ini* file.



**Note:** When loading an *ini* file using this Web page, parameters not included in the *ini* file are reset to default settings.

### ➤ To save the *ini* file:

1. Open the Configuration File page by doing one of the following:
  - From the Navigation tree, click the **Maintenance** tab, click the **Software Update** menu, and then click **Configuration File**.
  - On the toolbar, click **Device Actions**, and then from the drop-down menu, choose **Load Configuration File** or **Save Configuration File**.



2. To save the *ini* file to a folder on your computer, do the following:
  - a. Click the **Save INI File** button; the File Download dialog box appears.
  - b. Click the **Save** button, navigate to the folder where you want to save the *ini* file, and then click **Save**.
3. To load the *ini* file to the device, do the following:
  - a. Click the **Browse** button, navigate to the folder where the *ini* file is located, select the file, and then click **Open**; the name and path of the file appear in the field beside the **Browse** button.
  - b. Click the **Load INI File** button, and then at the prompt, click **OK**; the device uploads the *ini* file and then resets (from the *cmp* version stored on the flash memory). Once complete, the Web Login screen appears, requesting you to enter your user name and password.



## 31 Returning the System to a Previous State

Taking a system snapshot captures a complete Mediant Software E-SBC state, including the following:

- Installed Mediant Software E-SBC software
- Current configuration
- Auxiliary files
- Software License Key

The device does a first snapshot automatically upon initial installation. You may do up to 10 additional snapshots, if required, as described in "Taking a Snapshot" on page 325. You can restore the device to a previous snapshot, as described in "Returning to a Snapshot State" on page 326.

### 31.1 Taking a Snapshot

The procedure below describes how to make a snapshot of the current device state.

➤ **To take a snapshot using CLI:**

1. Establish a CLI connection with the device.
2. At the prompt, type the following command:  

```
enable
```
3. At the prompt, type the password:  

```
Password: Admin
```
4. At the prompt, type the following command to save the current configuration (burn) before creating a snapshot:  

```
write
```
5. At the prompt, type the following commands to take the snapshot:  

```
configure system
startup-n-recovery
create-system-snapshot <snapshot name>
```



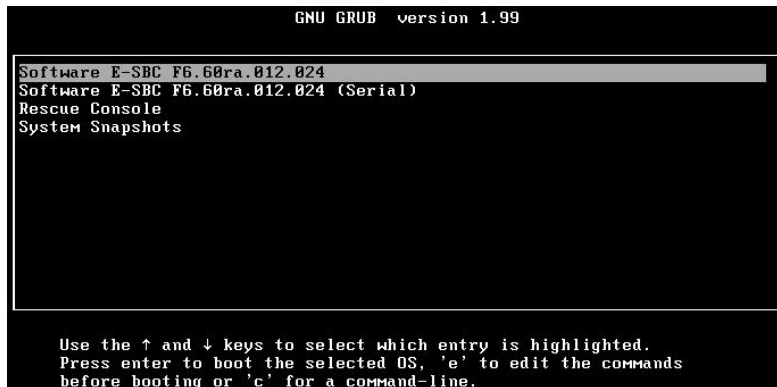
## 31.2 Returning to a Snapshot State

If you want to restore the device to a previous snapshot state, then follow the procedure below.

➤ **To return to a previous snapshot state:**

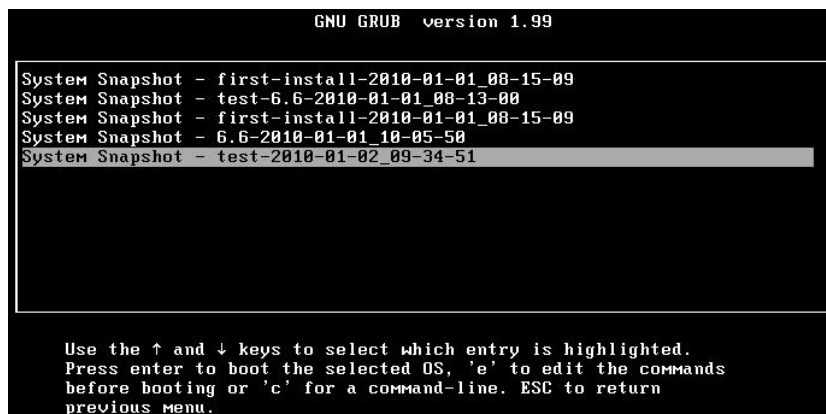
1. Reboot the server.
2. In the GRUB menu, displayed for a few seconds during the server start-up, press the Down key to prevent the server from starting the Mediant Software E-SBC software:

**Figure 31-1: GRUB Menu**



3. Select **System Snapshots**, and then press Enter; you're prompted to select a snapshot:

**Figure 31-2: Selecting a Snapshot**



4. Select a snapshot, and then press Enter; the system returns to the selected snapshot state. This operation may take up to 10 minutes to complete. The system automatically reboots after the return is complete.

## 31.3 Automatic Recovery to Default Snapshot

After three unsuccessful attempts at rebooting, the device automatically returns to the default snapshot.

The default snapshot is either:

- the first snapshot automatically taken upon initial installation from CD,
- or -
- the last snapshot taken.



## 32 Automatic Update

Automatic provisioning is useful for large-scale deployment of devices. In some cases, the devices are shipped to the end customer directly from the manufacturer. In other cases, they may pass through a staging warehouse. Configuration may occur at the staging warehouse or at the end-customer premises.

The devices may be pre-configured during the manufacturing process (commonly known as *private labeling*). Typically, a two-stage configuration process is implemented such that initial configuration includes only basic configuration, while the final configuration is done when the device is deployed in a live network.

Automatic provisioning can be used to update the following files:

- Software file (*cmp*)
- Auxiliary files (e.g., Call Progress Tones)
- Configuration file (*ini*)

The Automatic Update mechanism is applied per file, using specific parameters that define the URLs to the servers where the files are located, and the file names (see Automatic Update Parameters on page 471). These files can be stored on any standard Web, FTP, or NFS server and can be loaded periodically to the device using HTTP, HTTPS, FTP, or NFS. This mechanism can be used even for devices that are installed behind NAT and firewalls.

The Automatic Update mechanism can be triggered by the following:

- Upon device startup.
- At a user-defined time of day (e.g., 18:00), configured by the *ini* file parameter `AutoUpdatePredefinedTime`.
- Periodically (e.g., every 60 minutes), configured by the *ini* file parameter `AutoUpdateFrequency`.
- Upon startup but before the device is operational, if the Secure Startup feature is enabled (see 'Loading Files Securely (Disabling TFTP)' on page 332).
- Upon receipt of a special SIP Notify message (see 'Remotely Triggering Auto Update using SIP NOTIFY' on page 332)

When implementing Automatic Updates using HTTP/S, the device determines whether the file on the provisioning server is an updated one as follows:

- **Configuration file:** The device checks the timestamp according to the HTTP server response. Cyclical Redundancy Check (CRC) is only checked if the `AUPDCheckIfIniChanged` parameter is enabled. The device downloads the configuration file only if it was modified since the last successful configuration update.
- **Software file (*cmp*):** The device first downloads the file and then checks if its version number is different from the software version file currently stored on the device's flash memory.
- **Auxiliary files (e.g., CPT):** These files are updated only once. To update the auxiliary file again, you must modify the settings of the related parameter that configures its URL.

### 32.1 Configuring Automatic Update

The procedure below describes how to configure the Automatic Update feature. It describes a scenario where the devices download a "master" configuration file with common settings from an HTTP server. This "master" file applies common configuration and instructs each device to download a specific configuration file based on the device's MAC address from an HTTP server.





**Warning:** Do not use the Web interface to configure the device when the Automatic Update feature is implemented. If you do and save (burn) the new settings to the device's flash memory, the IniFileURL parameter is automatically set to 0 and Automatic Updates is consequently disabled. To enable Automatic Updates again, you would need to re-load the ini file (using the Web interface or BootP) with the correct IniFileURL settings. As a safeguard to an unintended burn-to-flash when resetting the device, if the device is configured for Automatic Updates, the 'Burn To FLASH' field under the Reset Configuration group in the Web interface's Maintenance Actions page is automatically set to **No** by default.



**Note:** For a description of all the Automatic Update *ini* file parameters, see Automatic Update Parameters on page 471.

➤ **To configure the Automatic Update feature (ini file example):**

1. Setup a Web server (e.g., <http://www.corp.com>) and place all the required configuration files on this server.
2. For each device, preconfigure the following parameter (DHCP / DNS are assumed):

```
IniFileURL = 'http://www.corp.com/master_configuration.ini'
```

3. Create a file named *master\_configuration.ini* with the following text:

```
Common configuration for all devices

CptFileURL = 'http://www.corp.com/call_progress.dat'
Check for updates every 60 minutes
AutoUpdateFrequency = 60
Additional configuration per device

Each device loads a file named based on its MAC address
(e.g., config_00908F033512.ini)
IniFileURL = 'http://www.corp.com/config_<MAC>.ini'
Reset the device after configuration is updated.
The device resets after all files are processed.
ResetNow = 1
```

You can modify the *master\_configuration.ini* file (or any of the *config\_<MAC>.ini* files) at any time. The device queries for the latest version every 60 minutes and applies the new settings immediately.

4. For additional security, use HTTPS or FTPS. The device supports HTTPS (RFC 2818) and FTPS using the AUTH TLS method <draft-murray-auth-ftp-ssl-16>.
5. To download configuration files from an NFS server, the NFS file system parameters should be defined in the *ini* file. The following is an example of an *ini* file for downloading files from NFS servers using NFS version 2:

```
Define NFS servers for Automatic Update
[NFSServers]
FORMAT NFSServers_Index = NFSServers_HostOrIP,
NFSServers_RootPath, NFSServers_NfsVersion;
NFSServers 1 = 10.31.2.10, /usr/share, 2 ;
NFSServers 2 = 192.168.100.7, /d/shared, 2 ;
[\NFSServers]
CptFileUrl =
'file://10.31.2.10/usr/share/public/usa_tones.dat'
```



```
VpFileUrl =
'file://192.168.100.7/d/shared/gateways/voiceprompt.dat'
```

The following *ini* file example can be used to activate the Automatic Update mechanism.

```
DNS is required for specifying domain names in URLs
[InterfaceTable]
FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_VlanID, InterfaceTable_InterfaceName,
InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress,
InterfaceTable_UnderlyingInterface;
InterfaceTable 0 = 6, 10, 10.13.4.12, 16, 10.13.0.1, 1, Mng,
10.1.1.11, 0.0.0.0, ;
[\InterfaceTable]

Load an extra configuration ini file using HTTP
IniFileURL = 'http://webserver.corp.com/Gateway/inifile.ini'
Load Call Progress Tones file using HTTPS
CptFileUrl = 'https://10.31.2.17/usa_tones.dat'
Load Voice Prompts file using FTPS with user 'root' and password
'wheel'
VpFileUrl = 'ftps://root:wheel@ftpserver.corp.com/vp.dat'
Update every day at 03:00 AM
AutoUpdatePredefinedTime = '03:00'
Note: The cmp file isn't updated since it's disabled by default
(AutoUpdateCmpFile).
```



#### Notes:

- The Automatic Update mechanism assumes that the external Web server conforms to the HTTP standard. If the Web server ignores the If-Modified-Since header, or doesn't provide the current date and time during the HTTP 200 OK response, the device may reset itself repeatedly. To overcome this problem, modify the update frequency, using the AutoUpdateFrequency parameter.
- To load a different configuration file (ini file) per device, add the string "<MAC>" to the URL (e.g., IniFileURL = 'http://www.corp.com/config\_<MAC>.ini'). This mnemonic is replaced with the device's hardware MAC address, resulting in an ini file name request that contains the device's MAC address (e.g., config\_00908F033512.ini).
- To prevent the device from accidentally upgrading its software, by default the Automatic Update feature does not apply a downloaded *cmp* file even if its URL was configured (using the CmpFileURL parameter). To enable this, set the AutoUpdateCmpFile parameter to 1.
- To enable the device to automatically reset after an ini file has been loaded, set the ResetNow parameter to 1. This is important if the downloaded configuration file includes parameters that require a device reset for its settings to be applied.
- By default, parameters that are not included in the downloaded configuration file are set to default. To retain the current settings of these parameters, set the SetDefaultOnINIFileProcess parameter to 0.



## 32.2 Automatic Configuration Methods

This section describes available methods that can be used for automatic device configuration.

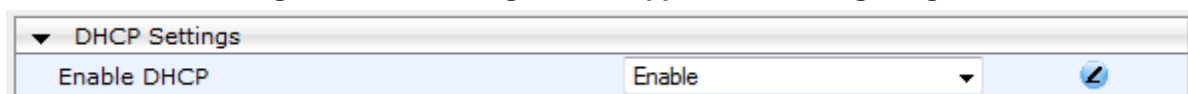
### 32.2.1 DHCP-based Configuration Server

The DHCP server can be configured to automatically provide each device with a temporary IP address so that individual MAC addresses are not required. Configuration occurs at a staging warehouse for this method.

➤ **To enable DHCP for obtaining an IP address:**

1. Open the Application Settings page (**Configuration** tab > **System** menu > **Application Settings**).

**Figure 32-1: Enabling DHCP - Application Settings Page**



2. From the 'Enable DHCP' drop-down list, select **Enable**.
3. Click **Submit**.



**Notes:** When using DHCP to acquire an IP address, the Multiple Interface table, VLANs and other advanced configuration options are disabled.

Below is an example configuration file for Linux DHCP server (dhcpd.conf). The devices are allocated temporary IP addresses in the range 10.31.4.53 to 10.31.4.75. TFTP is assumed to be on the same computer as the DHCP server (alternatively, the "next-server" directive may be used).

```
ddns-update-style ad-hoc;
default-lease-time 60;
max-lease-time 60;
class "gateways" {
 match if(substring(hardware, 1, 3) = 00:90:8f);
}
subnet 10.31.0.0 netmask 255.255.0.0 {
 pool {
 allow members of "audiocodes";
 range 10.31.4.53 10.31.4.75;
 filename "SIP_F6.60A.217.003.cmp -fb;device.ini";
 option routers 10.31.0.1;
 option subnet-mask 255.255.0.0;
 }
}
```

### 32.2.2 HTTP-based Automatic Updates

An HTTP/S server can be placed in the customer's network where configuration and software updates are available for download. This does not require additional servers at the customer premises and is NAT-safe.

For example, assume the core network HTTPS server is <https://www.corp.com>. A master configuration *ini* file should be placed on the server, e.g., <https://www.corp.com/gateways/master.ini>. This file could point to additional *ini* files,



auxiliary files (e.g., call progress tones), and software files (cmp), all on the same HTTP server or different HTTP servers in the network.

The main advantage of this method is that the HTTP configuration can be checked periodically when the device is deployed at the customer site. HTTP(S) is not sensitive to NAT devices, enabling configuration whenever needed without on-site intervention.

For additional security, the URL may contain a different port, and username and password.

The devices should only be pre-configured with the URL of the initial *ini* file, using one of the following methods:

- Methods described in 'DHCP-based Configuration Server' on page 330 or above, via TFTP at a staging warehouse. The configuration URL is configured using the IniFileURL parameter.
- Private labeling.
- Manually on-site, using the RS-232 port or Web interface.

When the device is deployed at the customer site, local DHCP server provides the devices with IP addressing and DNS server information. From the URL provided in the DHCP response, the device can then contact the HTTP server at the core network and automatically download its configuration. The URL can be a simple file name or contain the device's MAC or IP address, e.g.:

- `http://corp.com/config-<MAC>.ini` - which becomes, for example, `http://corp.com/config-00908f030012.ini`
- `http://corp.com/<IP>/config.ini` - which becomes, for example, `http://corp.com/192.168.0.7/config.ini`

### 32.2.3 Configuration using FTP or NFS

Some networks block access to HTTP(S). The Automatic Update feature provides limited support for FTP/FTPS connectivity. Periodic polling for updates is not possible since these protocols don't support conditional fetching, i.e., updating files only if it is changed on the server.

The only difference between this method and those described in 'HTTP-based Automatic Updates' on page 330 is that the protocol in the URL is "ftp" (instead of "http").



**Notes:**

- Unlike FTP, NFS is not NAT-safe.
- NFS v2/v3 is also supported.



## 32.3 Loading Files Securely (Disabling TFTP)

The TFTP protocol is not considered secure and some network operators block it using a firewall. It is possible to disable TFTP completely, using the *ini* file parameter `EnableSecureStartup` (set to 1). This way, secure protocols such as HTTPS may be used to fetch the device configuration.

➤ **To download the ini file to the device using HTTPS instead of TFTP:**

1. Prepare the device's configuration file on an HTTPS server and obtain a URL to the file (e.g., `https://192.168.100.53/gateways.ini`).
2. Enable DHCP, if necessary.
3. Enable SSH and connect to it.
4. In the CLI, use the *ini* file parameters `IniFileURL` (for defining the URL of the configuration file) and `EnableSecureStartup` (for disabling TFTP), and then restart the device with the new configuration:

```
/conf/scp IniFileURL https://192.168.100.53/gateways.ini
/conf/scp EnableSecureStartup 1
/conf/sar bootp
```



**Note:** Once Secure Startup has been enabled, it can only be disabled by setting `EnableSecureStartup` to 0 using the CLI.

## 32.4 Remotely Triggering Auto Update using SIP NOTIFY

The device can be remotely triggered to start the Automatic Update process upon receipt of a SIP NOTIFY that includes an Event header set to 'check-sync;reboot=false', as shown in the example below:

```
NOTIFY sip:<user>@<dsthost> SIP/2.0
To: sip:<user>@<dsthost>
From: sip:sipsak@<srchost>
CSeq: 10 NOTIFY
Call-ID: 1234@<srchost>
Event: check-sync;reboot=false
```

For this feature to function, Automatic Update must be enabled on the device. In other words, it must have a loaded ini file with the Automatic Update settings.

➤ **To enable remote trigger of Auto Update upon receipt of SIP NOTIFY:**

1. Open the Advanced Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Advanced Parameters**).
2. Under the **Misc Parameters** group, set the 'SIP Remote Reset' parameter to **Enable**.
3. Click **Submit**.



**Note:** This SIP Event header value is proprietary to AudioCodes.



## 33 Restoring Factory Defaults

You can restore the device's configuration to factory defaults using one of the following methods:

- CLI (see "Restoring Defaults using CLI" on page 333)
- Loading an empty *ini* file (see "Restoring Defaults using an ini File" on page 334)

### 33.1 Restoring Defaults using CLI

The device can be restored to factory defaults using CLI, as described in the procedure below.

➤ **To restore factory defaults using CLI:**

1. Access the CLI:
  - a. Connect the RS-232 serial port of the device to the communication port on your computer. For serial cabling, refer to the *Hardware Installation Manual*.
  - b. Establish serial communication with the device using a serial communication program (such as HyperTerminal™) with the following communication port settings:
    - ◆ **Baud Rate:** 115,200 bps
    - ◆ **Data Bits:** 8
    - ◆ **Parity:** None
    - ◆ **Stop Bits:** 1
    - ◆ **Flow Control:** None
2. At the CLI prompt, type the username (default is "Admin" - case sensitive), and then press Enter:  
# Username: Admin
3. At the prompt, type the password (default is "Admin" - case sensitive), and then press Enter:  
# Password: Admin
4. At the prompt, type the following, and then press Enter:  
# enable
5. At the prompt, type the password again, and then press Enter:  
# Password: Admin
6. At the prompt, type the following to reset the device to default settings, and then press Enter:  
# write factory



## 33.2 Restoring Defaults using an ini File

You can restore the device to factory default settings by loading an empty *ini* file to the device. This is done using the Web interface's Configuration File page (see "Backing Up and Loading Configuration File" on page 324). If the *ini* file does include content (e.g., parameters), ensure that they are on lines beginning with comment signs (i.e., semicolons ";") so that the device ignores them.



**Note:** The only settings that are not restored to default are the management (OAMP) IP address and the Web interface's login user name and password.



# Part IX

## Status, Performance Monitoring and Reporting







## 34 System Status

This section describes how to view various system statuses.

### 34.1 Viewing Device Information

The Device Information page displays various hardware and software information of the device. This page also lists any Auxiliary files that have been installed on the device and allows you to remove them.

➤ **To access the Device Information page:**

- Open the Device Information page (**Status & Diagnostics** tab > **System Status** menu > **Device Information**).

▼ General Settings	
MAC Address:	e4115b12f386
Serial Number:	250763193545606
Board Type:	Mediant SW
Device Up Time:	7d:20h:23m:17s:90th
Device Administrative State:	Unlocked
Device Operational State:	Enabled
Flash Size [Mbytes]:	0
RAM Size [Mbytes]:	4294967118
CPU Speed [MHz]:	40
▼ Versions	
Version ID:	6.60A.012.006
DSP Type:	1
DSP Software Version:	66015
DSP Software Name:	5039AE3_R
Flash Version:	0
▼ Loaded Files	

➤ **To delete a loaded file:**

- Click the **Delete** button corresponding to the file that you want to delete. Deleting a file takes effect only after device reset (see "Resetting the Device" on page 305).



## 34.2 Viewing Ethernet Port Information

The Ethernet Port Information page displays read-only information on the Ethernet port connections. This includes information such as duplex mode and speed.



**Note:** The Ethernet Port Information page can also be accessed from the Home page (see "Viewing the Home Page" on page 44).

➤ **To view Ethernet port information:**

- Open the Ethernet Port Information page (**Status & Diagnostics** tab > **System Status** menu > **Ethernet Port Information**).

	Active	Speed	Duplex Mode	State	Group Member
1	Yes	1000 Mbp	Full Duplex	Forwarding	GROUP_1
2	Yes	100 Mbps	Half Duplex	Forwarding	GROUP_2

**Table 34-1: Ethernet Port Information Parameters**

Parameter	Description
Active	Displays whether the port is active ("Yes") or not ("No").
Speed	Displays the speed (in Mbps) of the Ethernet port.
Duplex Mode	Displays whether the port is half- or full-duplex
State	Displays the state of the port: <ul style="list-style-type: none"> <li>▪ "Forwarding": Active port (data is being received and sent)</li> <li>▪ "Disabled": Redundancy port</li> </ul>
Group Member	Displays the port-pair group ID to which the port belongs.



## 35 Carrier-Grade Alarms

This section describes how to view the following types of alarms:

- Active alarms - see "Viewing Active Alarms" on page 339
- Alarm history - see "Viewing Alarm History" on page 339

### 35.1 Viewing Active Alarms

The Active Alarms page displays a list of currently active alarms. You can also access this page from the Home page (see "Viewing the Home Page" on page 44).

➤ **To view the list of active alarms:**

- Open the Active Alarms page (**Status & Diagnostics** tab > **System Status** menu > **Carrier-Grade Alarms** > **Active Alarms**).

For each alarm, the following information is provided:

- **Severity:** severity level of the alarm:
  - Critical (red)
  - Major (orange)
  - Minor (yellow)
- **Source:** unit from which the alarm was raised
- **Description:** brief explanation of the alarm
- **Date:** date and time that the alarm was generated

You can view the next 20 alarms (if exist), by clicking the **Go to page** button.

### 35.2 Viewing Alarm History

The Alarms History page displays a list of alarms that have been raised and traps that have been cleared.

➤ **To view the list of history alarms:**

- Open the Alarms History page (**Status & Diagnostics** tab > **System Status** menu > **Carrier-Grade Alarms** > **Alarms History**).

Sequential number	Severity	Source	Description	Date
1	Major	Board#1	Controller failure alarm Proxy Set 0: Proxy lost. looking for another proxy	6.1.2010 , 14:1:26
2	Cleared	Board#1	Alarm cleared: Controller failure alarm Proxy Set 0: Proxy lost. looking for another proxy	6.1.2010 , 14:1:26
3	Major	Board#1	Controller failure alarm Proxy Set ID 0	6.1.2010 , 14:1:26
4	Major	Board#1/WanLink#1	WAN link alarm. FE interface 1 is down.	6.1.2010 , 14:1:29
5	Minor	Board#1/EthernetLink#2	Ethernet link alarm. LAN port number 2 is down.	6.1.2010 , 14:1:29
6	Major	Board#1	NTP server alarm. No connection to NTP server.	6.1.2010 , 14:11:14

For each alarm, the following information is provided:

- **Severity:** severity level of the alarm:
  - Critical (red)
  - Major (orange)
  - Minor (yellow)
  - Cleared (green)



- **Source:** unit from which the alarm was raised
- **Description:** brief explanation of the alarm
- **Date:** date and time that the alarm was generated

You can view the next 20 alarms (if exist), by clicking the **Go to page** button.

➤ **To delete all the alarms in the table:**

1. Click the **Delete History Table** button; a confirmation message box appears.
2. Click **OK** to confirm.



## 36 Performance Monitoring

This section describes how to view performance monitoring.

### 36.1 Viewing MOS per Media Realm

The MOS Per Media Realm page displays statistics on Media Realms (configured in "Configuring Media Realms" on page 130). This page provides two graphs:

- Upper graph: displays the Mean Opinion Score (MOS) quality in RTCP data per selected Media Realm.
- Lower graph: displays the bandwidth of transmitted media (in Kbps) in RTCP data per Media Realm.



➤ To view the MOS per Media Realm graph:

1. Open the MOS Per Media Realm page (**Status & Diagnostics** tab > **Performance Monitoring** menu > **MOS Per Media Realm**).

Figure 36-1: MOS Per Media Realm Graph



2. From the 'Media Realm' drop-down list, select the Media Realm for which you want to view.

Use the **Zoom In**  button to increase the displayed time resolution or the **Zoom Out**  button to decrease it. Instead of using these zoom buttons, you can use the slide ruler. As you increase the resolution, more data is displayed on the graph. The minimum resolution is about 30 seconds; the maximum resolution is about an hour.

To pause the graph, click the **Pause** button; click **Play** to resume.



## 36.2 Viewing Quality of Experience

The Quality Of Experience page provides statistical information on calls per SRD or IP Group. The statistics can be further filtered to display incoming and/or outgoing call direction, and type of SIP dialog (INVITE, SUBSCRIBE, or all).

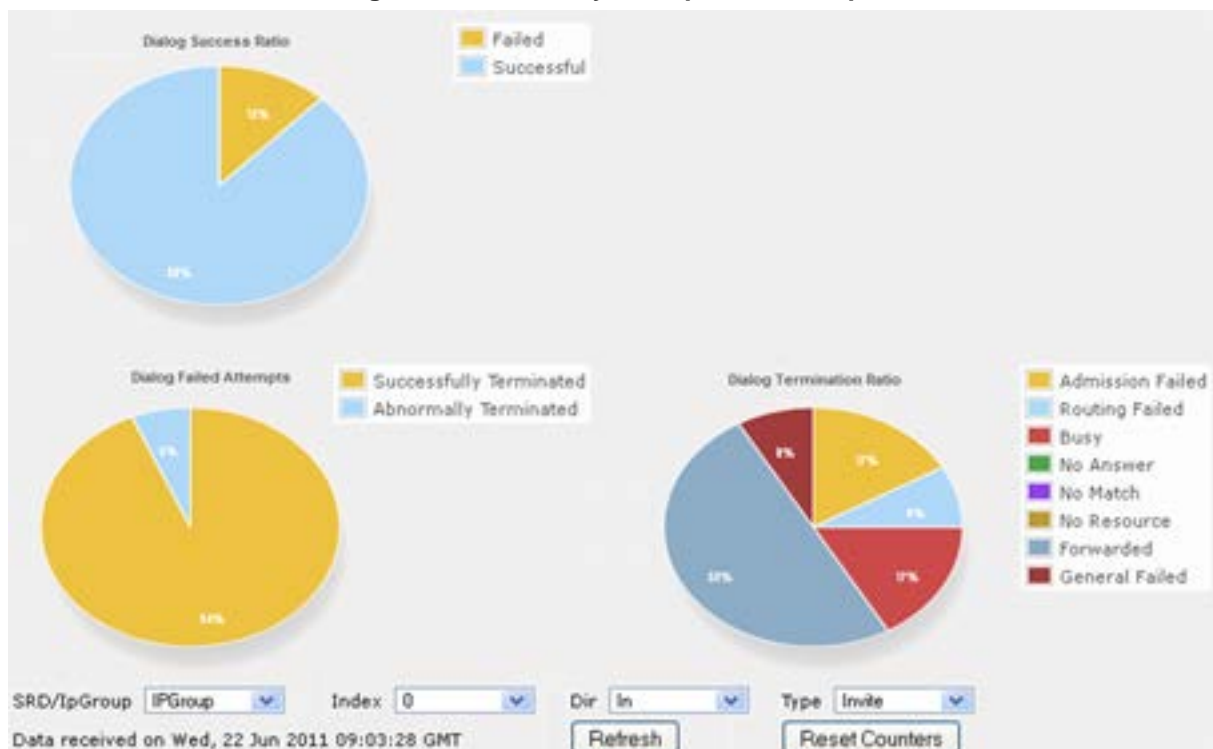
This page provides three pie charts:

- Dialog Success Ratio: displays the SIP call and subscribe (SUBSCRIBE) dialog success-failed ratio.
- Dialog Failed Attempts: displays the failed call attempts. This includes the number of calls and subscribes which were successfully and abnormally terminated.
- Dialog Termination Ratio: displays call termination by reason (e.g., due to no answer).

➤ **To view Quality of Experience:**

1. Open the Quality Of Experience page (**Status & Diagnostics** tab > **Performance Monitoring** menu > **Quality Of Experience**).

**Figure 36-2: Quality Of Experience Graph**



2. From the 'SRD/IpGroup' drop-down list, select whether you want to view QoE for an SRD or IP Group.
3. From the 'Index' drop-down list, select the SRD or IP Group index.
4. From the 'Dir' drop-down list, select the call direction:
  - **In** - incoming calls
  - **Out** - outgoing calls
  - **Both** - incoming and outgoing calls
5. From the 'Type' drop-down list, select the SIP message type:
  - **Invite** - INVITE
  - **Subscribe** - SUBSCRIBE
  - **Other** - all SIP messages

To refresh the charts, click **Refresh**. To reset the counters, click **Reset Counters**.



### 36.3 Viewing Average Call Duration

The Average Call Duration page displays information about a specific SRD or IP Group. This page includes two graphs:

- Upper graph: displays the number of calls (INVITEs).
- Lower graph: displays the average call duration.



➤ **To view average call duration:**

1. Open the Average Call Duration page (**Status & Diagnostics** tab > **Performance Monitoring** menu > **Average Call Duration**).

**Figure 36-3: Average Call Duration Graph**



2. From the 'SRD/IpGroup' drop-down list, select whether you want to view information for an SRD or IP Group.
3. From the 'Index' drop-down list, select the SRD or IP Group index.

Use the **Zoom In**  button to increase the displayed time resolution or the **Zoom Out**  button to decrease it. Instead of using these zoom buttons, you can use the slide ruler. As you increase the resolution, more data is displayed on the graph. The minimum resolution is about 30 seconds; the maximum resolution is about an hour.

To pause the graph, click the **Pause** button; click **Play** to resume.



## Reader's Notes



## 37 VoIP Status

This section describes how to view VoIP status and statistics.

### 37.1 Viewing Active IP Interfaces

The IP Interface Status page displays the device's active IP interfaces that are listed in the Multiple Interface Table page (see "Configuring IP Network Interfaces" on page 90).

➤ **To view the active IP network interfaces:**

- Open the IP Interface Status page (**Status & Diagnostics** tab > **VoIP Status** menu > **IP Interface Status**).

**Figure 37-1: IP Interface Status Page**

Index	Application Type	Address Type	Interface Mode	IP Address	Prefix Length	Gateway	VLAN ID	Interface Name
1	Maintenance	IPv4	IPv4 Manual	10.66.33.44	16	10.66.0.1	25	HA
0	O-M-C	IPv4	IPv4 Manual	10.3.50.40	16	10.3.0.1	1	O-M-C
2	Media	IPv4	IPv4 Manual	10.11.50.40	16	0.0.0.0	11	Media1
3	Media	IPv4	IPv4 Manual	10.13.50.40	16	0.0.0.0	13	Media2
4	Media	IPv4	IPv4 Manual	10.15.50.40	16	0.0.0.0	15	Media3
5	Media	IPv4	IPv4 Manual	10.12.50.40	16	0.0.0.0	112	Media4
6	Media	IPv4	IPv4 Manual	10.14.50.40	16	0.0.0.0	114	Media5

### 37.2 Viewing Registered Users

The SAS/SBC Registered Users page displays a list of registered SASSBC users recorded in the device's database.

➤ **To view registered SASSBC users:**

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

**Figure 37-2: SAS/SBC Registered Users Page**

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

**Table 37-1: SAS/SBC Registered Users Parameters**

Column Name	Description
<b>Address of Record</b>	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.
<b>Contact</b>	SIP URI that can be used to contact that specific instance of the User Agent for subsequent requests.



## Reader's Notes



## 38 Reporting Information to External Party

This section describes features for reporting various information to an external party.

### 38.1 RTP Control Protocol Extended Reports (RTCP XR)

RTP Control Protocol Extended Reports (RTCP XR) is a VoIP management control that defines a set of metrics containing information for assessing VoIP call quality and for diagnosing problems. RTCP XR (RFC 3611) extends the RTCP reports defined in RFC 3550 by providing additional VoIP metrics. RTCP XR information publishing is implemented in the device according to <draft-johnston-sipping-rtcp-summary-07>. This draft defines how a SIP User Agent (UA) publishes the detailed information to a defined collector. RTCP XR measures VoIP call quality such as packet loss, delay, signal / noise / echo levels, estimated R-factor, and mean opinion score (MOS). RTCP XR measures these parameters using metrics as listed in the table below.



**Note:** RTCP XR is a customer ordered feature and thus, must be included in the Software License Key installed on the device.

RTCP XR messages containing key call-quality-related metrics are exchanged periodically (user-defined) between the device and the SIP UA. This allows an analyzer to monitor these metrics midstream, or a device to retrieve them using SNMP. The device can send RTCP XR reports to an Event State Compositor (ESC) server using PUBLISH messages. These reports can be sent at the end of each call and according to a user-defined interval between consecutive reports.

**Table 38-1: RTCP XR Published VoIP Metrics**

Group	Metric Name
<b>General</b>	Start Timestamp
	Stop Timestamp
	Call-ID
	Local Address (IP, Port & SSRC)
	Remote Address (IP, Port & SSRC)
<b>Session Description</b>	Payload Type
	Payload Description
	Sample Rate
	Frame Duration
	Frame Octets
	Frames per Packets
	Packet Loss Concealment
	Silence Suppression State
<b>Jitter Buffer</b>	Jitter Buffer Adaptive
	Jitter Buffer Rate



Group	Metric Name
	Jitter Buffer Nominal
	Jitter Buffer Max
	Jitter Buffer Abs Max
<b>Packet Loss</b>	Network Packet Loss Rate
	Jitter Buffer Discard Rate
<b>Burst Gap Loss</b>	Burst Loss Density
	Burst Duration
	Gap Loss Density
	Gap Duration
	Minimum Gap Threshold
<b>Delay</b>	Round Trip Delay
	End System Delay
	One Way Delay
	Interarrival Jitter
	Min Absolute Jitter
	Signal
	Signal Level
	Noise Level
	Residual Echo Return Noise
<b>Quality Estimates</b>	Listening Quality R
	RLQ Est. Algorithm
	Conversational Quality R
	RCQ Est. Algorithm
	External R In
	Ext. R In Est. Algorithm
	External R Out
	Ext. R Out Est. Algorithm
	MOS-LQ
	MOS-LQ Est. Algorithm
	MOS-CQ
	MOS-CQ Est. Algorithm
	QoE Est. Algorithm



➤ **To configure RTCP XR:**

1. Open the RTP/RTCP Settings page (**Configuration** tab > **VoIP** menu > **Media** > **RTP/RTCP Settings**). The RTCP XR parameters are listed under the 'RTCP XR Settings' group, as shown below:

**Figure 38-1: RTCP XR Parameters in RTP/RTCP Settings Page**

▼ RTCP XR Settings	
Burst Threshold	-1
Delay Threshold	-1
R-Value Delay Threshold	-1
⚡ Enable RTCP XR	CE_VQMON_DISABLE ▼
Minimum Gap Size	16
RTCP XR Report Mode	Disable ▼
RTCP XR Packet Interval	0
Disable RTCP XR Interval Randomization	Disable ▼
RTCP XR Collection Server	
RTCP XR Collection Server Transport Type	Not Configured ▼

2. Configure the RTCP XR parameters, as required:
  - 'Enable RTCP XR' (*VQMonEnable*) - enables voice quality monitoring and RTCP XR.
  - 'Minimum Gap Size' (*VQMonGMin*) - defines the voice quality monitoring - minimum gap size (number of frames).
  - 'Burst Threshold' (*VQMonBurstTHR*) - defines the voice quality monitoring - excessive burst alert threshold.
  - 'Delay Threshold' (*VQMonDelayTHR*) - defines the voice quality monitoring - excessive delay alert threshold.
  - 'R-Value Delay Threshold' (*VQMonEOCRValTHR*) - defines the voice quality monitoring - end of call low quality alert threshold.
  - 'RTCP XR Report Mode' (*RTCPXRReportMode*) - determines whether RTCP XR reports are sent to the ESC and defines the interval in which they are sent.
  - 'RTCP XR Packet Interval' (*RTCPInterval*) - defines the time interval between adjacent RTCP reports.
  - 'Disable RTCP XR Interval Randomization' (*DisableRTCPRandomize*) - determines whether RTCP report intervals are randomized or whether each report interval accords exactly to the parameter RTCPInterval.
  - 'RTCP XR Collection Server' (*RTCPXREscIP*) - defines the IP address of the Event State Compositor (ESC).
  - 'RTCP XR Collection Server Transport Type' (*RTCPXRESCTransportType*) - determines the transport layer for outgoing SIP dialogs initiated by the device to the RTCP XR Collection Server.
3. Click **Submit**.
4. Reset the device for the settings to take effect.



## 38.2 Generating Call Detail Records

The Call Detail Record (CDR) contains vital statistic information on calls made from the device. The device can be configured to generate and report CDRs for various stages of the call, including SIP messages and/or media. You can configure when CDRs for a call are generated, for example, only at the end of the call or only at the start and end of the call. Once generated, the device sends the CDRs to a user-defined Syslog server.

The CDR Syslog message complies with RFC 3161 and is identified by Facility 17 (local1) and Severity 6 (Informational).

For CDR in RADIUS format, see "Configuring RADIUS Accounting" on page 354.

### 38.2.1 Configuring CDR Reporting

The procedure below describes how to configure CDR reporting.

➤ **To configure CDR reporting:**

1. Enable the Syslog feature for sending log messages generated by the device to a collecting log message server. For more information, see "Configuring Syslog" on page 365.
2. Open the Advanced Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** > **Advanced Parameters**). The CDR parameters appear under the 'CDR and Debug' group, as shown below:

**Figure 38-2: CDR Parameters in Advanced Parameters Page**

▼ CDR and Debug	
CDR Server IP Address	10.8.6.55
CDR Report Level	Start & End & Connect Call ▼
Media CDR Report Level	End Media ▼

3. Configure the parameters as required. For a description of the parameters, see "Syslog, CDR and Debug Parameters" on page 402.
4. Click **Submit**.



**Note:** If the CDR server IP address is not configured, the CDRs are sent to the Syslog server, configured in "Configuring Syslog" on page 365.



## 38.2.2 CDR Field Description

This section describes the CDR fields that are generated by the device.

### 38.2.2.1 CDR Fields for SBC Signaling

The CDR fields for SBC signaling are listed in the table below. The signaling CDRs are published for each SBC leg.

**Table 38-2: CDR Fields for SBC Signaling**

CDR Field Name	Description
<b>SBCReportType</b>	Report Type: <ul style="list-style-type: none"> <li>▪ <b>CALL_START</b></li> <li>▪ <b>CALL_CONNECT</b></li> <li>▪ <b>CALL_END</b></li> <li>▪ <b>DIALOG_START</b></li> <li>▪ <b>DIALOG_END</b></li> </ul>
<b>EPTyp</b>	Endpoint type ( <b>SBC</b> )
<b>SIPMethod</b>	SIP message type
<b>SIPCallId</b>	Unique ID of call
<b>SessionId</b>	Unique Session ID
<b>Orig</b>	Call originator: <ul style="list-style-type: none"> <li>▪ <b>LCL</b> - for local</li> <li>▪ <b>RMT</b> - for remote</li> </ul>
<b>SourceIp</b>	Source IP address
<b>SourcePort</b>	Source UDP port
<b>DestIp</b>	Destination IP address
<b>DestPort</b>	Destination UDP port
<b>TransportType</b>	Transport type: <ul style="list-style-type: none"> <li>▪ <b>UDP</b></li> <li>▪ <b>TCP</b></li> <li>▪ <b>TLS</b></li> </ul>
<b>SrcURI</b>	Source URI
<b>SrcURIBeforeMap</b>	Source URI before manipulation
<b>DstURI</b>	Destination URI
<b>DstURIBeforeMap</b>	Destination URI before manipulation
<b>Durat</b>	Call duration
<b>TrmSd</b>	Termination side (local or remote)
<b>TrmReason</b>	Termination reason



CDR Field Name	Description
<b>TrmReasonCategory</b>	Termination reason category: <ul style="list-style-type: none"> <li>Calls with duration 0 (i.e., not connected): <ul style="list-style-type: none"> <li>✓ <b>NO_ANSWER</b> - GWAPP_NORMAL_CALL_CLEAR, GWAPP_NO_USER_RESPONDING, GWAPP_NO_ANSWER_FROM_USER_ALERTED</li> <li>✓ <b>BUSY</b> - GWAPP_USER_BUSY</li> <li>✓ <b>NO_RESOURCES</b> - GWAPP_RESOURCE_UNAVAILABLE_UNSPECIFIED, RELEASE_BECAUSE_NO_CONFERENCE_RESOURCES_LEFT, RESOURCE_BECAUSE_NO_TRANSCODING_RESOURCES_LEFT, RELEASE_BECAUSE_GW_LOCKED</li> <li>✓ <b>NO_MATCH</b> - RELEASE_BECAUSE_UNMATCHED_CAPABILITIES</li> <li>✓ <b>FORWARDED</b> - RELEASE_BECAUSE_FORWARD</li> <li>✓ <b>GENERAL_FAILED</b> - any other reason</li> </ul> </li> <li>Calls with duration: <ul style="list-style-type: none"> <li>✓ <b>NORMAL_CALL_CLEAR</b> - GWAPP_NORMAL_CALL_CLEAR</li> <li>✓ <b>ABNORMALLY_TERMINATED</b> - Anything else</li> </ul> </li> <li><b>N/A</b> - Reasons not belonging to above categories</li> </ul>
<b>SetupTime</b>	Call setup time
<b>ConnectTime</b>	Call connect time
<b>ReleaseTime</b>	Call release time
<b>RedirectReason</b>	Redirect reason
<b>RedirectURINum</b>	Redirection URI
<b>RedirectURINumBeforeManip</b>	Redirect URI number before manipulation
<b>TxSigIPDiffServ</b>	Signaling IP DiffServ
<b>IPGroup</b>	IP Group description
<b>SrdId</b>	SRD name
<b>SIPInterfaceId</b>	SIP Interface ID
<b>ProxySetId</b>	Proxy Set ID
<b>IpProfileId</b>	IP Profile name
<b>MediaRealmId</b>	Media Realm name
<b>DirectMedia</b>	Direct media or traversing SBC: <ul style="list-style-type: none"> <li>yes</li> <li>no</li> </ul>
<b>SIPTrmReason</b>	SIP call termination reason (BYE, CANCEL, or SIP error codes, e.g., 404)
<b>SipTermDesc</b>	Description of SIP termination reason: <ul style="list-style-type: none"> <li>SIP Reason header, if exists, for example: SIP ;cause=200 ;text="Call completed elsewhere".</li> <li>If no SIP Reason header exists, the description is taken from the reason text, if exists, of the SIP response code, for example: "417 Unknown Resource-Priority".</li> <li>If no reason text exists in the SIP response code, the description is</li> </ul>



CDR Field Name	Description
	taken from an internal SIP response mapping mechanism. For example, if the device receives a SIP response "422", it sends in the CDR "422 Session Interval Too Small method" as the description.

An example of an SBC signaling CDR sent by the device is shown below:

```
[S=1] |SBCReportType |EPTyp| SIPCallId| SessionId |Orig |SourceIp
|SourcePort |DestIp |DestPort |TransportType |SrcURI
|SrcURIBeforeMap |DstURI |DstURIBeforeMap |Durat |TrmSd |TrmReason
|TrmReasonCategory |SetupTime |ConnectTime |ReleaseTime
|RedirectReason |RedirectURINum |RedirectURINumBeforeMap
|TxSigIPDiffServ |IPGroup (description) |SrdId (name)
|SIPInterfaceId |ProxySetId |IpProfileId (name) |MediaRealmId
(name) |DirectMedia |SIPTrmReason
[S=3] |CALL_END |SBC |170369730753201211288@10.132.10.245 |0 |RMT
|10.132.10.245 |5060 |10.132.10.250 |5070 |UDP |103@audiocodes.com
|103@audiocodes.com |101@10.132.10.250 |101@10.132.10.250 |0 |RMT
|GWAPP_NORMAL_CALL_CLEAR |NO_ANSWER |06:13:54.950 UTC Thu Mar 02
2012 |06:14:01.175 UTC Thu Mar 02 2012 |-1 | |40 |2 () |0
(5070SRD) |2 |3 |0 () |0 (lanmedia) |no |CANCEL
```

### 38.2.2.2 CDR Fields for SBC Media

The CDR fields for SBC media are listed in the table below. The media CDRs are published for each active media stream, thereby allowing multiple media CDRs, where each media CDR has a unique call ID corresponding to the signaling CDR.

**Table 38-3: CDR Fields for SBC Media**

CDR Field Name	Description
<b>MediaReportType</b>	Report type (media start, update, or end)
<b>SIPCallId</b>	Unique call ID
<b>Cid</b>	Channel CID
<b>MediaType</b>	Media type (audio, video, or text)
<b>Coder</b>	Coder name
<b>PacketInterval</b>	Coder packet interval
<b>LocalRtpIp</b>	Local RTP IP address
<b>LocalRtpPort</b>	Local RTP port
<b>RemoteRtpIp</b>	Remote RTP IP address
<b>RemoteRtpPort</b>	Remote RTP port
<b>InPackets</b>	Number of received packets
<b>OutPackets</b>	Number of sent packets
<b>LocalPackLoss</b>	Local packet loss
<b>RemotePackLoss</b>	Remote packet loss
<b>RTPdelay</b>	RTP delay



CDR Field Name	Description
RTPjitter	RTP jitter
TxRTPssrc	Tx RTP SSRC
RxRTPssrc	Local RTP SSRC
LocalRFactor	Local conversation quality
RemoteRFactor	Remote conversation quality
LocalMosCQ	Local MOS for conversation
RemoteMosCQ	Remote MOS for conversation
TxRTPIPDiffServ	Media IP DiffServ
LatchedRtplp	Remote IP address of the incoming RTP stream that the device "latched" on to as a result of the RTP latching mechanism for NAT traversal.
LatchedRtpPort	Remote RTP port of the incoming RTP stream that the device "latched" on to as a result of the RTP latching mechanism for NAT traversal.

## 38.3 Configuring RADIUS Accounting

The the RADIUS Parameters page allows you to enable RADIUS accounting of SIP calls by a RADIUS accounting server. The device can send the accounting messages to the RADIUS server upon call release, call connection and release, or call setup and release.



### Notes:

- For RADIUS accounting settings to take effect, you must save the settings to flash memory with a device reset.
- For a description of the RADIUS accounting parameters, see "RADIUS Parameters" on page 416.

### ➤ To configure RADIUS accounting:

1. Open the RADIUS Parameters page (**Configuration** tab > **VoIP** menu > **SIP Definitions** submenu > **RADIUS Parameters Settings**).

**Figure 38-3: RADIUS Accounting Parameters Page**

⚡ Enable RADIUS Access Control	Enable	▼
Accounting Server IP Address	0.0.0.0	
Accounting Port	1646	
RADIUS Accounting Type	At Call Release	▼
AAA Indications	None	▼

2. Configure the parameters as required.
3. Click **Submit**.
4. Reset the device with a burn to flash for the settings to take effect.



The table below describes the RADIUS Accounting CDR attributes included in the communication packets transmitted between the device and a RADIUS server.

**Table 38-4: Supported RADIUS Accounting CDR Attributes**

Attribute Number	Attribute Name	Vendor Specific Attribute (VSA) No.	Purpose	Value Format	Example	AAA
<b>Request Attributes</b>						
1	user-name	-	Account number or calling party number or blank	String up to 15 digits long	5421385747	Start Acc Stop Acc
4	nas-ip-address	-	IP address of the requesting device	Numeric	192.168.14.43	Start Acc Stop Acc
6	service-type	-	Type of service requested	Numeric	1: login	Start Acc Stop Acc
26	h323-incoming-conf-id	1	SIP call identifier	Up to 32 octets	-	Start Acc Stop Acc
26	h323-remote-address	23	IP address of the remote gateway	Numeric	-	Stop Acc
26	h323-conf-id	24	H.323/SIP call identifier	Up to 32 octets	-	Start Acc Stop Acc
26	h323-setup-time	25	Setup time in NTP format 1	String	-	Start Acc Stop Acc
26	h323-call-origin	26	The call's originator: Answering (IP) or Originator (PSTN)	String	Answer, Originate etc	Start Acc Stop Acc
26	h323-call-type	27	Protocol type or family used on this leg of the call	String	VoIP	Start Acc Stop Acc
26	h323-connect-time	28	Connect time in NTP format	String	-	Stop Acc
26	h323-disconnect-time	29	Disconnect time in NTP format	String	-	Stop Acc
26	H323-Disconnect-Cause	30	Q.931 disconnect cause code	Numeric	-	Stop Acc
26	h323-gw-id	33	Name of the gateway	String	SIPIDString	Start Acc Stop Acc
26	sip-call-id	34	SIP Call ID	String	abcde@ac.com	Start Acc Stop Acc
26	call-terminator	35	The call's terminator: PSTN-terminated call (Yes); IP-terminated call (No).	String	Yes, No	Stop Acc



Attribute Number	Attribute Name	Vendor Specific Attribute (VSA) No.	Purpose	Value Format	Example	AAA
30	called-station-id	-	Destination URI	String	8004567145	Start Acc
31	calling-station-id	-	Source URI	String	5135672127	Start Acc Stop Acc
40	acct-status-type	-	Account Request Type (start or stop) <b>Note:</b> 'start' isn't supported on the Calling Card application.	Numeric	1: start, 2: stop	Start Acc Stop Acc
41	acct-delay-time	-	No. of seconds tried in sending a particular record	Numeric	5	Start Acc Stop Acc
44	acct-session-id	-	A unique accounting identifier - match start & stop	String	34832	Start Acc Stop Acc
46	acct-session-time	-	For how many seconds the user received the service	Numeric	-	Stop Acc
47	acct-input-packets	-	Number of packets received during the call	Numeric	-	Stop Acc
48	acct-output-packets	-	Number of packets sent during the call	Numeric	-	Stop Acc
61	nas-port-type	-	Physical port type of device on which the call is active	String	0: Asynchronous	Start Acc Stop Acc
<b>Response Attributes</b>						
26	h323-return-code	103	The reason for failing authentication (0 = ok, other number failed)	Numeric	0 Request accepted	Stop Acc
44	acct-session-id	-	A unique accounting identifier – match start & stop	String	-	Stop Acc

Below is an example of RADIUS Accounting, where the non-standard parameters are preceded with brackets:

```
Accounting-Request (361)
user-name = 111
acct-session-id = 1
nas-ip-address = 212.179.22.213
nas-port-type = 0
acct-status-type = 2

acct-session-time = 1
acct-input-packets = 122
```



```
acct-output-packets = 220
called-station-id = 201
calling-station-id = 202
// Accounting non-standard parameters:
(4923 33) h323-gw-id =
(4923 23) h323-remote-address = 212.179.22.214
(4923 1) h323-ivr-out = h323-incoming-conf-id:02102944 600a1899
3fd61009 0e2f3cc5
(4923 30) h323-disconnect-cause = 22 (0x16)
(4923 27) h323-call-type = VOIP
(4923 26) h323-call-origin = Originate
(4923 24) h323-conf-id = 02102944 600a1899 3fd61009 0e2f3cc5
```



## Reader's Notes



# Part X

## Diagnostics







## 39 Syslog and Debug Recordings

Syslog is an event notification protocol that enables a device to send event notification messages across IP networks to event message collectors, also known as Syslog servers. The device contains an embedded Syslog client, which sends error reports / events that it generates to a remote Syslog server using the IP / UDP protocol. This information is a collection of error, warning, and system messages that records every internal operation of the device.

For receiving Syslog messages generated by the device, you can use any of the following Syslog servers:

- **Device's embedded Syslog server:** The device provides an embedded Syslog server, which is accessed through the Web interface. This provides limited Syslog server functionality.
- **Wireshark:** Third-party network protocol analyzer (<http://www.wireshark.org>).
- **Third-party, Syslog server:** Any third-party Syslog server program that enables filtering of messages according to parameters such as priority, IP sender address, time, and date.

### 39.1 Syslog Message Format

The Syslog message is sent from the device to a Syslog server as an ASCII (American Standard Code for Information Interchange) message. Syslog uses UDP as its underlying transport layer mechanism. By default, UDP port 514 is assigned to Syslog, but this can be changed (see "Configuring Syslog" on page 365).

Below is an example of a Syslog message:

```
13:10:57.811 : 10.13.4.12 : NOTICE : [S=235][SID:1034099026] (
lgr_flow)(63) UdpTransportObject#0- Adding socket event
for address 10.33.2.42:5060 [Time: 04-19-2012@18:29:39]
```

**Table 39-1: Syslog Message Format Description**

Message Item	Description
<b>Message Types</b>	<p>Syslog generates the following types of messages:</p> <ul style="list-style-type: none"> <li>■ <b>ERROR:</b> Indicates that a problem has been identified that requires immediate handling.</li> <li>■ <b>WARNING:</b> Indicates an error that might occur if measures are not taken to prevent it.</li> <li>■ <b>NOTICE:</b> Indicates that an unusual event has occurred.</li> <li>■ <b>INFO:</b> Indicates an operational message.</li> <li>■ <b>DEBUG:</b> Messages used for debugging.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>■ The INFO and DEBUG messages are required only for advanced debugging. Therefore, by default, they are not sent by the device.</li> <li>■ When viewing Syslog messages in the Web interface, these message types are color coded.</li> </ul>
<b>Message Sequence Number [S=&lt;number&gt;]</b>	<p>Syslog messages are sequentially numbered in the format [S=&lt;number&gt;], for example, "[S=643]".</p> <p>A skip in the number sequence of messages indicates a loss of message packets. For example, in the below Syslog message generation, messages 238 through 300 were not received. In other words, three Syslog messages were lost</p>



Message Item	Description
	<p>(the sequential numbers are indicated below in bold font):</p> <pre> 18:38:14. 52 : 10.33.45.72 : NOTICE: [S=<b>235</b>][SID:1034099026] (lgr_psbrdex)(619) recv &lt;-- DIGIT(0) Ch:0 OnTime:0 InterTime:100 Direction:0 System:1 [File: Line:-1] 18:38:14. 83 : 10.33.45.72 : NOTICE: [S=<b>236</b>][SID:1034099026] (lgr_flow)(620) #0:DIGIT_EV [File: Line:-1] 18:38:14. 83 : 10.33.45.72 : NOTICE: [S=<b>237</b>][SID:1034099026] (lgr_flow)(621)   #0:DIGIT_EV [File: Line:-1] 18:38:14.958 : 10.33.45.72 : NOTICE: [S=<b>301</b>][SID:1034099026] (lgr_flow)(625)   #0:DIGIT_EV [File: Line:-1] </pre>
<b>Log Number (lgr)(number)</b>	Ignore this number; it has been replaced by the Message Sequence Number (described previously).
<b>Session ID</b>	<p>Automatically assigned (random), unique session identifier (session-id / SID) number per call in the CDR of sent Syslog messages and debug recording packets. This enables you to filter the information (such as SIP, Syslog, and media) according to the SID.</p> <ul style="list-style-type: none"> <li>SBC application: A session is considered as both the outgoing and incoming legs, where both legs share the same SID.</li> </ul> <p>The benefit of this unique numbering is that it enables you to filter the information (such as SIP, Syslog, and media) according to a specific SID.</p> <p><b>Note:</b> Forked legs and alternative legs share the same SID.</p>
<b>Message Body</b>	Describes the message.
<b>Timestamp</b>	When the Network Time Protocol (NTP) is enabled, a timestamp string [ <b>hour</b> :minutes:seconds] is added to all Syslog messages.

### 39.1.1 Event Representation in Syslog Messages

The Syslog message events that the device sends are represented by unique abbreviations. An example of an abbreviated event in a Syslog message indicating packet loss (PL) is shown below:

```
Apr 4 12:00:12 172.30.1.14 PL:5 [Code:3a002] [CID:3294] [Time:
20:17:00]
```

The table below lists these unique event abbreviations:

**Table 39-2: Syslog Error Name Descriptions**

Error Abbreviation	Error Name Description
<b>AA</b>	Invalid Accumulated Packets Counter
<b>AC</b>	Invalid Channel ID
<b>AL</b>	Invalid Header Length



Error Abbreviation	Error Name Description
AO	Invalid Codec Type
AP	Unknown Aggregation Payload Type
AR	Invalid Routing Flag Received
AT	Simple Aggregation Packets Lost
CC	Command Checksum Error
CE	Invalid Cell Coder Code
CS	Command Sequence Error
ES	8 sec Timeout Before Disconnect
HO	Host Received Overrun
IA	Invalid AMR Payload
IC	Invalid CID Error
IG	Invalid G723 Code
IP	Invalid payload length
IR	Invalid RTCP Packet
IS	Invalid SID Length
LC	Transmitter Received Illegal Command
LF	Lost Fax Frames In High Speed Mode
LM	Lost Modem Frames In High Speed Mode
MI	Misalignment Error
MR	Modem Relay Is Not Supported
OR	DSP JB Overrun
PH	Packet Header Error
PL	RTP Packet Loss
RB	Counts the number of BFI Frames Received From The Host
RD	No Available Release Descriptor
RO	RTP Reorder
RP	Unknown RTP Payload Type
RS	RTP SSRC Error
UF	Unrecognized Fax Relay Command
AA	Invalid Accumulated Packets Counter
AC	Invalid Channel ID
AL	Invalid Header Length
AO	Invalid Codec Type
AP	Unknown Aggregation Payload Type
AR	Invalid Routing Flag Received



### 39.1.2 Identifying AudioCodes Syslog Messages using Facility Levels

The device's Syslog messages can easily be identified and distinguished from Syslog messages from other equipment, by setting its Facility level. The Facility levels of the device's Syslog messages are numerically coded with decimal values. Facility level may use any of the "local use" facilities (0 through 7), according to RFC 3164. Implementing Facility levels is useful, for example, if you collect the device's as well as other equipments' Syslog messages on the same server. Therefore, in addition to filtering Syslog messages according to IP address, the messages can be filtered according to Facility level.

The Facility level is configured using the SyslogFacility ini file parameter, which provides the following options:

**Table 39-3: Syslog Facility Levels**

Numerical Value	Facility Level
<b>16 (default)</b>	local use 0 (local0)
<b>17</b>	local use 1 (local1)
<b>18</b>	local use 2 (local2)
<b>19</b>	local use 3 (local3)
<b>20</b>	local use 4 (local4)
<b>21</b>	local use 5 (local5)
<b>22</b>	local use 6 (local6)
<b>23</b>	local use 7 (local7)

Syslog messages begin with a less-than (" $<$ ") character, followed by a number, which is followed by a greater-than (" $>$ ") character. This is optionally followed by a single ASCII space. The number is known as the *Priority* and represents both the Facility level and the Severity level. A Syslog message with Facility level 16 is shown below:

```
Facility: LOCAL0 - reserved for local use (16)
```

### 39.1.3 SNMP Alarms in Syslog Messages

SNMP alerts are sent to the Syslog server using the following formats:

- **Raised Alarms:** RAISE-ALARM: <Alarm Name>; Textual Description: <Textual Description>; Severity <Alarm Severity>; Source <Alarm Source>; Unique ID: <Alarm Unique ID >.

If additional information exists in the alarm, then these are also added: Additional Info1:/ Additional Info2:/ Additional Info3

The Messages' Severity is as follows:

**Table 39-4: Syslog Message Severity**

ITU Perceived Severity (SNMP Alarm's Severity)	AudioCodes' Syslog Severity
<b>Critical</b>	RecoverableMsg
<b>Major</b>	RecoverableMsg
<b>Minor</b>	RecoverableMsg
<b>Warning</b>	Notice



ITU Perceived Severity (SNMP Alarm's Severity)	AudioCodes' Syslog Severity
Indeterminate	Notice
Cleared	Notice

- **Cleared Alarms:** CLEAR-ALARM: <Alarm Name>; Textual Description: <Textual Description>; Severity <Alarm Severity>; Source <Alarm Source>; Unique ID: <Alarm Unique ID >; If exists Additional Info1:/ Additional Info2:/ Additional Info3:

## 39.2 Configuring Syslog Settings

The procedure below describes how to configure Syslog. This includes defining the Syslog server address as well as selecting the activities on the device (for example, a parameter value change) that you want reported to the server.



### Notes:

- For configuring CDR reporting, see "Configuring CDR Reporting" on page 350.
- For viewing Syslog messages in the Web interface, see "Viewing Syslog Messages" on page 370.
- For a detailed description on the Syslog parameters, see "Syslog, CDR and Debug Parameters" on page 402.

### ➤ To configure Syslog :

1. Open the Syslog Settings page (**Configuration** tab > **System** menu > **Syslog Settings**).

▼ Syslog Settings	
Enable Syslog	Enable ▼
Syslog Server IP Address	10.8.2.2
Syslog Server Port	514
Debug Level	0 ▼

▼ Activity Types to Report via 'Activity Log' Messages	
Parameters Value Change	<input type="checkbox"/>
Auxiliary Files Loading	<input type="checkbox"/>
Device Reset	<input type="checkbox"/>
Flash Memory Burning	<input type="checkbox"/>
Device Software Update	<input type="checkbox"/>
Access to Restricted Domains	<input type="checkbox"/>
Non-Authorized Access	<input type="checkbox"/>
Sensitive Parameters Value Change	<input type="checkbox"/>
Login and Logout	<input type="checkbox"/>

2. Enable the Syslog feature by setting the 'Enable Syslog' to **Enable**.



3. Define the Syslog server using the 'Syslog Server IP Address' and 'Syslog Server Port' parameters.
4. Configure the debug level using the 'Debug Level' parameter.
5. Under the 'Activity Types to Report ...' group, select the activities to report.
6. Click **Submit** to apply your changes.

## 39.3 Configuring Debug Recording

The device enables you to activate debug recording and send debug recording packets to a defined capturing server. When the debug recording is activated, the device duplicates all messages that are sent and/or received by it and then sends them to an external IP address. The debug recording can be done for different types of traffic for example, RTP/RTCP, T.38 and SIP.

Debug recording is used for advanced debugging when you need to analyze internal messages and signals. Debug recording is also useful for recording network traffic in environments where hub or port mirroring is unavailable and for recording internal traffic between two endpoints on the same device.



**Note:** Debug recording is collected only on the device's OAMP interface.

### ➤ To configure and activate debug recording:

1. Open the Logging Settings page (**Configuration** tab > **System** menu > **Logging** > **Logging Settings**).

**Figure 39-1: Logging Settings Page**

▼ Debug Recording	
Debug Recording Destination IP	<input type="text" value="10.13.4.22"/>
Debug Recording Destination Port	<input type="text" value="925"/>
Debug Recording Status	<input type="button" value="Start"/> ▼

2. Configure the debug capturing server using the 'Debug Recording Destination IP' and 'Debug Recording Destination Port' parameters.
3. From the 'Debug Recording Status' drop-down list, select **Start** to start the debug recording or **Stop** to end the recording.
4. Click **Submit** to apply your changes.



## 39.4 Filtering Syslog Messages and Debug Recordings

The device can filter Syslog messages and debug recording (DR) packets, sent by the device to a Syslog server and packet capturing application (such as Wireshark) respectively. This can be useful to reduce CPU consumption and minimize negative impact on VoIP performance.

You can configure up to 30 filtering rules, each based on a selected filtering criteria (e.g., an IP Group). Each filtering criteria can be configured with a range. For example, you can filter Syslog messages for IP Groups 1 through 4. For each filter criteria, you can enable or disable Syslog messages and debug recording.

Debug recording can also be filtered using various filtering criteria such as SIP signaling or signaling and media.

➤ **To configure logging filtering rules:**

1. Open the Logging Filters Table page (**Configuration** tab > **System** menu > **Logging** > **Logging Filters Table**).
2. Click the **Add** button; the Add Record dialog box appears:

**Figure 39-2: Logging Filters Table - Add Record Dialog Box**

The 'Add Record' dialog box contains the following fields and options:

- Index:** A text input field containing the value '1'.
- Type:** A dropdown menu currently showing 'Any Filter'.
- Value:** An empty text input field.
- Syslog:** A dropdown menu currently showing 'Enable'.
- Capture Type:** A dropdown menu currently showing 'Signaling + Media'.
- Buttons:** 'Submit' and 'Cancel' buttons at the bottom right.

3. Configure the logging filter, as required. See the table below for a description of the parameters.
4. Click **Submit** to save your changes.



**Notes:**

- To configure the Syslog debug level, use the 'Debug Level' parameter (see "Configuring Syslog" on page 365).
- The Logging Filters table can also be configured using the table ini file parameter, LoggingFilters.

**Table 39-5: Logging Filters Table Parameters Description**

Parameter	Description
Filter Type CLI: filter-type [LoggingFilters_Type]	Defines the filter criteria. <ul style="list-style-type: none"> <li>▪ [1] Any (default)</li> <li>▪ [8] IP Group = Filters according to a specified IP Group ID listed in the IP Group table.</li> <li>▪ [9] SRD = Filters according to a specified SRD ID listed in the</li> </ul>



Parameter	Description
	SRD table. <ul style="list-style-type: none"> <li>▪ <b>[10]</b> Classification = Filters according to a specified Classification rule listed in the Classification table (applicable only to the SBC and application).</li> <li>▪ <b>[11]</b> IP-to-IP Routing = Filters according to a specified SBC IP-to-IP routing rule listed in the IP-to-IP Routing table (applicable only to the SBC application).</li> <li>▪ <b>[12]</b> User = Filters according to a specified user defined by username or user@host.</li> <li>▪ <b>[13]</b> IP Trace = Filters according to a specified IP network trace wireshark-like expression. For a detailed description on configuring IP traces, see 'Filtering IP Network Traces' on page 368.</li> </ul>
Value CLI: value <b>[LoggingFilters_Value]</b>	Defines the value of the selected filtering type in the 'Filter Type' parameter. The value can be the following: <ul style="list-style-type: none"> <li>▪ A single value</li> <li>▪ A range, using a hyphen "-" between the two values, e.g., "1-3"</li> <li>▪ Multiple, non-contiguous values, using commas "," between each value, e.g., "1,3,9"</li> <li>▪ Any to indicate all</li> <li>▪ For IP trace expressions, see e 'Filtering IP Network Traces' on page 368</li> </ul>
Syslog <b>[LoggingFilters_Syslog]</b>	Enables Syslog messages for the defined logging filter: <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul>
Capture Type <b>[LoggingFilters_CaptureType]</b>	Enables debug recordings for the defined logging filter and defines what to record: <ul style="list-style-type: none"> <li>▪ <b>[0]</b> None (default)</li> <li>▪ <b>[1]</b> Signaling = Information related to signaling such as SIP signaling messages, Syslog, and CDR.</li> <li>▪ <b>[2]</b> Signaling &amp; Media = Signaling and media (RTP/RTCP/T.38).</li> <li>▪ <b>[3]</b> Signaling &amp; Media &amp; PCM = Signaling, media, and PCM.</li> </ul>

### 39.4.1 Filtering IP Network Traces

You can filter Syslog and debug recording messages for IP network traces, by setting the 'Filter Type' parameter to **IP Trace** in the Logging Filters table. IP traces are used to record any IP stream, according to destination and/or source IP address, or port and Layer-4 protocol (UDP, TCP or any other IP type as defined by <http://www.iana.com>).

When the **IP Trace** option is selected, only the 'Value' parameter is applicable; the 'Syslog' and 'Capture Type' parameters are not relevant. The 'Value' parameter configures the Wireshark-like filtering expressions for your IP trace. The following Wireshark-like expressions are supported:

#### Supported Wireshark-like Expressions for 'Value' Parameter

Expression	Description
ip.src, ip.dst	Source and destination IP address



Expression	Description
ip.addr	IP address - up to two IP addresses can be entered
ip.proto	IP protocol type (PDU) entered as an enumeration value (e.g., 1 is ICMP, 6 is TCP, 17 is UDP)
udp, tcp, icmp, sip, ldap, http, https	Single expressions for protocol type
udp.port, tcp.port	Transport layer
udp.srcport, tcp.srcport	Transport layer for source port
udp.dstport, tcp.dstport	Transport layer for destination port
and, &&, ==, <, >	Between expressions

Below are examples of configured expressions for the 'Value' parameter:

- udp && ip.addr==10.8.6.55
- ip.src==10.8.6.55 && udp.port>=5000 and udp.port<6000
- ip.dst==10.8.0.1/16
- ip.addr==10.8.6.40

For conditions requiring the "or" / "||" expression, add multiple table rows. For example, the Wireshark condition "(ip.src == 1.1.1.1 or ip.src == 2.2.2.2) and ip.dst == 3.3.3.3" can be configured using the following two table row entries:

1. ip.src == 1.1.1.1 and ip.dst == 3.3.3.3
2. ip.src == 2.2.2.2 and ip.dst == 3.3.3.3



**Note:** If the 'Value' field is left empty, the device will record all IP traffic types.



## 39.5 Viewing Syslog Messages

You can use the following tools to view the Syslog messages sent by the device:

- Web interface's Message Log page (see below).
- Any third-party Syslog server (e.g., Wireshark).

The procedure below describes how to view Syslog messages in the Web interface.



### Notes:

- It's not recommended to keep a Message Log session open for a prolonged period. This may cause the device to overload. For prolonged (and detailed) debugging, use an external Syslog server.
- You can select the Syslog messages in this page, and copy and paste them into a text editor such as Notepad. This text file (*txt*) can then be sent to AudioCodes Technical Support for diagnosis and troubleshooting.

### ➤ To activate the Web interface's Message Log:

1. Enable Syslog (see "Configuring Syslog" on page 365).
2. Open the Message Log page (**Status & Diagnostics** tab > **System Status** menu > **Message Log**); the Message Log page is displayed and the log is activated.

Figure 39-3: Message Log Page

```
Log is Activated

11d:14h:43m:9s (lgr_psbrdex) (2662) recv <-- ON_HOOK Ch:1
11d:14h:43m:9s (lgr_flow) (2663) #1:ON_HOOK_EV
11d:14h:43m:9s (lgr_flow) (2664) | #1:ON_HOOK_EV
11d:14h:43m:9s (lgr_psbrdif) (2665) #1:cpDigitMapHndlr_Stop - Stopped (0)
11d:14h:43m:9s (lgr_psbrdif) (2666) #1:CloseChannel: ChannelNum=1
11d:14h:43m:9s (lgr_psbrdif) (2667) Open channel: IsVoiceOn: 1, IsT38On: 1, IsVbdOn: 0, Is
11d:14h:43m:9s (lgr_psbrdif) (2668) #1:OpenChannel:on Trunk -1 BChannel:1 CID=1 with Voice
11d:14h:43m:9s (lgr_psbrdif) (2669) #1:OpenChannel VoiceVolume= 0, DTHFVolume = -11, Input
11d:14h:43m:9s (lgr_psbrdif) (2670) OpenChannel, CoderType = 15, Interval = 4, M = 1
11d:14h:43m:9s (lgr_psbrdif) (2671) #1:FAXTransportType = 1
11d:14h:43m:9s (lgr_psbrdif) (2672) #1:ConfigFaxModemChannelParams NSEMode=0, CNGDetMode=
11d:14h:43m:9s (lgr_psbrdif) (2673) Detectors: Amd:0, Ans:0 En:0 IBScmd:0xa1
11d:14h:43m:9s (lgr_psbrdif) (2674) #1:PSOSBoardInterface::StopPlayTone- Called
11d:14h:43m:9s (lgr_psbrdex) (2675) recv <-- OFF_HOOK Ch:1
11d:14h:43m:9s (lgr_flow) (2676) #1:OFF_HOOK_EV
11d:14h:43m:9s (lgr_flow) (2677) | #1:OFF_HOOK_EV
11d:14h:43m:9s (lgr_psbrdif) (2678) UpdateChannelParams, Channel 1
11d:14h:43m:9s (lgr_psbrdif) (2679) #1:ConfigFaxModemChannelParams NSEMode=0, CNGDetMode=
11d:14h:43m:9s (lgr_psbrdif) (2680) ActivateDigitMap for channel : 1, MaxDialStringLength
```

The displayed logged messages are color-coded as follows:

- Yellow - fatal error message
- Blue - recoverable error message (i.e., non-fatal error)
- Black - notice message

### ➤ To stop and clear the Message Log:

- Close the Message Log page by accessing any another page in the Web interface.



## 39.6 Collecting Debug Recording Messages

To collect debug recording packets, the open source program Wireshark is used. AudioCodes proprietary plug-in files for Wireshark, which are shipped in your software kit, are also required.



### Notes:

- The default debug recording port is 925. You can change the port in Wireshark (**Edit menu > Preferences > Protocols > AC DR**).
- The plug-ins are per major software release and are applicable to Wireshark Ver. 1.62.
- The plug-ins are backward compatible.
- From Wireshark Ver. 99.08, the tpncp.dat file must be located in the folder, ...WireShark\tpncp.

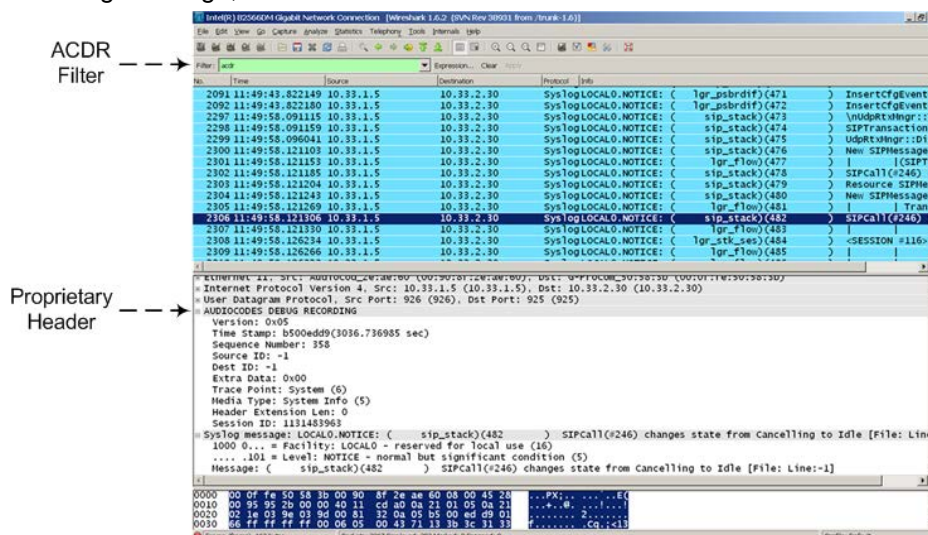
### ➤ To install Wireshark and the plug-ins for debug recording:

1. Install Wireshark on your computer. The Wireshark program can be downloaded from <http://www.wireshark.org>.
2. Copy the supplied AudioCodes plug-in files to the directory in which you installed Wireshark, as follows:

Copy this file	To this folder
...\dtds\cdr.dtd	Wireshark\dtds\
...\plugins\1.6.2*.dll	Wireshark\plugins\1.6.2
...\tpncp\tpncp.dat	Wireshark\tpncp

3. Start Wireshark.
4. In the Filter field, type "acdr" (see the figure below) to view the debug recording messages. Note that the source IP address of the messages is always the OAMP IP address of the device.

The device adds the header "AUDIOCODES DEBUG RECORDING" to each debug recording message, as shown below:



Reader's Notes



## Reader's Notes



## 40 Testing SIP Signaling Calls

A simulated endpoint can be configured on the device to test SIP signaling of calls between it and a remote destination. This feature is useful in that it can remotely verify SIP message flow without involving the remote end side in the debug process. The SIP test call simulates the SIP signaling process - call setup, SIP 1xx responses, and through to completing the SIP transaction with a 200 OK.

The test call sends Syslog messages to a Syslog server, showing the SIP message flow, DTMF signals, termination reasons, as well as voice quality statistics.

### 40.1 Configuring Test Call Endpoints

The Test Call table enables you to test the SIP signaling (setup and registration) of calls and media (DTMF signals) between a simulated phone on the device and a remote endpoint. These tests involve both incoming and outgoing calls, where the test endpoint can be configured as the caller or called party. Test calls can be dialed automatically at a user-defined interval and/or manually when required. The simulated phone and remote endpoints are defined as SIP URIs (user@host) and the remote destination can be defined as an IP Group, IP address, or according to an Outbound IP Routing rule. You can also enable automatic registration of the endpoint.

When a SIP test call is initiated, the device generates a SIP INVITE towards the remote endpoint (e.g., a SIP proxy server or softswitch). It simulates the SIP call setup process, managing SIP 1xx responses and completing the SIP transaction with a 200 OK.



#### Notes:

- By default, you can configure up to five test calls. This maximum can be increased by installing the relevant Software License Key. For more information, contact your AudioCodes sales representative.
- The Test Call Endpoint table can also be configured using the table ini file parameter Test\_Call (see 'SIP Test Call Parameters' on page 401).

#### ➤ To configure test calls:

1. Open the Test Call Table page (**Configuration** tab > **System** menu > **Test Call** > **Test Call Table**).
2. Click the **Add** button; the following dialog box appears:

Figure 40-1: General Tab of Test Call Table



3. Configure the test endpoint parameters as desired. See the table below for a description of these parameters.
4. Click **Submit** to apply your settings.

**Test Call Table Parameters**

Parameter	Description
<b>General Tab</b>	
Endpoint URI [Test_Call_EndpointURI]	<p>Defines the endpoint's URI. This can be defined as a user or user@host. The device identifies this endpoint only by the URI's user part. The URI's host part is used in the SIP From header in REGISTER requests.</p> <p>The valid value is a string of up to 150 characters. By default, this parameter is not configured.</p>
Called URI [Test_Call_CalledURI]	<p>Defines the destination (called) URI (user@host).</p> <p>The valid value is a string of up to 150 characters. By default, this parameter is not configured.</p>
Route By [Test_Call_DestType]	<p>Defines the type of routing method. This applies to incoming and outgoing calls.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> GW Tel2IP = (Default) Calls are matched by (or routed to) an SRD and Application type (defined in the SRD and Application Type parameters below).</li> <li>▪ <b>[1]</b> IP Group = Calls are matched by (or routed to) an IP Group ID.</li> <li>▪ <b>[2]</b> Dest Address = Calls are matched by (or routed to) an SRD and application type.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ For REGISTER messages, the option <b>[0]</b> cannot be used as the routing method.</li> <li>▪ For REGISTER messages, if option <b>[1]</b> is used, only Server-type IP Groups can be used.</li> </ul>
IP Group ID [Test_Call_IPGroupID]	<p>Defines the IP Group ID to which the test call is sent or from which it is received.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This parameter is applicable only if option <b>[1]</b> is configured for the 'Route By' parameter.</li> <li>▪ This IP Group is used for incoming and outgoing calls.</li> </ul>
Destination Address [Test_Call_DestAddress]	<p>Defines the destination host. This can be defined as an IP address[:port] or DNS name[:port].</p> <p><b>Note:</b> This parameter is applicable only if the 'Route By' parameter is set to <b>[2]</b> (Dest Address).</p>
Destination Transport Type [Test_Call_DestTransportType]	<p>Defines the transport type for outgoing calls.</p> <ul style="list-style-type: none"> <li>▪ <b>[-1]</b> Not configured (default)</li> <li>▪ <b>[0]</b> UDP</li> <li>▪ <b>[1]</b> TCP</li> <li>▪ <b>[2]</b> TLS</li> </ul> <p><b>Note:</b> This parameter is applicable only if the 'Route By' parameter is set to <b>[2]</b> (Dest Address).</p>



Parameter	Description
SRD [Test_Call_SRD]	Defines the SRD for the endpoint. The default is SRD 0. <b>Note:</b> This parameter is applicable only if the 'Route By' parameter is set any option except [1] (IP Group).
Application Type [Test_Call_ApplicationType]	Defines the application type for the endpoint. This, in effect, associates the IP Group and SRD to a specific SIP interface. <ul style="list-style-type: none"> <li>[0] GW &amp; IP2IP (default)</li> <li>[2] SBC</li> </ul>
<b>Authentication Tab</b>	
<b>Note:</b> These parameters are applicable only if the test endpoint is set to <b>Caller</b> (see the 'Call Party' parameter).	
Auto Register [Test_Call_AutoRegister]	Enables automatic registration of the endpoint. The endpoint can register to the device itself or to the 'Destination Address' or 'IP Group ID' parameter settings (see above). <ul style="list-style-type: none"> <li>[0] False (default)</li> <li>[1] True</li> </ul>
User Name [Test_Call_UserName]	Defines the authentication username. By default, no username is defined.
Password [Test_Call_Password]	Defines the authentication password. By default, no password is defined.
<b>Test Settings Tab</b>	
Call Party [Test_Call_CallParty]	Defines whether the test endpoint is the initiator or receiving side of the test call. <ul style="list-style-type: none"> <li>[0] Caller (default)</li> <li>[1] Called</li> </ul>
Maximum Channels for Session [Test_Call_MaxChannels]	Defines the maximum number of concurrent channels for the test session. For example, if you have configured an endpoint "101" and you set this parameter to "3", the device automatically creates three simulated endpoints - "101", "102" and "103" (i.e., consecutive endpoint URIs are assigned). The default is 1.
Call Duration [Test_Call_CallDuration]	Defines the call duration (in seconds). The valid value is -1 to 100000. The default is 20. A value of 0 means infinite. A value of -1 means that the parameter value is automatically calculated according to the values of the 'Calls per Second' and 'Maximum Channels for Session' parameters. <b>Note:</b> This parameter is applicable only if 'Call Party' is set to <b>Caller</b> .
Calls per Second [Test_Call_CallsPerSecond]	Defines the number of calls per second. <b>Note:</b> This parameter is applicable only if 'Call Party' is set to <b>Caller</b> .



Parameter	Description
Test Mode [Test_Call_TestMode]	<p>Defines the test session mode.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Once = (Default) The test runs until the lowest value between the following is reached: <ul style="list-style-type: none"> <li>✓ Maximum channels is reached for the test session, configured by 'Maximum Channels for Session'.</li> <li>✓ Call duration ('Call Duration') multiplied by calls per second ('Calls per Second').</li> <li>✓ Test duration expires, configured by 'Test Duration'.</li> </ul> </li> <li>▪ <b>[1]</b> Continuous = The test runs until the configured test duration is reached. If it reaches the maximum channels configured for the test session (in the 'Maximum Channels for Session'), it waits until the configured call duration of a currently established tested call expires before making the next test call. In this way, the test session stays within the configured maximum channels.</li> </ul> <p><b>Note:</b> This parameter is applicable only if 'Call Party' is set to <b>Caller</b>.</p>
Test Duration [Test_Call_TestDuration]	<p>Defines the test duration (in minutes).</p> <p>The valid value is 0 to 100000. The default is 0 (i.e., unlimited).</p> <p><b>Note:</b> This parameter is applicable only if 'Call Party' is set to <b>Caller</b>.</p>
Play [Test_Call_Play]	<p>Enables playing a user-defined DTMF signal to the answered side of the call.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> DTMF</li> </ul> <p>To configure the played DTMF signal, see 'Configuring DTMF Tones for Test Calls' on page 378.</p> <p><b>Note:</b> This parameter is applicable only if 'Call Party' is set to <b>Caller</b>.</p>
Schedule Interval [Test_Call_ScheduleInterval]	<p>Defines the interval (in minutes) between automatic outgoing test calls.</p> <p>The valid value range is 0 to 100000. The default is 0 (i.e., scheduling is disabled).</p> <p><b>Note:</b> This parameter is applicable only if 'Call Party' is set to <b>Caller</b>.</p>

## 40.1.1 Starting, Stopping and Restarting Test Calls

The procedure below describes how to start, stop, and restart test calls.

### ➤ To start, stop, and restart a test call:

1. In the Test Call table, select the required test call entry; the **Actions** button appears above the table.
2. From the **Actions** drop-down list, choose the required command:
  - **Dial:** starts the test call (this action is applicable only if the test call party is the caller).
  - **Drop Call:** stops the test call.
  - **Restart:** ends all established calls and then starts the test call session again.

The status of the test call is displayed in the 'Test Status' field of the Test Call table:

- "Idle": test call is not active.
- "Scheduled": test call is planned to run (according to 'Schedule Interval' parameter settings)
- "Running": test call has been started (i.e., the **Dial** command was clicked)



- "Receiving": test call has been automatically activated by calls received for the test call endpoint from the remote endpoint (when all these calls end, the status returns to "Idle")
- "Terminating": test call is in the process of terminating the currently established calls (this occurs if the **Drop Call** command is clicked to stop the test)
- "Done": test call has been successfully completed (or was prematurely stopped by clicking the **Drop Call** command)

A more detailed description of this field is displayed below the table when you click the **Show/Hide** button (see 'Viewing Test Call Statistics' on page 377).

### 40.1.2 Viewing Test Call Statistics

In addition to viewing a brief status description of the test call in the 'Test Status' field (as described in 'Starting, Stopping and Restarting Test Calls' on page 376), you can also view a more detailed status description which includes test call statistics.

➤ **To view statistics of a test call:**

1. Open the Test Call Table page (**Configuration** tab > **System** menu > **Test Call** > **Test Call Table**).
2. Select the test call table entry whose call statistics you want to view.
3. Click the **Show/Hide** button; the call statistics are displayed in the **Test Statistics** pane located below the table, as shown in the figure below:

**Figure 40-2: Viewing Test Call Statistics**

The screenshot shows the 'Test Call Table' interface. At the top, there are buttons for 'Add +', 'Edit ✎', 'Delete -', and 'Action ▾'. A 'Show/Hide' button is in the top right. The table has columns: Index, Endpoint URI, Called URI, Route By, IP Group ID, Destination Address, SRD, Application Type, Call Party, and Test Status. One row is visible with Index 0, Endpoint URI 101, Called URI 102, Route By GW Tel2IP, IP Group ID -1, Destination Address 10.13.4.12, SRD 0, Application Type GW & IP2IP, Call Party Caller, and Test Status Running. Below the table, there is a 'Test Call Table #0' section with details for the selected call, and a 'Test Statistics' section with various metrics.

Index	Endpoint URI	Called URI	Route By	IP Group ID	Destination Address	SRD	Application Type	Call Party	Test Status
0	101	102	GW Tel2IP	-1	10.13.4.12	0	GW & IP2IP	Caller	Running

**Test Call Table #0**

Endpoint URI: 101  
Route By: GW Tel2IP  
Destination Address: 10.13.4.12  
SRD: 0  
Auto Register: Disable  
Password:  
Maximum Channels for Session: 4  
Calls per Second: 10  
Test Duration (minutes): 4  
Schedule Interval (minutes): 0

Called URI: 102  
IP Group ID: -1  
Destination Transport Type:  
Application Type: GW & IP2IP  
User Name:  
Call Party: Caller  
Call Duration (seconds): 20  
Test Mode: Once  
Play: DTMF

**Test Statistics**

Elapsed Time [HH:MM:SS]: 00:00:11  
Call Attempts: 4  
Total Failed Attempts: 2  
Test Status: Running  
Detailed Status: Running (Calls: 2, ASR: 50%)

Active Calls: 2  
Total Established Calls: 2  
Remote Disconnections Count: 0  
Average CPS:

The 'Test Statistics' pane displays the following test session information:

- **Elapsed Time:** Duration of the test call since it was started (or restarted).
- **Active Calls:** The number of currently active test calls.
- **Call Attempts:** The number of calls that were attempted.
- **Total Established Calls:** The total number of calls that were successfully established.
- **Total Failed Attempts:** The total number of calls that failed to be established.
- **Remote Disconnections Count:** Number of calls that were disconnected by the remote side.
- **Average CPS:** The average calls per second.
- **Test Status:** Displays the status (brief description) as displayed in the 'Test Status' field (see 'Starting, Stopping and Restarting Test Calls' on page 376).



- **Detailed Status:** Displays a detailed description of the test call status::
  - "Idle": The test call is currently not active.
  - "Scheduled - Established Calls: <established calls>, ASR: <%>": The test call is planned to run (according to 'Schedule Interval' parameter settings) and also shows the following summary of completed test calls:
    - ◆ Total number of test calls that were established.
    - ◆ Number of successfully answered calls out of the total number of calls attempted (ASR).
  - "Running (Calls: <number of active calls>, ASR: <%>)": The test call has been started (i.e., the **Dial** command was clicked) and shows the following:
    - ◆ Number of currently active test calls.
    - ◆ Number of successfully answered calls out of the total number of calls attempted (Answer Seizure Ratio or ASR).
  - "Receiving (<number of active calls>)": The test call has been automatically activated by calls received for this configured test call endpoint from the configured remote endpoint. When all these calls terminate, the status returns to "Idle".
  - "Terminating (<number of active calls>)": The **Drop Call** command has been clicked to stop the test call and the test call is in the process of terminating the currently active test calls.
  - "Done - Established Calls: <established calls>, ASR: <%>": The test call has been successfully completed (or was prematurely stopped by clicking the **Drop Call** command) and shows the following:
    - ◆ Total number of test calls that were established.
    - ◆ Number of successfully answered calls out of the total number of calls attempted (ASR).



**Note:** On the receiving side, when the first call is accepted in "Idle" state, statistics are reset.

## 40.2 Configuring DTMF Tones for Test Calls

By default, no DTMF signal is played to an answered test call (incoming or outgoing). However, you can enable this per configured test call in the Test Call table (see 'Configuring Test Call Endpoints' on page 373). If enabled, the default DTMF signal that is played is "3212333". You can change this as described below.



**Note:** To generate DTMF tones, the device's DSP resources are required.

### ➤ To configure the played DTMF signal to answered test call:

1. Open the Test Call Settings page (**Configuration** tab > **System** menu > **Test Call** > **Test Call Settings**).

Test Call DTMF String	3212333
-----------------------	---------

2. In the 'Test Call DTMF String' field, enter the DTMF string (up to 15 digits).
3. Click **Submit**.



### 40.3 Configuring SBC Test Call with External Proxy

The SBC Test Call feature tests incoming SBC SIP call flow between a simulated test endpoint on the device and a remote SIP endpoint, when registration and routing is done through an external proxy/registrar server such as a hosted IP PBX in the WAN. In other words, the complete SIP flow, including the path to/from the external proxy/registrar can be tested.

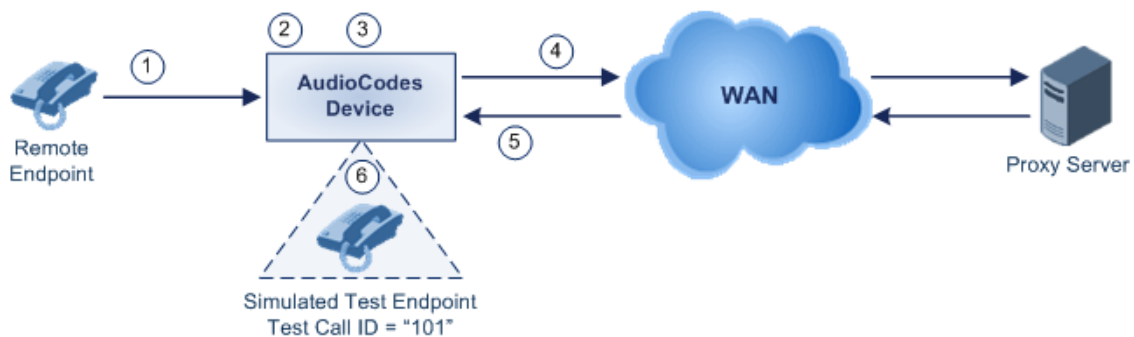
As this test call type involves an SBC call, you need to configure regular SBC rules such as classification and IP-to-IP routing. Therefore, this test call also allows you to verify correct SBC configuration.

For this test call, you also need to configure the following call IDs:

- Test Call ID - prefix number of the simulated endpoint on the device.
- SBC Test ID - prefix number of called number for identifying incoming call as SBC test call. The device removes this prefix, enabling it to route the call according to the IP-to-IP Routing rules to the external proxy/registrar, instead of directly to the simulated endpoint. Only when the device receives the call from the proxy/registrar, does it route the call to the simulated endpoint.

The figure below displays an example of an SBC test call:

**Figure 40-3: SBC Test Call Example**



1. The call is received from the remote endpoint with the called number prefix "8101".
2. As the 'SBC Test ID' parameter is set to "8", the device identifies this call as a test call and removes the digit "8" from the called number prefix, leaving it as "101".
3. The device performs the regular SBC processing such as classification and manipulation.
4. The device routes the call, according to the configured SBC IP-to-IP routing rules, to the proxy server.
5. The device receives the call from the proxy server.
6. As the 'Test Call ID' parameter is set to "101", the device identifies the incoming call as a test call and sends it directly to the simulated test endpoint "101".



➤ **To configure SBC call testing:**

1. Configure the test call parameters:
  - a. Open the Test Call Settings page (**Configuration** tab > **System** menu > **Test Call** > **Test Call Settings**).

**Figure 40-4: Test Call Settings Page**

Test Call ID	<input type="text"/>
SBC Test ID	<input type="text"/>

- b. In the 'Test Call ID' field, enter a prefix number for the simulated test endpoint on the device.
  - c. In the 'SBC Test ID' field, enter a called prefix number for identifying the call as an SBC test call.
  - d. Click **Submit** to apply your settings.
2. Configure regular SBC call processing rules for called number prefix "101", such as classification and IP-to-IP routing through a proxy server.

**Notes:**

- For a full description of this parameter, see 'SIP Test Call Parameters' on page 401.
- This test call is initiated only upon receipt of incoming calls and with the configured prefix.
- This call test is done on all SIP interfaces.
- This test call is applicable only to the SBC application.

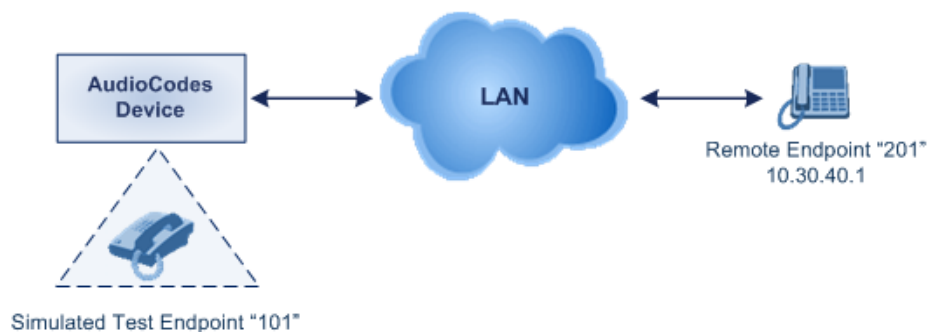


## 40.4 Test Call Configuration Examples

Below are a few examples of test call configurations.

- **Single Test Call Scenario:** This example describes the configuration of a simple test call scenario that includes a single test call between a simulated test endpoint on the device and a remote endpoint.

**Figure 40-5: Single Test Call Example**

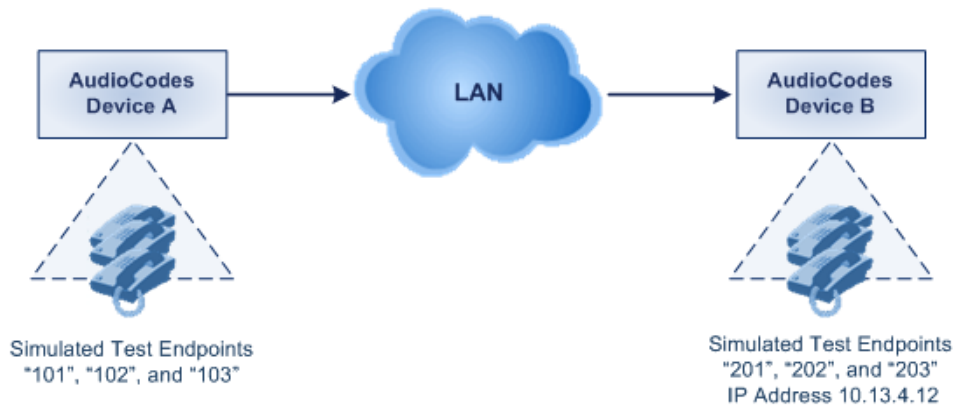


- Test Call table configuration:
  - ◆ Endpoint URI: "101"
  - ◆ Called URI: "201"
  - ◆ Route By: Dest Address
  - ◆ Destination Address: "10.30.40.01"
  - ◆ Call Party: Caller
  - ◆ Test Mode: Once (default)



- **Batch Test Call Scenario:** This example describes the configuration of a batch test call setup for scheduled and continuous call testing of multiple endpoints. The test call is done between two AudioCodes devices - Device A and Device B - with simulated test endpoints. This eliminates the need for phone users, who would otherwise need to answer and end calls many times for batch testing. The calls are initiated from Device A, where Device B serves as the remote answering endpoint.

**Figure 40-6: Batch Test Call Example**

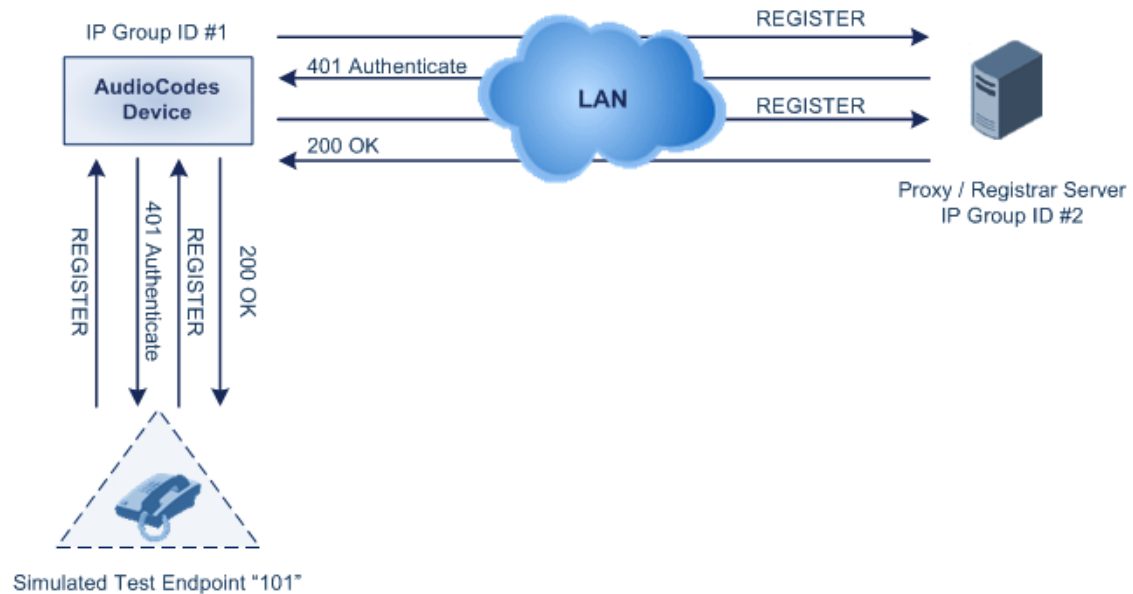


- Test Call table configuration at Device A:
  - ◆ Endpoint URI: "101"
  - ◆ Called URI: "201"
  - ◆ Route By: Dest Address
  - ◆ Destination Address: "10.13.4.12"
  - ◆ Call Party: Caller
  - ◆ Maximum Channels for Session: "3" (this setting configures three endpoints - "101", "102" and "103")
  - ◆ Call Duration: "5" (seconds)
  - ◆ Calls per Sec: "1"
  - ◆ Test Mode: Continuous
  - ◆ Test Duration: "3" (minutes)
  - ◆ Schedule Interval: "180" (minutes)
- Test Call table configuration at Device B:
  - ◆ Endpoint URI: "201"
  - ◆ Call Party: Caller
  - ◆ Maximum Channels for Session: "3" (this setting configures three endpoints - "201", "202" and "203")



- **Registration Test Call Scenario:** This example describes the configuration for testing the registration and authentication (i.e., username and password) process of a simulated test endpoint on the device with an external proxy/registrar server. This is useful, for example, for verifying that endpoints located in the LAN can register with an external proxy and subsequently, communicate with one another.

**Figure 40-7: Test Call Registration Example**



This example assumes that you have configured your device for communication between LAN phone users such as IP Groups to represent the device (10.13.4.12) and the proxy server, and IP-to-IP routing rules to route calls between these IP Groups.

- Test Call table configuration:
  - ◆ Endpoint URI: "101"
  - ◆ Called URI: "itsp"
  - ◆ Route By: Dest Address
  - ◆ Destination Address: "10.13.4.12" (this is the IP address of the device itself)
  - ◆ Auto Register: Enable
  - ◆ User Name: "testuser"
  - ◆ Password: "12345"
  - ◆ Call Party: Caller



# Part XI

## Appendix







## 41 Dialing Plan Notation for Routing and Manipulation

The device supports flexible dialing plan notations for denoting the prefix and/or suffix source and/or destination numbers and SIP URI user names in the routing and manipulation tables.

**Table 41-1: Dialing Plan Notations for Prefixes and Suffixes**

Notation	Description
<b>x</b> (letter "x")	Denotes any single digit.
<b>#</b> (pound symbol)	<ul style="list-style-type: none"> <li>When used at the end of a prefix, it denotes the end of a number. For example, <b>54324xx#</b> represents a 7-digit number that starts with the digits 54324.</li> <li>When used anywhere in the suffix, it is part of the number. For example, <b>(3#45)</b> can represent the number string, 123#45.</li> </ul>
<b>*</b> (asterisk symbol)	<ul style="list-style-type: none"> <li>When used in the prefix, it denotes any number.</li> <li>When used in the suffix, it is part of the number. For example, <b>(3*45)</b> can represent the number string, 123*45.</li> </ul>
<b>\$</b> (dollar sign)	<p>Denotes an empty prefix for incoming IP calls that do not have a user part in the Request-URI, or for incoming Tel calls that do not have a called or calling number. This is used for the following matching criteria:</p> <ul style="list-style-type: none"> <li>Source and Destination Phone Prefix</li> <li>Source and Destination Username</li> <li>Source and Destination Calling Name Prefix</li> </ul>
<b>Range of Digits</b> <b>Notes:</b> <ul style="list-style-type: none"> <li>Dial plans denoting a prefix that is a range must be enclosed in square brackets, e.g., <b>[4-8]</b> or <b>23xx[456]</b>.</li> <li>Dial plans denoting a prefix that is not a range is not enclosed, e.g., <b>12345#</b>.</li> <li>Dial plans denoting a suffix must be enclosed in parenthesis, e.g., <b>(4)</b> and <b>(4-8)</b>.</li> <li>Dial plans denoting a suffix that include multiple ranges, the range must be enclosed in square brackets, e.g., <b>(23xx[4,5,6])</b>.</li> <li>An example for entering a combined prefix and suffix dial plan - assume you want to match a rule whose destination phone prefix is 4 to 8, and suffix is 234, 235, or 236. The entered value would be the following: <b>[4-8](23[4,5,6])</b>.</li> </ul>	
<b>[n-m]</b> or <b>(n-m)</b>	<p>Represents a range of numbers, for example:</p> <ul style="list-style-type: none"> <li>To depict numbers from 5551200 to 5551300: <ul style="list-style-type: none"> <li>✓ Prefix: <b>[5551200-5551300]#</b></li> <li>✓ Suffix: <b>(5551200-5551300)</b></li> </ul> </li> <li>To depict numbers from 123100 to 123200: <ul style="list-style-type: none"> <li>✓ Prefix: <b>123[100-200]</b></li> <li>✓ Suffix: <b>(123[100-200])</b></li> </ul> </li> <li>To depict prefix and suffix numbers together: <ul style="list-style-type: none"> <li>✓ 03(100): for any number that starts with 03 and ends with 100.</li> <li>✓ <b>[100-199](100,101,105)</b>: for a number that starts with 100 to 199 and ends with 100, 101 or 105.</li> <li>✓ 03(abc): for any number that starts with 03 and ends with abc.</li> <li>✓ 03(5xx): for any number that starts with 03 and ends with 5xx.</li> <li>✓ 03(400,401,405): for any number that starts with 03 and ends with</li> </ul> </li> </ul>



Notation	Description
	<p>400 or 401 or 405.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>The value <math>n</math> must be less than the value <math>m</math>.</li> <li>Only numerical ranges are supported (not alphabetical letters).</li> <li>For suffix ranges, the starting (<math>n</math>) and ending (<math>m</math>) numbers in the range must have the same number of digits. For example, (23-34) is correct, but (3-12) is not.</li> </ul>
[ $n,m,\dots$ ] or ( $n,m,\dots$ )	<p>Represents multiple numbers. For example, to depict a one-digit number starting with 2, 3, 4, 5, or 6:</p> <ul style="list-style-type: none"> <li>Prefix: <b>[2,3,4,5,6]#</b></li> <li>Suffix: <b>(2,3,4,5,6)</b></li> <li>Prefix with Suffix: <b>[2,3,4,5,6](8,7,6)</b> - prefix is denoted in square brackets; suffix in parenthesis</li> </ul> <p>For <b>prefix only</b>, the notations <math>d[n,m]e</math> and <math>d[n-m]e</math> can also be used:</p> <ul style="list-style-type: none"> <li>To depict a five-digit number that starts with 11, 22, or 33: <b>[11,22,33]xxx#</b></li> <li>To depict a six-digit number that starts with 111 or 222: <b>[111,222]xxx#</b></li> </ul> <p><b>Note:</b> Up to three digits can be used to denote each number.</p>
[ $n1-m1,n2-m2,a,b,c,n3-m3$ ] or ( $n1-m1,n2-m2,a,b,c,n3-m3$ )	<p>Represents a mixed notation of single numbers and multiple ranges. For example, to depict numbers 123 to 130, 455, 766, and 780 to 790:</p> <ul style="list-style-type: none"> <li>Prefix: <b>[123-130,455,766,780-790]</b></li> <li>Suffix: <b>(123-130,455,766,780-790)</b></li> </ul> <p><b>Note:</b> The ranges and the single numbers used in the dial plan must have the same number of digits. For example, each number range and single number in the dialing plan example above consists of three digits.</p>



**Note:** When configuring phone numbers or prefixes in the Web interface, enter them only as digits without any other characters. For example, if you wish to enter the phone number 555-1212, it must be entered as 5551212 without the hyphen (-). If the hyphen is entered, the entry is invalid.



## 42 Configuration Parameters Reference

The device's configuration parameters, default values, and their descriptions are documented in this section.



**Note:** Parameters and values enclosed in square brackets [...] represent the *ini* file parameters and their enumeration values.

### 42.1 Networking Parameters

This subsection describes the device's networking parameters.

#### 42.1.1 Ethernet Parameters

The Ethernet parameters are described in the table below.

**Table 42-1: Ethernet Parameters**

Parameter	Description
Physical Ports Settings Table	
Web: Physical Ports Settings <b>[PhysicalPortsTable]</b>	<p>This table parameter configures the physical Ethernet ports</p> <p>The format of this parameter is as follows:</p> <pre>[ PhysicalPortsTable ] FORMAT PhysicalPortsTable_Index = PhysicalPortsTable_Port, PhysicalPortsTable_Mode, PhysicalPortsTable_NativeVlan, PhysicalPortsTable_SpeedDuplex, PhysicalPortsTable_PortDescription, PhysicalPortsTable_GroupMember, PhysicalPortsTable_GroupStatus; [ \PhysicalPortsTable ]</pre> <p>For example:</p> <pre>PhysicalPortsTable 0 = GE_4_1, 1, 1, 4, "User Port #0", GROUP_1, Active; PhysicalPortsTable 1 = GE_4_2, 1, 1, 4, "User Port #1", GROUP_1, Redundant;</pre> <p><b>Note:</b> For a description of this parameter, see Configuring Physical Ethernet Ports on page 87.</p>
Ethernet Group Settings Table	
Web: Ethernet Group Settings <b>[EtherGroupTable]</b>	<p>Defines the transmit (Tx) and receive (Rx) settings for the Ethernet port groups. The format of this parameter is as follows:</p> <pre>[EtherGroupTable] FORMAT EtherGroupTable_Index = EtherGroupTable_Group, EtherGroupTable_Mode, EtherGroupTable_Member1, EtherGroupTable_Member2; [\EtherGroupTable]</pre> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>For a description of this parameter, see Configuring Tx/Rx for Ethernet Port-Pair Groups on page 88.</li> </ul>



## 42.1.2 Multiple VoIP Network Interfaces and VLAN Parameters

The IP network interfaces and VLAN parameters are described in the table below.

**Table 42-2: IP Network Interfaces and VLAN Parameters**

Parameter	Description
<b>Multiple Interface Table</b>	
Web: Multiple Interface Table <b>[InterfaceTable]</b>	<p>This table parameter configures the Multiple Interface table. The format of this parameter is as follows:</p> <p><b>[InterfaceTable]</b>            FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes, InterfaceTable_InterfaceMode, InterfaceTable_IPAddress, InterfaceTable_PrefixLength, InterfaceTable_Gateway, InterfaceTable_VlanID, InterfaceTable_InterfaceName, InterfaceTable_PrimaryDNSServerIPAddress, InterfaceTable_SecondaryDNSServerIPAddress, InterfaceTable_UnderlyingInterface;  <b>[InterfaceTable]</b></p> <p>For example:            InterfaceTable 0 = 0, 0, 192.168.85.14, 16, 0.0.0.0, 1, Management;            InterfaceTable 1 = 2, 0, 200.200.85.14, 24, 0.0.0.0, 200, Control;            InterfaceTable 2 = 1, 0, 211.211.85.14, 24, 211.211.85.1, 211, Media;</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>For a description of this parameter, see "Configuring IP Network Interfaces" on page 90.</li> </ul>
<b>VLAN Parameters</b>	
<b>[EnableNTPasOAM]</b>	<p>Defines the application type for Network Time Protocol (NTP) services.</p> <ul style="list-style-type: none"> <li><b>[1]</b> = OAMP (default)</li> <li><b>[0]</b> = Control</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>

## 42.1.3 Routing Parameters

The IP network routing parameters are described in the table below.

**Table 42-3: IP Network Routing Parameters**

Parameter	Description
Web: Disable ICMP Redirects <b>[DisableICMPRedirects]</b>	<p>Determines whether the device accepts or ignores ICMP Redirect messages.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) ICMP Redirect messages are handled by the device.</li> <li><b>[1]</b> Enable = ICMP Redirect messages are ignored.</li> </ul>
<b>Static IP Routing Table</b>	
Web: IP Routing Table <b>[StaticRouteTable]</b>	<p>Defines up to 30 static IP routing rules for the device. These rules can be associated with IP interfaces defined in the Multiple Interface table (InterfaceTable parameter). The routing decision for sending the outgoing IP packet is based on the source subnet/VLAN. If not associated with an IP interface, the static IP rule is based on destination</p>



Parameter	Description
	<p>IP address.</p> <p>When the destination of an outgoing IP packet does not match one of the subnets defined in the Multiple Interface table, the device searches this table for an entry that matches the requested destination host/network. If such an entry is found, the device sends the packet to the indicated router (i.e., next hop). If no explicit entry is found, the packet is sent to the default gateway according to the source interface of the packet (if defined).</p> <p>The format of this parameter is as follows:</p> <p><b>[ StaticRouteTable ]</b></p> <p>FORMAT StaticRouteTable_Index = StaticRouteTable_InterfaceName, StaticRouteTable_Destination, StaticRouteTable_PrefixLength, StaticRouteTable_Gateway, StaticRouteTable_Description;</p> <p><b>[ \StaticRouteTable ]</b></p> <p><b>Note:</b> For a description of this parameter, see "Configuring Static IP Routing" on page <a href="#">99</a>.</p>

### 42.1.4 Quality of Service Parameters

The Quality of Service (QoS) parameters are described in the table below.

**Table 42-4: QoS Parameters**

Parameter	Description
<b>Layer-2 Class Of Service (CoS) Parameters (VLAN Tag Priority Field)</b>	
Web: DiffServ Table EMS: QoS Settings – DSCP to QoS Mapping <b>[DiffServToVlanPriority]</b>	<p>This table parameter configures DiffServ-to-VLAN Priority mapping. For each packet sent to the LAN, the VLAN Priority of the packet is set according to the DiffServ value in the IP header of the packet. The format of this ini file is as follows:</p> <p><b>[ DiffServToVlanPriority ]</b></p> <p>FORMAT DiffServToVlanPriority_Index = DiffServToVlanPriority_DiffServ, DiffServToVlanPriority_VlanPriority;</p> <p><b>[ \DiffServToVlanPriority ]</b></p> <p>For example:</p> <p>DiffServToVlanPriority 0 = 46, 6;            DiffServToVlanPriority 1 = 40, 6;            DiffServToVlanPriority 2 = 26, 4;            DiffServToVlanPriority 3 = 10, 2;</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>For a description of this table, see Configuring Quality of Service on page <a href="#">102</a></li> </ul>
<b>Layer-3 Class of Service (TOS/DiffServ) Parameters</b>	
Web: Media Premium QoS <b>[PremiumServiceClassMediaDiffServ]</b>	<p>Defines the DiffServ value for Premium Media CoS content.</p> <p>The valid range is 0 to 63. The default is 46.</p>



Parameter	Description
	<b>Note:</b> The value for the Premium Control DiffServ is determined by the following (according to priority): <ul style="list-style-type: none"> <li>IPDiffServ value in the selected IP Profile (IPProfile parameter).</li> <li>PremiumServiceClassMediaDiffServ.</li> </ul>
Web: Control Premium QoS [PremiumServiceClassControlDiffServ]	Defines the DiffServ value for Premium Control CoS content (Call Control applications). The valid range is 0 to 63. The default is 40. <b>Notes:</b> <ul style="list-style-type: none"> <li>The value for the Premium Control DiffServ is determined by the following (according to priority): <ul style="list-style-type: none"> <li>✓ SigIPDiffServ value in the selected IP Profile (IPProfile parameter).</li> <li>✓ PremiumServiceClassControlDiffServ.</li> </ul> </li> </ul>
Web: Gold QoS [GoldServiceClassDiffServ]	Defines the DiffServ value for the Gold CoS content (Streaming applications). The valid range is 0 to 63. The default is 26.
Web: Bronze QoS [BronzeServiceClassDiffServ]	Defines the DiffServ value for the Bronze CoS content (OAMP applications). The valid range is 0 to 63. The default is 10.

## 42.1.5 NAT and STUN Parameters

The Network Address Translation (NAT) parameters are described in the table below.

**Table 42-5: NAT Parameters**

Parameter	Description
<b>NAT Parameters</b>	
Web: NAT Traversal [DisableNAT]	Enables the NAT mechanism. For more information, see "First Incoming Packet Mechanism" on page 112. <ul style="list-style-type: none"> <li>[0] Enable</li> <li>[1] Disable (default)</li> </ul>
Web: NAT IP Address [StaticNatIP]	Defines the global (public) IP address of the device to enable static NAT between the device and the Internet. <b>Note:</b> For this parameter to take effect, a device reset is required.

## 42.1.6 NFS Parameters

The Network File Systems (NFS) configuration parameters are described in the table below.

**Table 42-6: NFS Parameters**

Parameter	Description
[NFSBasePort]	Defines the start of the range of numbers used for local UDP ports used by the NFS client. The maximum number of local ports is maximum



Parameter	Description
	channels plus maximum NFS servers. The valid range is 0 to 65535. The default is 47000.
<b>NFS Table</b>	
Web: NFS Table <b>[NFSServers]</b>	<p>This table parameter defines up to 16 NFS file systems so that the device can access a remote server's shared files and directories for loading cmp, ini, and auxiliary files (using the Automatic Update mechanism).</p> <p>The format of this table ini file parameter is as follows:</p> <pre>[NFSServers] FORMAT NFSServers_Index = NFSServers_HostOrIP, NFSServers_RootPath, NFSServers_NfsVersion, NFSServers_AuthType, NFSServers_UID, NFSServers_GID, NFSServers_VlanType; [NFSServers]</pre> <p>For example: NFSServers 1 = 101.1.13, /audio1, 3, 1, 0, 1, 1;</p> <p><b>Note:</b> For a detailed description of this table, see "Configuring NFS Settings" on page <a href="#">107</a>.</p>

### 42.1.7 DNS Parameters

The Domain name System (DNS) parameters are described in the table below.

**Table 42-7: DNS Parameters**

Parameter	Description
<b>Internal DNS Table</b>	
Web: Internal DNS Table <b>[DNS2IP]</b>	<p>This table parameter defines the internal DNS table for resolving host names into IP addresses. Up to four different IP addresses (in dotted-decimal notation) can be assigned to a host name.</p> <p>The format of this parameter is as follows:</p> <pre>[Dns2Ip] FORMAT Dns2Ip_Index = Dns2Ip_DomainName, Dns2Ip_FirstIpAddress, Dns2Ip_SecondIpAddress, Dns2Ip_ThirdIpAddress, Dns2Ip_FourthIpAddress; [Dns2Ip]</pre> <p>For example: Dns2Ip 0 = DnsName, 1.1.1.1, 2.2.2.2, 3.3.3.3, 4.4.4.4;</p> <p><b>Note:</b> For a detailed description of this table parameter, see "Configuring the Internal DNS Table" on page <a href="#">104</a>.</p>
<b>Internal SRV Table</b>	
Web: Internal SRV Table <b>[SRV2IP]</b>	<p>This table parameter defines the internal SRV table for resolving host names into DNS A-Records. Three different A-Records can be assigned to a host name. Each A-Record contains the host name, priority, weight, and port. The format of this parameter is as follows:</p> <pre>[SRV2IP] FORMAT SRV2IP_Index = SRV2IP_InternalDomain, SRV2IP_TransportType, SRV2IP_Dns1, SRV2IP_Priority1, SRV2IP_Weight1, SRV2IP_Port1, SRV2IP_Dns2, SRV2IP_Priority2,</pre>



Parameter	Description
	SRV2IP_Weight2, SRV2IP_Port2, SRV2IP_Dns3, SRV2IP_Priority3, SRV2IP_Weight3, SRV2IP_Port3; [SRV2IP] For example: SRV2IP 0 = SrvDomain,0,Dnsname1,1,1,500,Dnsname2,2,2,501,\$\$,0,0,0; <b>Note:</b> For a detailed description of this table parameter, see "Configuring the Internal SRV Table" on page 106.

## 42.1.8 DHCP Parameters

The Dynamic Host Control Protocol (DHCP) parameters are described in the table below.

**Table 42-8: DHCP Parameters**

Parameter	Description
Web: Enable DHCP [DHCPEnable]	Enables Dynamic Host Control Protocol (DHCP) functionality. <ul style="list-style-type: none"> <li>[0] Disable (default)</li> <li>[1] Enable</li> </ul> <b>Notes:</b> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>After you enable the DHCP server, do the following: <ol style="list-style-type: none"> <li>Enable DHCP and save the configuration.</li> <li>Perform a cold reset using the device's hardware reset button (soft reset using the Web interface doesn't trigger the DHCP procedure and this parameter reverts to 'Disable').</li> </ol> </li> <li>This parameter is a special 'Hidden' parameter. Once defined and saved in flash memory, its assigned value doesn't revert to its default even if the parameter doesn't appear in the <i>ini</i> file.</li> </ul>
[DHCPspeedFactor]	Defines the DHCP renewal speed. <ul style="list-style-type: none"> <li>[0] = Disable</li> <li>[1] = (Default) Normal</li> <li>[2] to [10] = Fast</li> </ul> When set to 0, the DHCP lease renewal is disabled. Otherwise, the renewal time is divided by this factor. Some DHCP-enabled routers perform better when set to 4. <b>Note:</b> For this parameter to take effect, a device reset is required.



## 42.1.9 NTP and Daylight Saving Time Parameters

The Network Time Protocol (NTP) and daylight saving time parameters are described in the table below.

**Table 42-9: NTP and Daylight Saving Time Parameters**

Parameter	Description
<b>NTP Parameters</b>	
<b>Note:</b> For more information on Network Time Protocol (NTP), see "Simple Network Time Protocol Support" on page 83.	
Web: NTP Server DN/IP [NTPServerIP]	Defines the IP address (in dotted-decimal notation or as an FQDN) of the NTP server. The advantage of using an FQDN is that multiple IP addresses can be resolved from the DNS server, providing NTP server redundancy.  The default IP address is 0.0.0.0 (i.e., internal NTP client is disabled).
Web: NTP Secondary Server IP [NTPSecondaryServerIP]	Defines a second NTP server's address as an FQDN or an IP address (in dotted-decimal notation). This NTP is used for redundancy; if the primary NTP server fails, then this NTP server is used.  The default IP address is 0.0.0.0.
Web: NTP UTC Offset [NTPServerUTCOffset]	Defines the Universal Time Coordinate (UTC) offset (in seconds) from the NTP server.  The default offset is 0. The offset range is -43200 to 43200.
Web: NTP Update Interval [NTPUpdateInterval]	Defines the time interval (in seconds) that the NTP client requests for a time update.  The default interval is 86400 (i.e., 24 hours). The range is 0 to 214783647.  <b>Note:</b> It is not recommend to set this parameter to beyond one month (i.e., 2592000 seconds).
<b>Daylight Saving Time Parameters</b>	
Web: Day Light Saving Time [DayLightSavingTimeEnable]	Enables daylight saving time. <ul style="list-style-type: none"> <li>▪ [0] Disable (default)</li> <li>▪ [1] Enable</li> </ul>
Web: Start Time or Day of Month Start [DayLightSavingTimeStart]	Defines the date and time when daylight saving begins. This value can be configured using any of the following formats: <ul style="list-style-type: none"> <li>▪ Day of year - <i>mm:dd:hh:mm</i>, where: <ul style="list-style-type: none"> <li>✓ <i>mm</i> denotes month</li> <li>✓ <i>dd</i> denotes date of the month</li> <li>✓ <i>hh</i> denotes hour</li> <li>✓ <i>mm</i> denotes minutes</li> </ul> For example, "05:01:08:00" denotes daylight saving starting from May 1 at 8 A.M. </li> <li>▪ Day of month - <i>mm:day/wk:hh:mm</i>, where: <ul style="list-style-type: none"> <li>✓ <i>mm</i> denotes month (e.g., 04)</li> <li>✓ <i>day</i> denotes day of week (e.g., FRI)</li> <li>✓ <i>wk</i> denotes week of the month (e.g., 03)</li> <li>✓ <i>hh</i> denotes hour (e.g., 23)</li> </ul> </li> </ul>



Parameter	Description
	<p>✓ <i>mm</i> denotes minutes (e.g., 10)</p> <p>For example, "04:FRI/03:23:00" denotes Friday, the third week of April, at 11 P.M. The week field can be 1-5, where 5 denotes the last occurrence of the specified day in the specified month. For example, "04:FRI/05:23:00" denotes the last Friday of April, at 11 P.M.</p>
Web: End Time or Day of Month End [DayLightSavingTimeEnd]	Defines the date and time when daylight saving ends. For a description of the format of this value, see the DayLightSavingTimeStart parameter.
Web: Offset [DayLightSavingTimeOffset]	Defines the daylight saving time offset (in minutes). The valid range is 0 to 120. The default is 60.

## 42.2 Management Parameters

This subsection describes the device's Web and Telnet parameters.

### 42.2.1 General Parameters

The general management parameters are described in the table below.

**Table 42-10: General Management Parameters**

Parameter	Description
Web: Web and Telnet Access List Table [WebAccessList_x]	<p>This table configures up to ten IP addresses that are permitted to access the device's Web interface and Telnet interfaces. Access from an undefined IP address is denied. When no IP addresses are defined in this table, this security feature is inactive (i.e., the device can be accessed from any IP address).</p> <p>The default is 0.0.0.0 (i.e., the device can be accessed from any IP address).</p> <p>For example: WebAccessList_0 = 10.13.2.66 WebAccessList_1 = 10.13.77.7</p> <p>For a description of this parameter, see "Configuring Web and Telnet Access List" on page 54.</p>

### 42.2.2 Web Parameters

The Web parameters are described in the table below.

**Table 42-11: Web Parameters**

Parameter	Description
Web: Enable web access from all interfaces [EnableWebAccessFromAllInterfaces]	<p>Enables Web access from any of the device's IP network interfaces (i.e., OAMP, Control, and/or Media). This feature applies to HTTP and HTTPS protocols.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = (Default) Disable – Web access is only through the OAMP interface.</li> </ul>



Parameter	Description
	<ul style="list-style-type: none"> <li><b>[1]</b> = Enable - Web access is through any network interface.</li> </ul>
Web: Password Change Interval <b>[WebUserPassChangeInterval]</b>	<p>Defines the duration (in minutes) of the validity of Web login passwords. When this duration expires, the password of the Web user must be changed.</p> <p>The valid value is 0 to 100000, where 0 means that the password is always valid. The default is 1140.</p> <p><b>Note:</b> This parameter is applicable only when using the Web Users table, where the default value of the 'Password Age' parameter in the Web Users table inherits this parameter's value.</p>
Web: User inactivity timer <b>[UserInactivityTimer]</b>	<p>Defines the duration (in days) for which a user has not logged in to the Web interface, after which the status of the user becomes inactive and can no longer access the Web interface. These users can only log in to the Web interface if their status is changed (to New or Valid) by a System Administrator or Master user.</p> <p>The valid value is 0 to 10000, where 0 means inactive. The default is 90.</p> <p><b>Note:</b> This parameter is applicable only when using the Web Users table.</p>
Web: Session Timeout <b>[WebSessionTimeout]</b>	<p>Defines the duration (in minutes) of Web inactivity of a logged-in user, after which the user is automatically logged off the Web interface.</p> <p>The valid value is 0-100000, where 0 means no timeout. The default is 15.</p> <p><b>Note:</b> This parameter can apply to all users, or per user when set in the Web Users table.</p>
Web: Deny Access On Fail Count <b>[DenyAccessOnFailCount]</b>	<p>Defines the maximum number of failed login attempts, after which the requesting IP address is blocked.</p> <p>The valid value range is 0 to 10. The values 0 and 1 mean immediate block. The default is 3.</p>
Web: Deny Authentication Timer <b>[DenyAuthenticationTimer]</b>	<p>Defines the duration (in seconds) for which login to the Web interface is denied from a specific IP address (for all users) when the number of failed login attempts has exceeded the maximum. This maximum is defined by the DenyAccessOnFailCount parameter. Only after this time expires can users attempt to login from this same IP address.</p> <p>The valid value is 0 to 100000, where 0 means that login is not denied regardless of number of failed login attempts. The default is 60.</p>
Web: Display Login Information <b>[DisplayLoginInformation]</b>	<p>Enables display of user's login information on each successful login attempt.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = Disable (default)</li> <li><b>[1]</b> = Enable</li> </ul>
<b>[EnableMgmtTwoFactorAuthentication]</b>	<p>Enables Web login authentication using a third-party, smart card.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = Disable (default)</li> <li><b>[1]</b> = Enable</li> </ul> <p>When enabled, the device retrieves the Web user's login username from the smart card, which is automatically displayed (read-only) in</p>



Parameter	Description
	<p>the Web Login screen; the user is then required to provide only the login password.</p> <p>Typically, a TLS connection is established between the smart card and the device's Web interface, and a RADIUS server is implemented to authenticate the password with the username. Thus, this feature implements a two-factor authentication - what the user has (the physical card) and what the user knows (i.e., the login password).</p>
[HTTPport]	<p>Defines the LAN HTTP port for Web management (default is 80). To enable Web management from the LAN, configure the desired port.</p> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
[DisableWebConfig]	<p>Determines whether the entire Web interface is read-only.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = (Default) Enables modifications of parameters.</li> <li>▪ <b>[1]</b> = Web interface is read-only.</li> </ul> <p>When in read-only mode, parameters can't be modified. In addition, the following pages can't be accessed: 'Web User Accounts', 'Certificates', 'Regional Settings', 'Maintenance Actions' and all file-loading pages ('Load Auxiliary Files', 'Software Upgrade Wizard', and 'Configuration File').</p> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
[ResetWebPassword]	<p>Resets the username and password of the primary ("Admin") and secondary ("User") accounts to their default settings ("Admin" and "Admin" respectively), and deletes all other users that may have been configured.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = (Default) Password and username retain their values.</li> <li>▪ <b>[1]</b> = Password and username are reset.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ For this parameter to take effect, a device reset is required.</li> <li>▪ You cannot reset the username and password through the Web interface (by loading an ini file or on the AdminPage). To reset the username and password, use SNMP: <ul style="list-style-type: none"> <li>a. Set acSysGenericINILine to WEBPasswordControlViaSNMP = 1, and reset the device with a flash burn (set acSysActionSetResetControl to 1 and acSysActionSetReset to 1).</li> <li>b. Change the username and password in the acSysWEBAccessEntry table. Use the following format: Username acSysWEBAccessUserName: old/pass/new Password acSysWEBAccessUserCode: username/old/new</li> </ul> </li> </ul>



Parameter	Description
<b>[WelcomeMessage]</b>	<p>Enables and defines a Welcome message that appears on the Web Login page for logging in to the Web interface.</p> <p>The format of this parameter is as follows:</p> <pre>[WelcomeMessage ] FORMAT WelcomeMessage_Index = WelcomeMessage_Text [\WelcomeMessage]</pre> <p>For Example:</p> <pre>FORMAT WelcomeMessage_Index = WelcomeMessage_Text WelcomeMessage 1 = "*****" ; WelcomeMessage 2 = "***** This is a Welcome message *****" ; WelcomeMessage 3 = "*****" ;</pre> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>Each index row represents a line of text in the Welcome message box. Up to 20 lines (or rows) of text can be defined.</li> <li>The configured text message must be enclosed in double quotation marks (i.e., "...").</li> <li>If this parameter is not configured, no Welcome message is displayed.</li> </ul>
Web: HA Device Name <b>[HAUnitIdName]</b>	<p>Defines a name for the device, which is displayed on the Home page to indicate the active device.</p> <p>The valid value is a string of up to 128 characters. For the default value, the device assigns either "Device 1" or "Device 2", so that active and redundant devices have different default names.</p>

### 42.2.3 Telnet Parameters

The Telnet parameters are described in the table below.

**Table 42-12: Telnet Parameters**

Parameter	Description
Web: Embedded Telnet Server <b>[TelnetServerEnable]</b>	<p>Enables the device's embedded Telnet server. Telnet is disabled by default for security.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable Unsecured</li> <li><b>[2]</b> Enable Secured (SSL)</li> </ul> <p><b>Note:</b> Only the primary Web User Account (which has Security Administration access level) can access the device using Telnet (see "Configuring Web User Accounts" on page 46).</p>
Web: Telnet Server TCP Port <b>[TelnetServerPort]</b>	<p>Defines the port number for the embedded Telnet server.</p> <p>The valid range is all valid port numbers. The default port is 23.</p>
Web: Telnet Server Idle Timeout <b>[TelnetServerIdleDisconnect]</b>	<p>Defines the timeout (in minutes) for disconnection of an idle Telnet session. When set to zero, idle sessions are not disconnected.</p> <p>The valid range is any value. The default is 0.</p> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>



## 42.2.4 SNMP Parameters

The SNMP parameters are described in the table below.

**Table 42-13: SNMP Parameters**

Parameter	Description
Web: Enable SNMP [DisableSNMP]	Enables SNMP. <ul style="list-style-type: none"> <li>[0] Enable = (Default) SNMP is enabled.</li> <li>[1] Disable = SNMP is disabled and no traps are sent.</li> </ul>
[SNMPPort]	Defines the device's local (LAN) UDP port used for SNMP Get/Set commands. The range is 100 to 3999. The default port is 161. <b>Note:</b> For this parameter to take effect, a device reset is required.
[KeepAliveTrapPort]	Defines the port to which keep-alive traps are sent. The valid range is 0 - 65534. The default is port 162.
[SendKeepAliveTrap]	Enables keep-alive traps and sends them every 9/10 of the time as defined by the NATBindingDefaultTimeout parameter. <ul style="list-style-type: none"> <li>[0] = Disable</li> <li>[1] = Enable</li> </ul> <b>Note:</b> For this parameter to take effect, a device reset is required.
[SNMPSysOid]	Defines the base product system OID. The default is eSNMP_AC_PRODUCT_BASE_OID_D. <b>Note:</b> For this parameter to take effect, a device reset is required.
[SNMPTrapEnterpriseOid]	Defines the Trap Enterprise OID. The default is eSNMP_AC_ENTERPRISE_OID. The inner shift of the trap in the AcTrap subtree is added to the end of the OID in this parameter. <b>Note:</b> For this parameter to take effect, a device reset is required.
[acUserInputAlarmDescription]	Defines the description of the input alarm.
[acUserInputAlarmSeverity]	Defines the severity of the input alarm.
[AlarmHistoryTableMaxSize]	Defines the maximum number of rows in the Alarm History table. This parameter can be controlled by the Config Global Entry Limit MIB (located in the Notification Log MIB). The valid range is 50 to 1000. The default is 50. <b>Note:</b> For this parameter to take effect, a device reset is required.
[SNMPEngineIDString]	Defines the SNMP engine ID for SNMPv2/SNMPv3 agents. This is used for authenticating a user attempting to access the SNMP agent on the device. The ID can be a string of up to 36 characters. The default is 00:00:00:00:00:00:00:00:00:00:00:00:00 (12 Hex octets characters). The provided key must be set with 12 Hex values delimited by a colon (":") in the format xx:xx:...:xx. For example, 00:11:22:33:44:55:66:77:88:99:aa:bb <b>Notes:</b> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>Before setting this parameter, all SNMPv3 users must be deleted; otherwise, the parameter setting is ignored.</li> </ul>



Parameter	Description
	<ul style="list-style-type: none"> <li>If the supplied key does not pass validation of the 12 Hex values input or it is set with the default value, the engine ID is generated according to RFC 3411.</li> </ul>
<b>Web: SNMP Trap Destination Parameters</b>	
<b>Note:</b> Up to five SNMP trap managers can be defined.	
SNMP Manager [SNMPManagerIsUsed_x]	<p>Determines the validity of the parameters (IP address and port number) of the corresponding SNMP Manager used to receive SNMP traps.</p> <ul style="list-style-type: none"> <li>[0] (Check box cleared) = Disabled (default)</li> <li>[1] (Check box selected) = Enabled</li> </ul>
Web: IP Address [SNMPManagerTableIP_x]	<p>Defines the IP address of the remote host used as an SNMP Manager. The device sends SNMP traps to this IP address. Enter the IP address in dotted-decimal notation, e.g., 108.10.1.255.</p>
Web: Trap Port [SNMPManagerTrapPort_x]	<p>Defines the port number of the remote SNMP Manager. The device sends SNMP traps to this port.</p> <p>The valid SNMP trap port range is 100 to 4000. The default port is 162.</p>
Web: Trap Enable [SNMPManagerTrapSendingEnable_x]	<p>Enables the sending of traps to the corresponding SNMP manager.</p> <ul style="list-style-type: none"> <li>[0] Disable = Sending is disabled.</li> <li>[1] Enable = (Default) Sending is enabled.</li> </ul>
Web: Trap User [SNMPManagerTrapUser_x]	<p>Defines the SNMPv3 USM user or SNMPv2 user to associate with the trap destination. This determines the trap format, authentication level, and encryption level. By default, it is associated with the SNMPv2 user (SNMP trap community string).</p> <p>The valid value is a string.</p>
Web: Trap Manager Host Name [SNMPTrapManagerHostName]	<p>Defines an FQDN of the remote host used as an SNMP manager. The resolved IP address replaces the last entry in the Trap Manager table (defined by the SNMPManagerTableIP parameter) and the last trap manager entry of snmpTargetAddrTable in the snmpTargetMIB. For example: 'mngr.corp.mycompany.com'.</p> <p>The valid range is a string of up to 99 characters.</p>
<b>SNMP Community String Parameters</b>	
Community String [SNMPReadOnlyCommunityString_x]	<p>Defines up to five read-only SNMP community strings (up to 19 characters each). The default string is 'public'.</p>
Community String [SNMPReadWriteCommunityString_x]	<p>Defines up to five read/write SNMP community strings (up to 19 characters each). The default string is 'private'.</p>
Trap Community String [SNMPTrapCommunityString]	<p>Defines the Community string used in traps (up to 19 characters). The default string is 'trapuser'.</p>
<b>SNMP Trusted Managers Table</b>	
Web: SNMP Trusted Managers [SNMPTrustedMgr_x]	<p>Defines up to five IP addresses of remote trusted SNMP managers from which the SNMP agent accepts and processes SNMP Get and Set requests.</p>



Parameter	Description
	<b>Notes:</b> <ul style="list-style-type: none"> <li>By default, the SNMP agent accepts SNMP Get and Set requests from any IP address, as long as the correct community string is used in the request. Security can be enhanced by using Trusted Managers, which is an IP address from which the SNMP agent accepts and processes SNMP requests.</li> <li>If no values are assigned to these parameters any manager can access the device.</li> <li>Trusted managers can work with all community strings.</li> </ul>
<b>SNMP V3 Users Table</b>	
Web: SNMP V3 Users <b>[SNMPUsers]</b>	<p>This <i>parameter</i> table defines SNMP v3 users. The format of this parameter is as follows:</p> <pre>[SNMPUsers] FORMAT SNMPUsers_Index = SNMPUsers_Username, SNMPUsers_AuthProtocol, SNMPUsers_PrivProtocol, SNMPUsers_AuthKey, SNMPUsers_PrivKey, SNMPUsers_Group; [SNMPUsers]</pre> <p>For example: SNMPUsers 1 = v3admin1, 1, 0, myauthkey, -, 1; The example above configures user 'v3admin1' with security level authNoPriv(2), authentication protocol MD5, authentication text password 'myauthkey', and ReadWriteGroup2.</p> <p><b>Note:</b> For a description of this table, see "Configuring SNMP V3 Users" on page 68.</p>

## 42.2.5 Serial Parameters

The RS-232 serial parameters are described in the table below.

**Table 42-14: Serial Parameters**

Parameter	Description
<b>[DisableRS232]</b>	<p>Enables the device's RS-232 (serial) port.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = Enabled</li> <li><b>[1]</b> = (Default) Disabled</li> </ul> <p>The RS-232 serial port can be used to change the networking parameters and view error/notification messages. For how to establish a serial communication with the device, refer to the <i>Installation Manual</i>.</p> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
<b>[SerialBaudRate]</b>	<p>Defines the RS-232 baud rate.</p> <p>The valid values include the following: 1200, 2400, 9600, 14400, 19200, 38400, 57600, or 115200.</p> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
<b>[SerialData]</b>	<p>Defines the RS-232 data bit.</p> <ul style="list-style-type: none"> <li><b>[7]</b> = 7-bit</li> <li><b>[8]</b> = (Default) 8-bit</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>



Parameter	Description
<b>[SerialParity]</b>	<p>Defines the RS-232 polarity.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = (Default) None</li> <li>▪ <b>[1]</b> = Odd</li> <li>▪ <b>[2]</b> = Even</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
<b>[SerialStop]</b>	<p>Defines the RS-232 stop bit.</p> <ul style="list-style-type: none"> <li>▪ <b>[1]</b> = (Default) 1-bit (default)</li> <li>▪ <b>[2]</b> = 2-bit</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
<b>[SerialFlowControl]</b>	<p>Defines the RS-232 flow control.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = (Default) None</li> <li>▪ <b>[1]</b> = Hardware</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>

## 42.3 Debugging and Diagnostics Parameters

This subsection describes the device's debugging and diagnostic parameters.

### 42.3.1 General Parameters

The general debugging and diagnostic parameters are described in the table below.

**Table 42-15: General Debugging and Diagnostic Parameters**

Parameter	Description
Web: Delay After Reset <b>[sec]</b> <b>[GWAppDelayTime]</b>	<p>Defines the time interval (in seconds) that the device's operation is delayed after a reset.</p> <p>The valid range is 0 to 45. The default is 7 seconds.</p> <p><b>Note:</b> This feature helps overcome connection problems caused by some LAN routers or IP configuration parameters' modifications by a DHCP server.</p>
<b>[EnableAutoRAITransmitBER]</b>	<p>Enables the device to send a remote alarm indication (RAI) when the bit error rate (BER) is greater than 0.001.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul>

### 42.3.2 SIP Test Call Parameters

The SIP Signaling Test Call parameters are described in the table below.

**Table 42-16: SIP Test Call Parameters**

Parameter	Description
Web: Test Call DTMF String	Defines the DTMF tone that is played for answered test calls (incoming and outgoing).



Parameter	Description
[TestCallIDtmfString]	The DTMF string can be up to 15 strings. The default is "3212333". An empty string means that no DTMF is played.
Web: Test Call ID [TestCallID]	<p>Defines the test call prefix number (<i>ID</i>) of the simulated phone on the device. Incoming calls received with this called prefix number are identified as test calls.</p> <p>This can be any string of up to 15 characters. By default, no number is defined.</p> <p><b>Note:</b> This parameter is only for testing incoming calls destined to this prefix number.</p>
Web: SBC Test ID CLI: sbc-test-id [SBCTestID]	<p>Defines the SBC test call prefix (ID) for identifying SBC test calls that traverse the device to register with an external routing entity such as an IP PBX or proxy server.</p> <p>This parameter functions together with the TestCallID parameter, which defines the prefix of the simulated endpoint. Upon receiving an incoming call with this prefix, the device removes the prefix, enabling it to forward the test call to the external entity. Upon receiving the call from the external entity, the device identifies the call as a test call according to its prefix, defined by the TestCallID, and then sends the call to the simulated endpoint.</p> <p>For example, assume SBCTestID is set to 4 and TestCallID to 2. If a call is received with called destination 4200, the device removes the prefix 4 and routes the call to the IP PBX. When it receives the call from the IP PBX, it identifies the call as a test call (i.e., prefix 2) and therefore, sends it to the simulated endpoint.</p> <p>The valid value can be any string of up to 15 characters. By default, no number is defined.</p> <p><b>Note:</b> This feature is applicable only to the SBC application.</p>
<b>Test Call Table</b>	
Web: Test Call Table [Test_Call]	<p>Defines the local and remote endpoints to be tested.</p> <p>[Test_Call]</p> <p>FORMAT Test_Call_Index = Test_Call_EndpointURI, Test_Call_CalledURI, Test_Call_RouteBy, Test_Call_IPGroupID, Test_Call_DestAddress, Test_Call_DestTransportType, Test_Call_SRD, Test_Call_ApplicationType, Test_Call_AutoRegister, Test_Call_UserName, Test_Call_Password, Test_Call_CallParty, Test_Call_MaxChannels, Test_Call_CallDuration, Test_Call_CallsPerSecond, Test_Call_TestMode, Test_Call_TestDuration, Test_Call_Play, Test_Call_ScheduleInterval;</p> <p>[Test_Call]</p> <p><b>Note:</b> For a description of this table, see "Configuring Test Calls" on page 373.</p>

### 42.3.3 Syslog, CDR and Debug Parameters

The Syslog, CDR and debug parameters are described in the table below.

**Table 42-17: Syslog, CDR and Debug Parameters**

Parameter	Description
Web: Enable Syslog	Determines whether the device sends logs and error messages (e.g.,



Parameter	Description
<b>[EnableSyslog]</b>	<p>CDRs) generated by the device to a Syslog server.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ If you enable Syslog, you must enter an IP address of the Syslog server (using the SyslogServerIP parameter).</li> <li>▪ Syslog messages may increase the network traffic.</li> <li>▪ To configure Syslog SIP message logging levels, use the GwDebugLevel parameter.</li> </ul>
Web: Syslog Server IP Address <b>[SyslogServerIP]</b>	<p>Defines the IP address (in dotted-decimal notation) of the computer on which the Syslog server is running. The Syslog server is an application designed to collect the logs and error messages generated by the device.</p> <p>The default IP address is 0.0.0.0.</p>
Web: Syslog Server Port <b>[SyslogServerPort]</b>	<p>Defines the UDP port of the Syslog server.</p> <p>The valid range is 0 to 65,535. The default port is 514.</p>
<b>[MaxBundleSyslogLength]</b>	<p>Defines the maximum size (in bytes) threshold of logged Syslog messages bundled into a single UDP packet, after which they are sent to a Syslog server.</p> <p>The valid value range is 0 to 1220 (where 0 indicates that no bundling occurs). The default is 1220.</p> <p><b>Note:</b> This parameter is applicable only if the GwDebugLevel parameter is set to 7.</p>
Web: CDR Server IP Address <b>[CDRSyslogServerIP]</b>	<p>Defines the destination IP address to where CDR logs are sent. The default is a null string, which causes CDR messages to be sent with all Syslog messages to the Syslog server.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ The CDR messages are sent to UDP port 514 (default Syslog port).</li> <li>▪ This mechanism is active only when Syslog is enabled (i.e., the parameter EnableSyslog is set to 1).</li> </ul>
Web: CDR Report Level <b>[CDRReportLevel]</b>	<p>Enables signaling-related CDRs to be sent to a Syslog server and determines the call stage at which they are sent.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> None = (Default) CDRs are not used.</li> <li>▪ <b>[1]</b> End Call = CDR is sent to the Syslog server at the end of each call.</li> <li>▪ <b>[2]</b> Start &amp; End Call = CDR report is sent to Syslog at the start and end of each call.</li> <li>▪ <b>[3]</b> Connect &amp; End Call = CDR report is sent to Syslog at connection and at the end of each call.</li> <li>▪ <b>[4]</b> Start &amp; End &amp; Connect Call = CDR report is sent to Syslog at the start, at connection, and at the end of each call.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ To enable media-related CDRs for SBC calls, use the MediaCDRReportLevel parameter.</li> <li>▪ The CDR Syslog message complies with RFC 3161 and is identified by: Facility = 17 (local1) and Severity = 6 (Informational).</li> <li>▪ This mechanism is active only when Syslog is enabled (i.e., the parameter EnableSyslog is set to 1).</li> </ul>



Parameter	Description
Web: Media CDR Report Level <b>[MediaCDRReportLevel]</b>	<p>Enables media-related CDRs of SBC calls to be sent to a Syslog server and determines the call stage at which they are sent.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> None = (Default) No media-related CDR is sent.</li> <li>▪ <b>[1]</b> End Media = Sends a CDR only at the end of the call.</li> <li>▪ <b>[2]</b> Start &amp; End Media = Sends a CDR once the media starts. In some calls it may only be after the call is established, but in other calls the media may start at ringback tone. A CDR is also sent upon termination (end) of the media in the call.</li> <li>▪ <b>[3]</b> Update &amp; End Media = Sends a CDR when an update occurs in the media of the call. For example, a call starts and a ringback tone occurs, a re-INVITE is sent for a fax call and as a result, a CDR with the MediaReportType field set to "Update" is sent, as the media was changed from voice to T.38. A CDR is also sent upon termination (end) of the media in the call.</li> <li>▪ <b>[4]</b> Start &amp; End &amp; Update Media = Sends a CDR at the start of the media, upon an update in the media (if occurs), and at the end of the media.</li> </ul> <p><b>Note:</b> To enable CDR generation as well as enable signaling-related CDRs, use the CDRReportLevel parameter.</p>
Web: Debug Level <b>[GwDebugLevel]</b>	<p>Defines the Syslog debug logging level.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> 0 = (Default) Debug is disabled.</li> <li>▪ <b>[1]</b> 1 = Flow debugging is enabled.</li> <li>▪ <b>[5]</b> 5 = Flow, device interface, stack interface, session manager, and device interface expanded debugging are enabled.</li> <li>▪ <b>[7]</b> 7 = This option is recommended when the device is running under "heavy" traffic. In this mode: <ul style="list-style-type: none"> <li>✓ The Syslog debug level automatically changes between level 5, level 1, and level 0, depending on the device's CPU consumption so that VoIP traffic isn't affected.</li> <li>✓ Syslog messages are bundled into a single UDP packet, after which they are sent to a Syslog server (bundling size is determined by the MaxBundleSyslogLength parameter). Bundling reduces the number of UDP Syslog packets, thereby improving CPU utilization.</li> </ul> </li> </ul> <p>Note that when this option is used, in order to read Syslog messages with Wireshark, a special plug-in (i.e., acsyslog.dll) must be used. Once the plug-in is installed, the Syslog messages are decoded as "AC SYSLOG" and are displayed using the 'acsyslog' filter instead of the regular 'syslog' filter.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This parameter is typically set to 5 if debug traces are required. However, in cases of heavy traffic, option 7 is recommended.</li> <li>▪ Options 2, 3, 4, and 6 are not recommended.</li> </ul>
Web: Syslog Facility Number <b>[SyslogFacility]</b>	<p>Defines the Facility level (0 through 7) of the device's Syslog messages, according to RFC 3164. This allows you to identify Syslog messages generated by the device. This is useful, for example, if you collect the device's and other equipments' Syslog messages, at one single server. The device's Syslog messages can easily be identified and distinguished from other Syslog messages by its Facility level. Therefore, in addition to filtering Syslog messages according to IP address, the messages can be filtered according to Facility level.</p> <ul style="list-style-type: none"> <li>▪ <b>[16]</b> = (Default) local use 0 (local0)</li> </ul>



Parameter	Description
	<ul style="list-style-type: none"> <li>▪ <b>[17]</b> = local use 1 (local1)</li> <li>▪ <b>[18]</b> = local use 2 (local2)</li> <li>▪ <b>[19]</b> = local use 3 (local3)</li> <li>▪ <b>[20]</b> = local use 4 (local4)</li> <li>▪ <b>[21]</b> = local use 5 (local5)</li> <li>▪ <b>[22]</b> = local use 6 (local6)</li> <li>▪ <b>[23]</b> = local use 7 (local7)</li> </ul>
Web: Activity Types to Report via Activity Log Messages <b>[ActivityListToLog]</b>	<p>Defines the Activity Log mechanism of the device, which sends log messages to a Syslog server for reporting certain types of Web operations according to the below user-defined filters.</p> <ul style="list-style-type: none"> <li>▪ <b>[pvc]</b> Parameters Value Change = Changes made on-the-fly to parameters. Note that the <i>ini</i> file parameter, EnableParametersMonitoring can also be used to set this option, using values <b>[0]</b> (disable) or <b>[1]</b> (enable).</li> <li>▪ <b>[afl]</b> Auxiliary Files Loading = Loading of auxiliary files.</li> <li>▪ <b>[dr]</b> Device Reset = Reset of device via the 'Maintenance Actions' page.  <b>Note:</b> For this option to take effect, a device reset is required.</li> <li>▪ <b>[fb]</b> Flash Memory Burning = Burning of files or parameters to flash (in 'Maintenance Actions' page).</li> <li>▪ <b>[swu]</b> Device Software Update = cmp file loading via the Software Upgrade Wizard.</li> <li>▪ <b>[ard]</b> Access to Restricted Domains = Access to restricted domains, which include the following Web pages:               <ul style="list-style-type: none"> <li>✓ (1) ini parameters (AdminPage)</li> <li>✓ (2) General Security Settings</li> <li>✓ (3) Configuration File</li> <li>✓ (5) Software Upgrade Key Status</li> <li>✓ (7) Web &amp; Telnet Access List</li> <li>✓ (8) WEB User Accounts</li> </ul> </li> <li>▪ <b>[naa]</b> Non-Authorized Access = Attempt to access the Web interface with a false or empty user name or password.</li> <li>▪ <b>[spc]</b> Sensitive Parameters Value Change = Changes made to sensitive parameters:               <ul style="list-style-type: none"> <li>✓ (1) IP Address</li> <li>✓ (2) Subnet Mask</li> <li>✓ (3) Default Gateway IP Address</li> <li>✓ (4) ActivityListToLog</li> </ul> </li> <li>▪ <b>[ll]</b> Login and Logout = Every login and logout attempt.</li> </ul> <p>For example: ActivityListToLog = 'pvc', 'afl', 'dr', 'fb', 'swu', 'ard', 'naa', 'spc'</p> <p><b>Note:</b> For the <i>ini</i> file, values must be enclosed in single quotation marks.</p>
Web: Debug Recording Destination IP <b>[DebugRecordingDestIP]</b>	Defines the IP address of the server for capturing debug recording.
Web: Debug Recording Destination Port <b>[DebugRecordingDestPort]</b>	Defines the UDP port of the server for capturing debug recording. The default is 925.



Parameter	Description
Debug Recording Status <b>[DebugRecordingStatus]</b>	Activates or de-activates debug recording. <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Stop (default)</li> <li>▪ <b>[1]</b> Start</li> </ul>
<b>Logging Filters Table</b>	
Web: Logging Filters Table <b>[LoggingFilters]</b>	<p>This table parameter defines logging filtering rules for Syslog messages and debug recordings. The format of this parameter is as follows:</p> <p><b>[ LoggingFilters ]</b>  FORMAT LoggingFilters_Index = LoggingFilters_Type,  LoggingFilters_Value, LoggingFilters_Syslog,  LoggingFilters_CaptureType;  <b>[ \LoggingFilters ]</b></p> <p><b>Note:</b> For a detailed description of this table, see "Filtering Syslog Messages and Debug Recordings" on page <a href="#">367</a>.</p>

#### 42.3.4 Resource Allocation Indication Parameters

The Resource Allocation Indication (RAI) parameters are described in the table below.

**Table 42-18: RAI Parameters**

Parameter	Description
<b>[EnableRAI]</b>	<p>Enables RAI alarm generation if the device's busy endpoints exceed a user-defined threshold.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = (Default) Disable RAI (Resource Available Indication) service.</li> <li>▪ <b>[1]</b> = RAI service enabled and an SNMP 'acBoardCallResourcesAlarm' Alarm Trap is sent.</li> </ul>
<b>[RAIHighThreshold]</b>	<p>Defines the high threshold percentage of total calls that are active (busy endpoints). When the percentage of the device's busy endpoints exceeds this high threshold, the device sends the SNMP acBoardCallResourcesAlarm alarm trap with a 'major' alarm status. The range is 0 to 100. The default is 90.</p> <p><b>Note:</b> The percentage of busy endpoints is calculated by dividing the number of busy endpoints by the total number of "enabled" endpoints.</p>
<b>[RAILowThreshold]</b>	<p>Defines the low threshold percentage of total calls that are active (busy endpoints). When the percentage of the device's busy endpoints falls below this low threshold, the device sends an SNMP acBoardCallResourcesAlarm alarm trap with a 'cleared' alarm status. The range is 0 to 100%. The default is 90%.</p>
<b>[RAILoopTime]</b>	<p>Defines the time interval (in seconds) that the device periodically checks call resource availability. The valid range is 1 to 200. The default is 10.</p>



## 42.4 Security Parameters

This subsection describes the device's security parameters.

### 42.4.1 General Parameters

The general security parameters are described in the table below.

**Table 42-19: General Security Parameters**

Parameter	Description
<b>Firewall Table</b>	
Web: Internal Firewall Parameters <b>[AccessList]</b>	<p>This table parameter defines the device's access list (firewall), which defines network traffic filtering rules.</p> <p>The format of this parameter is as follows:  <b>[AccessList]</b>            FORMAT AccessList_Index = AccessList_Source_IP, AccessList_Source_Port, AccessList_PrefixLen, AccessList_Source_Port, AccessList_Start_Port, AccessList_End_Port, AccessList_Protocol, AccessList_Use_Specific_Interface, AccessList_Interface_ID, AccessList_Packet_Size, AccessList_Byte_Rate, AccessList_Byte_Burst, AccessList_Allow_Type;  <b>[AccessList]</b></p> <p>For example:            AccessList 10 = mgmt.customer.com, , 32, 0, 80, tcp, 1, OAMP, 0, 0, 0, allow;            AccessList 22 = 10.4.0.0, , 16, 4000, 9000, any, 0, , 0, 0, 0, block;</p> <p>In the example above, Rule #10 allows traffic from the host 'mgmt.customer.com' destined to TCP ports 0 to 80 on interface OAMP (OAMP). Rule #22 blocks traffic from the subnet 10.4.xxx.yyy destined to ports 4000 to 9000.</p> <p><b>Note:</b> For a description of this table, see "Configuring Firewall Settings" on page 115.</p>

### 42.4.2 HTTPS Parameters

The Secure Hypertext Transport Protocol (HTTPS) parameters are described in the table below.

**Table 42-20: HTTPS Parameters**

Parameter	Description
Web: Secured Web Connection (HTTPS) <b>[HTTPSOnly]</b>	<p>Determines the protocol used to access the Web interface.</p> <ul style="list-style-type: none"> <li><b>[0]</b> HTTP and HTTPS (default).</li> <li><b>[1]</b> HTTPS Only = Unencrypted HTTP packets are blocked.</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
<b>[HTTPSPort]</b>	<p>Defines the local Secured HTTPS port of the device. This parameter allows secure remote device Web management from the LAN. To enable secure Web management from the LAN,</p>



Parameter	Description
	<p>configure the desired port.</p> <p>The valid range is 1 to 65535 (other restrictions may apply within this range). The default port is 443.</p> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
Web/: HTTPS Cipher String [HTTSPSCipherString]	<p>Defines the Cipher string for HTTPS (in OpenSSL cipher list format). For the valid range values, refer to URL <a href="http://www.openssl.org/docs/apps/ciphers.html">http://www.openssl.org/docs/apps/ciphers.html</a>.</p> <p>The default is 'RC4:EXP' (Export encryption algorithms). For example, use 'ALL' for all ciphers suites (e.g., for ARIA encryption for TLS). The only ciphers available are RC4 and DES, and the cipher bit strength is limited to 56 bits.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>If the "Strong Encryption" Software License Key is enabled, the default of this parameter is changed to 'RC4:EXP', enabling RC-128bit encryption.</li> <li>The value 'ALL' can be configured only if the "Strong Encryption" Software License Key is enabled.</li> </ul>
Web: HTTP Authentication Mode [WebAuthMode]	<p>Determines the authentication mode used for the Web interface.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Basic Mode = (Default) Basic authentication (clear text) is used.</li> <li><b>[1]</b> Web Based Authentication = Digest authentication (MD5) is used.</li> </ul> <p><b>Note:</b> If you enable RADIUS login (i.e., the WebRADIUSLogin parameter is set to 1), you must set the WebAuthMode parameter to Basic Mode [0].</p>
<b>Web:</b> Requires Client Certificates for HTTPS connection [HTTPSRequireClientCertificate]	<p>Determines whether client certificates are required for HTTPS connection.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) Client certificates are not required.</li> <li><b>[1]</b> Enable = Client certificates are required. The client certificate must be preloaded to the device and its matching private key must be installed on the managing PC. Time and date must be correctly set on the device for the client certificate to be verified.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>For a description on implementing client certificates, see "Client Certificates" on page 80.</li> </ul>



### 42.4.3 SRTP Parameters

The Secure Real-Time Transport Protocol (SRTP) parameters are described in the table below.

**Table 42-21: SRTP Parameters**

Parameter	Description
Web: Media Security <b>[EnableMediaSecurity]</b>	<p>Enables Secure Real-Time Transport Protocol (SRTP).</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable = (Default) SRTP is disabled.</li> <li>▪ <b>[1]</b> Enable = SRTP is enabled.</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
Web: Media Security Behavior <b>[MediaSecurityBehaviour]</b>	<p>Determines the device's mode of operation when SRTP is used (i.e., when the parameter EnableMediaSecurity is set to 1).</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Preferable = (Default) The device initiates encrypted calls. However, if negotiation of the cipher suite fails, an unencrypted call is established. Incoming calls that don't include encryption information are accepted.</li> <li>▪ <b>[1]</b> Mandatory = The device initiates encrypted calls, but if negotiation of the cipher suite fails, the call is terminated. Incoming calls that don't include encryption information are rejected.</li> <li>▪ <b>[2]</b> Disable = The IP Profile for which this parameter is set does not support encrypted calls (i.e., SRTP).</li> <li>▪ <b>[3]</b> Preferable - Single Media = The device sends SDP with a single media ('m=') line only (e.g., m=audio 6000 RTP/AVP 4 0 70 96) with RTP/AVP and crypto keys. The remote UA can respond with SRTP or RTP parameters: <ul style="list-style-type: none"> <li>✓ If the remote SIP UA does not support SRTP, it uses RTP and ignores the crypto lines.</li> <li>✓ In the opposite direction, if the device receives an SDP offer with a single media (as shown above), it responds with SRTP (RTP/SAVP) if the EnableMediaSecurity parameter is set to 1. If SRTP is not supported (i.e., EnableMediaSecurity is set to 0), it responds with RTP.</li> </ul> </li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ Before configuring this parameter, set the EnableMediaSecurity parameter to 1.</li> <li>▪ If this parameter is set to Preferable <b>[3]</b> and two 'm=' lines are received in the SDP offer, the device prefers the SAVP (secure audio video profile) regardless of the order in the SDP.</li> <li>▪ Option <b>[2]</b> Disable is applicable only to IP Profiles.</li> <li>▪ This parameter can also be configured per IP Profile, using the IPProfile parameter (see "Configuring IP Profiles" on page 189).</li> </ul>
Web: Master Key Identifier (MKI) Size <b>[SRTPTxPacketMKISize]</b>	<p>Defines the size (in bytes) of the Master Key Identifier (MKI) in SRTP Tx packets.</p> <p>The range is 0 to 4. The default is 0 (i.e., new keys are generated without MKI).</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ You can also configure MKI size in an IP Profile.</li> <li>▪ The device can forward MKI size as is for SRTP-to-SRTP flows or override the MKI size during negotiation, using IP Profiles.</li> </ul>



Parameter	Description
	This can be done on the inbound or outbound leg.
Web: Symmetric MKI Negotiation <b>[EnableSymmetricMKI]</b>	<p>Enables symmetric MKI negotiation.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) The device includes the MKI in its 200 OK response according to the SRTPTxPacketMKISize parameter (if set to 0, then it is not included; if set to any other value, it is included with this value).</li> <li><b>[1]</b> Enable = The answer crypto line contains (or excludes) an MKI value according to the selected crypto line in the offer. For example, assume that the device receives an INVITE containing the following two crypto lines in SDP: <pre> a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:TAaxNnQt8/qLQMnDuG4vxYfWl6K7eBK/ufk04pR4  2^31 1:1 a=crypto:3 AES_CM_128_HMAC_SHA1_80 inline:bnuYZnMxSfUiGitviWJZmzr7OF3AiRO0l5Vnh0kH  2^31 </pre> <p>The first crypto line includes the MKI parameter "1:1". In the 200 OK response, the device selects one of the crypto lines (i.e., '2' or '3'). Typically, it selects the first line that supports the crypto suite. However, for SRTP-to-SRTP in SBC sessions, it can be determined by the remote side on the outgoing leg. If the device selects crypto line '2', it includes the MKI parameter in its answer SDP, for example:</p> <pre> a=crypto:2 AES_CM_128_HMAC_SHA1_80 inline:RlVyAlxV/qwBjkEklU4kSJyl3wCtYeZLq1/QFuxw  2^31 1:1 </pre> <p>If the device selects a crypto line that does not contain the MKI parameter, then the MKI parameter is not included in the crypto line in the SDP answer (even if the SRTPTxPacketMKISize parameter is set to any value other than 0).</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>To enable symmetric MKI, the SRTPTxPacketMKISize parameter must be set to any value other than 0.</li> <li>You can also enable MKI negotiation per IP Profile.</li> </ul> </li> </ul>
Web: SRTP offered Suites <b>[SRTPofferedSuites]</b>	<p>Defines the offered crypto suites (cipher encryption algorithms) for SRTP.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) All available crypto suites.</li> <li><b>[1]</b> CIPHER SUITES AES CM 128 HMAC SHA1 80 = device uses AES-CM encryption with a 128-bit key and HMAC-SHA1 message authentication with a 80-bit tag.</li> <li><b>[2]</b> CIPHER SUITES AES CM 128 HMAC SHA1 32 = device uses AES-CM encryption with a 128-bit key and HMAC-SHA1 message authentication with a 32-bit tag.</li> </ul> <p><b>Note:</b> This parameter also affects the selection of the crypto in the device's answer. For example, if the device receives an offer with two crypto lines containing HMAC_SHA1_80 and HMAC_SHA_32, it uses the HMAC_SHA_32 key in its SIP 200 OK response if the parameter is set to 2.</p>
Web: Disable Authentication On Transmitted RTP Packets <b>[RTPAuthenticationDisableTx]</b>	<p>Enables authentication on transmitted RTP packets in a secured RTP session.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Enable (default)</li> <li><b>[1]</b> Disable</li> </ul>



Parameter	Description
Web: Disable Encryption On Transmitted RTP Packets <b>[RTPEncryptionDisableTx]</b>	Enables encryption on transmitted RTP packets in a secured RTP session. <ul style="list-style-type: none"> <li><b>[0]</b> Enable (default)</li> <li><b>[1]</b> Disable</li> </ul>
Web: Disable Encryption On Transmitted RTCP Packets <b>[RTCPEncryptionDisableTx]</b>	Enables encryption on transmitted RTCP packets in a secured RTP session. <ul style="list-style-type: none"> <li><b>[0]</b> Enable (default)</li> <li><b>[1]</b> Disable</li> </ul>
<b>[ResetSRTPStateUponRekey]</b>	Enables synchronization of the SRTP state between the device and a server when a new SRTP key is generated upon a SIP session expire. This feature ensures that the roll-over counter (ROC), one of the parameters used in the SRTP encryption/decryption process of the SRTP packets, is synchronized on both sides for transmit and receive packets. <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) Disabled. ROC is not reset on the device side.</li> <li><b>[1]</b> = Enabled. If the session expires causing a session refresh through a re-INVITE, the device or server generates a new key and the device resets the ROC index (and other SRTP fields) as done by the server, resulting in a synchronized SRTP.</li> </ul> <b>Notes:</b> <ul style="list-style-type: none"> <li>This feature can also be configured for an IP Profile.</li> <li>If this feature is disabled and the server resets the ROC upon a re-key generation, one-way voice may occur.</li> </ul>

#### 42.4.4 TLS Parameters

The Transport Layer Security (TLS) parameters are described in the table below.

**Table 42-22: TLS Parameters**

Parameter	Description
Web: TLS Version <b>[TLSVersion]</b>	Determines the supported versions of SSL/TLS (Secure Socket Layer/Transport Layer Security). <ul style="list-style-type: none"> <li><b>[0]</b> SSL 2.0-3.0 and TLS 1.0 = (Default) SSL 2.0, SSL 3.0, and TLS 1.0 are supported.</li> <li><b>[1]</b> TLS 1.0 Only = only TLS 1.0 is used.</li> </ul> When set to 0, SSL/TLS handshakes always start with SSL 2.0 and switch to TLS 1.0 if both peers support it. When set to 1, TLS 1.0 is the only version supported; clients attempting to contact the device using SSL 2.0 are rejected. <b>Note:</b> For this parameter to take effect, a device reset is required.
Web: TLS Client Re-Handshake Interval <b>[TLSReHandshakeInterval]</b>	Defines the time interval (in minutes) between TLS Re-Handshakes initiated by the device. The interval range is 0 to 1,500 minutes. The default is 0 (i.e., no TLS Re-Handshake).



Parameter	Description
Web: TLS Mutual Authentication <b>[SIPSRequireClientCertificate]</b>	<p>Determines the device's behavior when acting as a server for TLS connections.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) The device does not request the client certificate.</li> <li><b>[1]</b> Enable = The device requires receipt and verification of the client certificate to establish the TLS connection.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>The SIPS certificate files can be changed using the parameters HTTPSCertFileName and HTTPSRootFileName.</li> </ul>
Web: Peer Host Name Verification Mode <b>[PeerHostNameVerificationMode]</b>	<p>Determines whether the device verifies the Subject Name of a remote certificate when establishing TLS connections.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default).</li> <li><b>[1]</b> Server Only = Verify Subject Name only when acting as a client for the TLS connection.</li> <li><b>[2]</b> Server &amp; Client = Verify Subject Name when acting as a server or client for the TLS connection.</li> </ul> <p>When a remote certificate is received and this parameter is not disabled, the value of SubjectAltName is compared with the list of available Proxies. If a match is found for any of the configured Proxies, the TLS connection is established.</p> <p>The comparison is performed if the SubjectAltName is either a DNS name (DNSName) or an IP address. If no match is found and the SubjectAltName is marked as 'critical', the TLS connection is not established. If DNSName is used, the certificate can also use wildcards ("*") to replace parts of the domain name.</p> <p>If the SubjectAltName is not marked as 'critical' and there is no match, the CN value of the SubjectName field is compared with the parameter TLSRemoteSubjectName. If a match is found, the connection is established. Otherwise, the connection is terminated.</p> <p><b>Note:</b> If you set this parameter to <b>[2]</b> (Server &amp; Client), for this functionality to operate, you also need to set the SIPSRequireClientCertificate parameter to <b>[1]</b> (Enable).</p>
Web: TLS Client Verify Server Certificate <b>[VerifyServerCertificate]</b>	<p>Determines whether the device, when acting as a client for TLS connections, verifies the Server certificate. The certificate is verified with the Root CA information.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <p><b>Note:</b> If Subject Name verification is necessary, the parameter PeerHostNameVerificationMode must be used as well.</p>
Web: Strict Certificate Extension Validation <b>[RequireStrictCert]</b>	<p>Enables the validation of the extensions (keyUsage and extendedKeyUsage) of peer certificates. This validation ensures that the signing CA is authorized to sign certificates and that the end-entity certificate is authorized to negotiate a secure TLS connection.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul>
Web: TLS Remote Subject Name	<p>Defines the Subject Name that is compared with the name</p>



Parameter	Description
<b>[TLSRemoteSubjectName]</b>	<p>defined in the remote side certificate when establishing TLS connections.</p> <p>If the SubjectAltName of the received certificate is not equal to any of the defined Proxies Host names/IP addresses and is not marked as 'critical', the Common Name (CN) of the Subject field is compared with this value. If not equal, the TLS connection is not established. If the CN uses a domain name, the certificate can also use wildcards ("*") to replace parts of the domain name.</p> <p>The valid range is a string of up to 49 characters.</p> <p><b>Note:</b> This parameter is applicable only if the parameter PeerHostNameVerificationMode is set to 1 or 2.</p>
Web: Client Cipher String <b>[TLSClientCipherString]</b>	<p>Defines the cipher-suite string for TLS clients.</p> <p>The valid value is up to 255 strings. The default is "ALL:!ADH".</p> <p>For example: TLSClientCipherString = 'EXP'</p> <p>This parameter complements the HTTPSCipherString parameter (which affects TLS servers). For possible values and additional details, refer to: <a href="http://www.openssl.org/docs/apps/ciphers.html">http://www.openssl.org/docs/apps/ciphers.html</a></p>
<b>[TLSPkeySize]</b>	<p>Defines the key size (in bits) for RSA public-key encryption for newly self-signed generated keys for SSH.</p> <ul style="list-style-type: none"> <li>▪ <b>[512]</b></li> <li>▪ <b>[768]</b></li> <li>▪ <b>[1024]</b> (default)</li> <li>▪ <b>[2048]</b></li> </ul>

### 42.4.5 SSH Parameters

Secure Shell (SSH) parameters are described in the table below.

**Table 42-23: SSH Parameters**

Parameter	Description
Web: Enable SSH Server <b>[SSHServerEnable]</b>	<p>Enables the device's embedded SSH server.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul>
Web: Server Port <b>[SSHServerPort]</b>	<p>Defines the port number for the embedded SSH server.</p> <p>Range is any valid port number. The default port is 22.</p>
Web: SSH Admin Key <b>[SSHAdminKey]</b>	<p>Defines the RSA public key for strong authentication for logging in to the SSH interface (if enabled).</p> <p>The value should be a base64-encoded string. The value can be a maximum length of 511 characters.</p>
Web: Require Public Key <b>[SSHRequirePublicKey]</b>	<p>Enables RSA public keys for SSH.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = (Default) RSA public keys are optional if a value is configured for the parameter SSHAdminKey.</li> <li>▪ <b>[1]</b> = RSA public keys are mandatory.</li> </ul> <p><b>Note:</b> To define the key size, use the TLSPkeySize parameter.</p>



Parameter	Description
Web: Max Payload Size <b>[SSHMaxPayloadSize]</b>	Defines the maximum uncompressed payload size (in bytes) for SSH packets. The valid value is 550 to 32768. The default is 32768.
Web: Max Binary Packet Size <b>[SSHMaxBinaryPacketSize]</b>	Defines the maximum packet size (in bytes) for SSH packets. The valid value is 582 to 35000. The default is 35000.
<b>[SSHMaxSessions]</b>	Defines the maximum number of simultaneous SSH sessions. The valid range is 1 to 2. The default is 2 sessions.
Web: Enable Last Login Message <b>[SSHEnableLastLoginMessage]</b>	Enables message display in SSH sessions of the time and date of the last SSH login. The SSH login message displays the number of unsuccessful login attempts since the last successful login. <ul style="list-style-type: none"> <li><b>[0]</b> Disable</li> <li><b>[1]</b> Enable (default)</li> </ul> <b>Note:</b> The last SSH login information is cleared when the device is reset.
Web: Max Login Attempts <b>[SSHMaxLoginAttempts]</b>	Defines the maximum SSH login attempts allowed for entering an incorrect password by an administrator before the SSH session is rejected. The valid range is 1 to 3. the default is 3.

## 42.4.6 OCSP Parameters

The Online Certificate Status Protocol (OCSP) parameters are described in the table below.

**Table 42-24: OCSP Parameters**

Parameter	Description
Web: Enable OCSP Server <b>[OCSPEnable]</b>	Enables or disables certificate checking using OCSP. <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul>
Web: Primary Server IP <b>[OCSPServerIP]</b>	Defines the IP address of the OCSP server. The default IP address is 0.0.0.0.
Web: Secondary Server IP <b>[OCSPSecondaryServerIP]</b>	Defines the IP address (in dotted-decimal notation) of the secondary OCSP server (optional). The default IP address is 0.0.0.0.
Web: Server Port <b>[OCSPServerPort]</b>	Defines the OCSP server's TCP port number. The default port number is 2560.
Web: Default Response When Server Unreachable <b>[OCSPDefaultResponse]</b>	Determines the default OCSP behavior when the server cannot be contacted. <ul style="list-style-type: none"> <li><b>[0]</b> Reject = (Default) Rejects peer certificate.</li> <li><b>[1]</b> Allow = Allows peer certificate.</li> </ul>



## 42.4.7 IDS Parameters

The Intrusion Detection System (IDS) parameters are described in the table below.

**Table 42-25: IDS Parameters**

Parameter	Description
Web: Intrusion Detection System (IDS) CLI: enable-ids <b>[EnableIDS]</b>	Enables the IDS feature. <ul style="list-style-type: none"> <li>[0] Disable (default)</li> <li>[1] Enable</li> </ul> <b>Note:</b> For this parameter to take effect, a device reset is required.
CLI: ids-clear-period <b>[IDSArmClearPeriod]</b>	Defines the interval (in seconds) after which an IDS alarm is cleared from the Active Alarms table if no thresholds are crossed during this time. However, this "quiet" period must be at least twice the Threshold Window value. For example, if IDSArmClearPeriod is set to 20 sec and the Threshold Window is set to 15 sec, the IDSArmClearPeriod parameter is ignored and the alarm is cleared only after 30 seconds (2 x 15 sec). The valid value is 0 to 86400. The default is 300.
<b>IDS Policy Table</b>	
Web: IDS Policy Table <b>[IDSPolicy]</b>	Defines IDS Policies. The format of the ini file parameter is: [ IDSPolicy ] FORMAT IDSPolicy_Index = IDSPolicy_Name, IDSPolicy_Description; [ \IDSPolicy ] For a detailed description of this table, see 'Configuring IDS Policies' on page 122.
<b>IDS Rule Table</b>	
Web: IDS Rule Table <b>[IDSRule]</b>	Defines rules for the IDS Policies. The format of the ini file parameter is: [ IDSRule ] FORMAT IDSRule_Index = IDSRule_Policy, IDSRule_RuleID, IDSRule_Reason, IDSRule_ThresholdScope, IDSRule_ThresholdWindow, IDSRule_MinorAlarmThreshold, IDSRule_MajorAlarmThreshold, IDSRule_CriticalAlarmThreshold; [ \IDSRule ] For a detailed description of this table, see 'Configuring IDS Policies' on page 122.
<b>IDS Match Table</b>	
Web: IDS Match Table <b>[IDSMatch]</b>	Defines target rules per IDS Policy. The format of the ini file parameter is: [ IDSMatch ] FORMAT IDSMatch_Index = IDSMatch_SIPInterface, IDSMatch_ProxySet, IDSMatch_Subnet, IDSMatch_Policy; [ \IDSMatch ] For a detailed description of this table, see 'Assigning IDS Policies' on page 125.



## 42.5 RADIUS Parameters

The RADIUS parameters are described in the table below.

**Table 42-26: RADIUS Parameters**

Parameter	Description
<b>RADIUS Accounting Parameters</b>	
Web: Enable RADIUS Access Control <b>[EnableRADIUS]</b>	<p>Enables the RADIUS application.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (Default)</li> <li>▪ <b>[1]</b> Enable</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
Web: Accounting Server IP Address <b>[RADIUSAccServerIP]</b>	Defines the IP address of the RADIUS accounting server.
Web: Accounting Port <b>[RADIUSAccPort]</b>	<p>Defines the port of the RADIUS accounting server.</p> <p>The default is 1646.</p>
Web: RADIUS Accounting Type <b>[RADIUSAccountingType]</b>	<p>Determines when the RADIUS accounting messages are sent to the RADIUS accounting server.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> At Call Release = (Default) Sent at call release only.</li> <li>▪ <b>[1]</b> At Connect &amp; Release = Sent at call connect and release.</li> <li>▪ <b>[2]</b> At Setup &amp; Release = Sent at call setup and release.</li> </ul>
Web: AAA Indications <b>[AAAIIndications]</b>	<p>Determines the Authentication, Authorization and Accounting (AAA) indications.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> None = (Default) No indications.</li> <li>▪ <b>[3]</b> Accounting Only = Only accounting indications are used.</li> </ul>
<b>General RADIUS Parameters</b>	
Web: Use RADIUS for Web/Telnet Login <b>[WebRADIUSLogin]</b>	<p>Enables RADIUS queries for Web and Telnet login authentication. When enabled, logging into the device's Web and Telnet embedded servers is done through a RADIUS server. The device communicates with a user-defined RADIUS server and verifies the given username and password against a remote database, in a secure manner.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ For RADIUS login authentication to function, you also need to set the following parameters: <ul style="list-style-type: none"> <li>✓ EnableRADIUS = 1 (Enable)</li> <li>✓ WebAuthMode = 0 (Basic Mode)</li> </ul> </li> <li>▪ RADIUS authentication requires HTTP basic authentication, where the username and password are transmitted in clear text over the network. Therefore, it's recommended to set the HTTPSONly parameter to 1 in order to force the use of HTTPS, since the transport is encrypted.</li> <li>▪ If using RADIUS authentication to log into the CLI, only the primary Web User Account, which has Security Administration access level, can access the device's CLI (see 'Configuring Web User Accounts' on page 46).</li> </ul>
Web: RADIUS Authentication	Defines the IP address of the RADIUS authentication server.



Parameter	Description
Server IP Address <b>[RADIUSAuthServerIP]</b>	<b>Note:</b> For this parameter to take effect, a device reset is required.
Web: RADIUS Authentication Server Port <b>[RADIUSAuthPort]</b>	Defines the port of the RADIUS Authentication Server. <b>Note:</b> For this parameter to take effect, a device reset is required.
Web: RADIUS Shared Secret <b>[SharedSecret]</b>	Defines the 'Secret' used to authenticate the device to the RADIUS server. This should be a cryptically strong password.
<b>RADIUS Authentication Parameters</b>	
Web: Default Access Level <b>[DefaultAccessLevel]</b>	Defines the default access level for the device when the RADIUS (authentication) response doesn't include an access level attribute. The valid range is 0 to 255. The default is 200 (i.e., Security Administrator).
Web: Device Behavior Upon RADIUS Timeout <b>[BehaviorUponRadiusTimeout]</b>	Defines the device's response upon a RADIUS timeout. <ul style="list-style-type: none"> <li><b>[0]</b> Deny Access = Denies access.</li> <li><b>[1]</b> Verify Access Locally = (Default) Checks password locally.</li> </ul>
Web: Local RADIUS Password Cache Mode <b>[RadiusLocalCacheMode]</b>	Determines the device's mode of operation regarding the timer (configured by the parameter RadiusLocalCacheTimeout) that determines the validity of the user name and password (verified by the RADIUS server). <ul style="list-style-type: none"> <li><b>[0]</b> Absolute Expiry Timer = When you access a Web page, the timeout doesn't reset, instead it continues decreasing.</li> <li><b>[1]</b> Reset Timer Upon Access = (Default) Upon each access to a Web page, the timeout always resets (reverts to the initial value configured by RadiusLocalCacheTimeout).</li> </ul>
Web: Local RADIUS Password Cache Timeout <b>[RadiusLocalCacheTimeout]</b>	Defines the time (in seconds) the locally stored user name and password (verified by the RADIUS server) are valid. When this time expires, the user name and password become invalid and a must be re-verified with the RADIUS server. The valid range is 1 to 0xFFFFFFFF. The default is 300 (5 minutes). <ul style="list-style-type: none"> <li><b>[-1]</b> = Never expires.</li> <li><b>[0]</b> = Each request requires RADIUS authentication.</li> </ul>
Web: RADIUS VSA Vendor ID <b>[RadiusVSAVendorID]</b>	Defines the vendor ID that the device accepts when parsing a RADIUS response packet. The valid range is 0 to 0xFFFFFFFF. The default is 5003.
Web: RADIUS VSA Access Level Attribute <b>[RadiusVSAAccessAttribute]</b>	Defines the code that indicates the access level attribute in the Vendor Specific Attributes (VSA) section of the received RADIUS packet. The valid range is 0 to 255. The default is 35.
<b>[MaxRADIUSSessions]</b>	Defines the number of concurrent calls that can communicate with the RADIUS server (optional). The valid range is 0 to 240. The default is 240.
<b>[RADIUSRetransmission]</b>	Defines the number of retransmission retries. The valid range is 1 to 10. The default is 3.



Parameter	Description
[RadiusTO]	Defines the time interval (measured in seconds) that the device waits for a response before a RADIUS retransmission is issued. The valid range is 1 to 30. The default is 10.

## 42.6 SIP Media Realm Parameters

The Media Realm parameters are described in the table below.

**Table 42-27: Media Realm Parameters**

Parameter	Description
<b>Media Realm Table</b>	
Web: Media Realm Table [CpMediaRealm]	<p>This table parameter defines the Media Realm table. The Media Realm table allows you to divide a Media-type interface (defined in the Multiple Interface table) into several realms, where each realm is specified by a UDP port range.</p> <p>The format of this parameter is as follows:</p> <p>[CpMediaRealm]            FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName, CpMediaRealm_IPv4IF, CpMediaRealm_IPv6IF, CpMediaRealm_PortRangeStart, CpMediaRealm_MediaSessionLeg, CpMediaRealm_PortRangeEnd, CpMediaRealm_TransRateRatio, CpMediaRealm_IsDefault;            \CpMediaRealm]</p> <p>For example,            CpMediaRealm 1 = Mrealm1, Voice, , 6600, 20, 6790, , 1;            CpMediaRealm 2 = Mrealm2, Voice, , 6800, 10, 6890; , 0;</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>For a detailed description of this table, see "Configuring Media Realms" on page 130.</li> </ul>
<b>Bandwidth Management per Media Realm Table</b>	
Web: Bandwidth Management [BWManagement]	<p>This table parameter defines bandwidth management rules per Media Realm.</p> <p>The format of this parameter is as follows:</p> <p>[ BWManagement ]            FORMAT BWManagement_Index = BWManagement_MediaRealmIndex, BWManagement_ThresholdIndex, BWManagement_RuleAction, BWManagement_Threshold, BWManagement_Hysteresis;            \ BWManagement ]</p> <p>Where ThresholdIndex is the bandwidth threshold rule type:</p> <ul style="list-style-type: none"> <li><b>[0]</b> High Threshold Rule</li> <li><b>[1]</b> Critical Threshold Rule</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>This table can include up to two row entries (where 0 is the first</li> </ul>



Parameter	Description
	index). <ul style="list-style-type: none"> <li>For a detailed description of this table, see "Configuring Bandwidth Management per Media Realm" on page 135.</li> </ul>
Quality of Experience Parameters	
Web: Server IP CLI: server-ip <b>[QOEServerIP]</b>	Defines the IP address of AudioCodes Session Experience Manager (SEM) server to where the quality experience reports are sent. <b>Note:</b> For this parameter to take effect, a device reset is required.
Web: Port <b>[QOEPort]</b>	Defines the port of the SEM server. The valid value range is 0 to 65534. The default is 5000.
Web: Interface Name <b>[QOEInterfaceName]</b>	Defines the IP network interface on which the quality experience reports are sent. The default is the OAMP interface. <b>Note:</b> For this parameter to take effect, a device reset is required.
Web: Connection Mode <b>[QOEConnectionMode]</b>	Defines the connection between the device and the SEM. <ul style="list-style-type: none"> <li><b>[0]</b> Server = The device receives connection from the server.</li> <li><b>[1]</b> Client (default) = The device connects to the SEM.</li> <li><b>[2]</b> None</li> </ul> <b>Note:</b> Currently, only the client connection is supported.
Web: Information Level <b>[QOEInformationLevel]</b>	Defines the level (i.e., amount of detail) of voice quality information that is sent to the SEM server. <ul style="list-style-type: none"> <li><b>[0]</b> Standard (default)</li> <li><b>[1]</b> Enhanced</li> <li><b>[2]</b> Debug</li> </ul>
Web: Use Mos LQ <b>[QOEUseMosLQ]</b>	Enables the reporting of the MOS-LQ (listening quality). If disabled, the MOS-CQ (conversational quality) is reported. MOS-LQ measures the quality of audio for listening purposes only. MOS-LQ does not take into account bi-directional effects such as delay and echo. MOS-CQ takes into account listening quality in both directions, as well as the bi-directional effects. <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul>
Media Realm > Quality of Experience Table	
Web: Media Realm > Quality Of Experience <b>[QOERules]</b>	This table configures Quality of Experience parameters per Media Realm. <b>[ QOERules ]</b> ORMAT QOERules_Index = QOERules_MediaRealmIndex, QOERules_RuleIndex, QOERules_MonitoredParam, QOERules_Direction, QOERules_Profile, QOERules_GreenYellowThreshold, QOERules_GreenYellowHysteresis, QOERules_YellowRedThreshold, QOERules_YellowRedHysteresis, QOERules_GreenYellowOperation, QOERules_GreenYellowOperationDetails, QOERules_YellowRedOperation, QOERules_YellowRedOperationDetails; <b>[ \QOERules ]</b> <b>Note:</b> For a detailed description of this table, see Configuring Quality of Experience Parameters per Media Realm on page 132.



## 42.7 Control Network Parameters

### 42.7.1 IP Group, Proxy, Registration and Authentication Parameters

The proxy server, registration and authentication SIP parameters are described in the table below.

**Table 42-28: Proxy, Registration and Authentication SIP Parameters**

Parameter	Description
<b>IP Group Table</b>	
Web: IP Group Table <b>[IPGroup]</b>	<p>This table configures IP Groups.</p> <p>The ini file format of this parameter is as follows:</p> <pre>[IPGroup] FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Description, IPGroup_ProxySetId, IPGroup_SIPGroupName, IPGroup_ContactUser, IPGroup_EnableSurvivability, IPGroup_ServingIPGroup, IPGroup_SipReRoutingMode, IPGroup_AlwaysUseRouteTable, IPGroup_RoutingMode, IPGroup_SRD, IPGroup_MediaRealm, IPGroup_ClassifyByProxySet, IPGroup_ProfileId, IPGroup_MaxNumOfRegUsers, IPGroup_InboundManSet, IPGroup_OutboundManSet, IPGroup_RegistrationMode, IPGroup_AuthenticationMode, IPGroup_MethodList, IPGroup_EnableSBCCClientForking, IPGroup_SourceUriInput, IPGroup_DestUriInput, IPGroup_ContactName; [/IPGroup]</pre> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>For a description of this table, see "Configuring IP Groups" on page 164.</li> </ul>
<b>Account Table</b>	
Web: Account Table <b>[Account]</b>	<p>This table parameter configures the Account table for registering and/or authenticating (digest) IP Groups (e.g., an IP-PBX) to another IP Group (e.g., an Internet Telephony Service Provider - ITSP). The format of this parameter is as follows:</p> <pre>[Account] FORMAT Account_Index = Account_ServedTrunkGroup, Account_ServedIPGroup, Account_ServingIPGroup, Account_Username, Account_Password, Account_HostName, Account_Register, Account_ContactUser, Account_ApplicationType; [/Account]</pre> <p>For example: Account 1 = 1, -1, 1, user, 1234, acl, 1, ITSP1;</p> <p><b>Note:</b> For a detailed description of this table, see "Configuring Account Table" on page 177.</p>
<b>Proxy Registration Parameters</b>	
Web: Use Default Proxy <b>[IsProxyUsed]</b>	<p>Enables the use of a SIP proxy server.</p> <ul style="list-style-type: none"> <li><b>[0]</b> No = (Default) Proxy isn't used and instead, the internal routing table is used.</li> </ul>



Parameter	Description
	<ul style="list-style-type: none"> <li><b>[1]</b> Yes = Proxy server is used. Define the IP address of the proxy server in the Proxy Sets table (see "Configuring Proxy Sets Table" on page 171).</li> </ul> <p><b>Note:</b> If you are not using a proxy server, you must define outbound IP call routing rules in the IP-to-IP Routing table (see Configuring SBC IP-to-IP Routing on page 236).</p>
Web: Proxy Name <b>[ProxyName]</b>	<p>Defines the Home Proxy domain name. If specified, this name is used as the Request-URI in REGISTER, INVITE and other SIP messages, and as the host part of the To header in INVITE messages. If not specified, the Proxy IP address is used instead.</p> <p>The valid value is a string of up to 49 characters.</p> <p><b>Note:</b> This parameter functions together with the UseProxyIPasHost parameter.</p>
Web: Use Proxy IP as Host <b>[UseProxyIPasHost]</b>	<p>Enables the use of the proxy server's IP address (in dotted-decimal notation) as the host name in SIP From and To headers in REGISTER requests.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <p>If this parameter is disabled and the device registers to an IP Group (i.e., proxy server), it uses the string configured by the ProxyName parameter as the host name in the REGISTER's Request-URI and uses the string configured by the IP Group table parameter, SIPGroupName as the host name in the To and From headers. If the IP Group is configured with a Proxy Set that has multiple IP addresses, all the REGISTER messages sent to these proxies are sent with the same host name.</p> <p><b>Note:</b> If this parameter is disabled and the ProxyName parameter is not configured, the proxy's IP address is used as the host name in the REGISTER Request-URI.</p>
Web: Redundancy Mode <b>[ProxyRedundancyMode]</b>	<p>Determines whether the device switches back to the primary Proxy after using a redundant Proxy.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Parking = (Default) The device continues working with a redundant (now active) Proxy until the next failure, after which it works with the next redundant Proxy.</li> <li><b>[1]</b> Homing = The device always tries to work with the primary Proxy server (i.e., switches back to the primary Proxy whenever it's available).</li> </ul> <p><b>Note:</b> To use this Proxy Redundancy mechanism, you need to enable the keep-alive with Proxy option, by setting the parameter EnableProxyKeepAlive to 1 or 2.</p>
Web: Proxy IP List Refresh Time <b>[ProxyIPListRefreshTime]</b>	<p>Defines the time interval (in seconds) between each Proxy IP list refresh.</p> <p>The range is 5 to 2,000,000. The default interval is 60.</p>
Web: Always Use Proxy <b>[AlwaysSendToProxy]</b>	<p>Determines whether the device sends SIP messages and responses through a Proxy server.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) Use standard SIP routing rules.</li> <li><b>[1]</b> Enable = All SIP messages and responses are sent to the Proxy server.</li> </ul>



Parameter	Description
	<p><b>Note:</b> This parameter is applicable only if a Proxy server is used (i.e., the parameter IsProxyUsed is set to 1).</p>
Web: DNS Query Type [DNSQueryType]	<p>Enables the use of DNS Naming Authority Pointer (NAPTR) and Service Record (SRV) queries to resolve Proxy and Registrar servers and to resolve all domain names that appear in the SIP Contact and Record-Route headers.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> A-Record (default)</li> <li>▪ <b>[1]</b> SRV</li> <li>▪ <b>[2]</b> NAPTR</li> </ul> <p>If set to A-Record <b>[0]</b>, no NAPTR or SRV queries are performed.</p> <p>If set to SRV <b>[1]</b> and the Proxy/Registrar IP address parameter, Contact/Record-Route headers, or IP address defined in the Routing tables contain a domain name, an SRV query is performed. The device uses the first host name received from the SRV query. The device then performs a DNS A-record query for the host name to locate an IP address.</p> <p>If set to NAPTR <b>[2]</b>, an NAPTR query is performed. If it is successful, an SRV query is sent according to the information received in the NAPTR response. If the NAPTR query fails, an SRV query is performed according to the configured transport type.</p> <p>If the Proxy/Registrar IP address parameter, the domain name in the Contact/Record-Route headers, or the IP address defined in the Routing tables contain a domain name with port definition, the device performs a regular DNS A-record query.</p> <p>If a specific Transport Type is defined, a NAPTR query is not performed.</p> <p><b>Note:</b> To enable NAPTR/SRV queries for Proxy servers only, use the parameter ProxyDNSQueryType.</p>
Web: Proxy DNS Query Type [ProxyDNSQueryType]	<p>Enables the use of DNS Naming Authority Pointer (NAPTR) and Service Record (SRV) queries to discover Proxy servers.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> A-Record (default)</li> <li>▪ <b>[1]</b> SRV</li> <li>▪ <b>[2]</b> NAPTR</li> </ul> <p>If set to A-Record <b>[0]</b>, no NAPTR or SRV queries are performed.</p> <p>If set to SRV <b>[1]</b> and the Proxy IP address parameter contains a domain name without port definition (e.g., ProxyIP = domain.com), an SRV query is performed. The SRV query returns up to four Proxy host names and their weights. The device then performs DNS A-record queries for each Proxy host name (according to the received weights) to locate up to four Proxy IP addresses. Therefore, if the first SRV query returns two domain names and the A-record queries return two IP addresses each, no additional searches are performed.</p> <p>If set to NAPTR <b>[2]</b>, an NAPTR query is performed. If it is successful, an SRV query is sent according to the information received in the NAPTR response. If the NAPTR query fails, an SRV query is performed according to the configured transport type.</p> <p>If the Proxy IP address parameter contains a domain name</p>



Parameter	Description
	<p>with port definition (e.g., ProxyIP = domain.com:5080), the device performs a regular DNS A-record query.</p> <p>If a specific Transport Type is defined, a NAPTR query is not performed.</p> <p><b>Note:</b> When enabled, NAPTR/SRV queries are used to discover Proxy servers even if the parameter DNSQueryType is disabled.</p>
Web: Password <b>[Password]</b>	<p>Defines the password for Basic/Digest authentication with a Proxy/Registrar server. A single password is used for all device ports.</p> <p>The default is 'Default_Passwd'.</p>
Web: Cnonce <b>[Cnonce]</b>	<p>Defines the Cnonce string used by the SIP server and client to provide mutual authentication.</p> <p>The value is free format, i.e., 'Cnonce = 0a4f113b'. The default is 'Default_Cnonce'.</p>
Web: Mutual Authentication Mode <b>[MutualAuthenticationMode]</b>	<p>Determines the device's mode of operation when Authentication and Key Agreement (AKA) Digest Authentication is used.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Optional = (Default) Incoming requests that don't include AKA authentication information are accepted.</li> <li>▪ <b>[1]</b> Mandatory = Incoming requests that don't include AKA authentication information are rejected.</li> </ul>
<b>Proxy IP Table</b>	
Web: Proxy IP Table <b>[ProxyIP]</b>	<p>This table parameter configures the Proxy Set table with Proxy Set IDs, each with up to five Proxy server IP addresses (or fully qualified domain name/FQDN). Each Proxy Set can be defined with a transport type (UDP, TCP, or TLS). The format of this parameter is as follows:</p> <p>[ProxyIP]            FORMAT ProxyIp_Index = ProxyIp_IpAddress,            ProxyIp_TransportType, ProxyIp_ProxySetId;            [\ProxyIP]</p> <p>For example:            ProxyIp 0 = 10.33.37.77, -1, 0;            ProxyIp 1 = 10.8.8.10, 0, 2;            ProxyIp 2 = 10.5.6.7, -1, 1;</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ To assign various attributes (such as Proxy Load Balancing) per Proxy Set ID, use the parameter ProxySet.</li> <li>▪ For a description of this table, see "Configuring Proxy Sets Table" on page 171.</li> </ul>
<b>Proxy Set Table</b>	
Web: Proxy Set Table <b>[ProxySet]</b>	<p>This table parameter configures the Proxy Set ID table. It is used in conjunction with the ProxyIP table ini file parameter, which defines the IP addresses per Proxy Set ID.</p> <p>The ProxySet table ini file parameter defines additional attributes per Proxy Set ID. This includes, for example, Proxy keep-alive and load balancing and redundancy mechanisms (if a Proxy Set contains more than one proxy address).</p>



Parameter	Description
	<p>The format of this parameter is as follows:</p> <p>[ProxySet]            FORMAT ProxySet_Index = ProxySet_EnableProxyKeepAlive,            ProxySet_ProxyKeepAliveTime,            ProxySet_ProxyLoadBalancingMethod,            ProxySet_IsProxyHotSwap, ProxySet_SRD,            ProxySet_ClassificationInput,            ProxySet_ProxyRedundancyMode;            [\ProxySet]</p> <p>For example:            ProxySet 0 = 0, 60, 0, 0, 0, , 1;            ProxySet 1 = 1, 60, 1, 0, 1, , 0;</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For configuring the Proxy Set IDs and their IP addresses, use the parameter ProxyIP.</li> <li>For a description of this table, see "Configuring Proxy Sets Table" on page 171.</li> </ul>
<b>Registrar Parameters</b>	
Web: Registration Time [RegistrationTime]	<p>Defines the time interval (in seconds) for registering to a Proxy server. The value is used in the SIP Expires header. This parameter also defines the time interval between Keep-Alive messages when the parameter EnableProxyKeepAlive is set to 2 (REGISTER).</p> <p>Typically, the device registers every 3,600 sec (i.e., one hour). The device resumes registration according to the parameter RegistrationTimeDivider.</p> <p>The valid range is 10 to 2,000,000. The default is 180.</p>
Web: Re-registration Timing [%] [RegistrationTimeDivider]	<p>Defines the re-registration timing (in percentage). The timing is a percentage of the re-register timing set by the Registrar server.</p> <p>The valid range is 50 to 100. The default is 50.</p> <p>For example: If this parameter is set to 70% and the Registration Expires time is 3600, the device re-sends its registration request after 3600 x 70% (i.e., 2520 sec).</p> <p><b>Note:</b> This parameter may be overridden if the parameter RegistrationTimeThreshold is greater than 0.</p>
Web: Registration Retry Time [RegistrationRetryTime]	<p>Defines the time interval (in seconds) after which a registration request is re-sent if registration fails with a 4xx response or if there is no response from the Proxy/Registrar server.</p> <p>The default is 30 seconds. The range is 10 to 3600.</p>
Web: Registration Time Threshold [RegistrationTimeThreshold]	<p>Defines a threshold (in seconds) for re-registration timing. If this parameter is greater than 0, but lower than the computed re-registration timing (according to the parameter RegistrationTimeDivider), the re-registration timing is set to the following: timing set by the Registration server in the SIP Expires header minus the value of the parameter RegistrationTimeThreshold.</p> <p>The valid range is 0 to 2,000,000. The default is 0.</p>
Web: Re-register On INVITE Failure [RegisterOnInviteFailure]	<p>Enables immediate re-registration if no response is received for an INVITE request sent by the device.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> </ul>



Parameter	Description
	<ul style="list-style-type: none"> <li>▪ <b>[1] Enable</b> When enabled, the device immediately expires its re-registration timer and commences re-registration to the same Proxy upon any of the following scenarios: <ul style="list-style-type: none"> <li>▪ The response to an INVITE request is 407 (Proxy Authentication Required) without an authentication header included.</li> <li>▪ The remote SIP UA abandons a call before the device has received any provisional response (indicative of an outbound proxy server failure).</li> <li>▪ The remote SIP UA abandons a call and the only provisional response the device has received for the call is 100 Trying (indicative of a home proxy server failure, i.e., the failure of a proxy in the route after the outbound proxy).</li> <li>▪ The device terminates a call due to the expiration of RFC 3261 Timer B or due to the receipt of a 408 (Request Timeout) response and the device has not received any provisional response for the call (indicative of an outbound proxy server failure).</li> <li>▪ The device terminates a call due to the receipt of a 408 (Request Timeout) response and the only provisional response the device has received for the call is the 100 Trying provisional response (indicative of a home proxy server failure).</li> </ul> </li> </ul>
Web: ReRegister On Connection Failure <b>[ReRegisterOnConnectionFailure]</b>	<p>Enables the device to perform SIP re-registration upon TCP/TLS connection failure.</p> <ul style="list-style-type: none"> <li>▪ <b>[0] Disable (default)</b></li> <li>▪ <b>[1] Enable</b></li> </ul>
<b>[UnregistrationMode]</b>	<p>Enables the device to perform explicit unregisters.</p> <ul style="list-style-type: none"> <li>▪ <b>[0] Disable (default)</b></li> <li>▪ <b>[1] Enable</b> = The device sends an asterisk ("*") value in the SIP Contact header, instructing the Registrar server to remove all previous registration bindings. The device removes SIP User Agent (UA) registration bindings in a Registrar, according to RFC 3261. Registrations are soft state and expire unless refreshed, but they can also be explicitly removed. A client can attempt to influence the expiration interval selected by the Registrar. A UA requests the immediate removal of a binding by specifying an expiration interval of "0" for that contact address in a REGISTER request. UA's should support this mechanism so that bindings can be removed before their expiration interval has passed. Use of the "*" Contact header field value allows a registering UA to remove all bindings associated with an address-of-record (AOR) without knowing their precise values.</li> </ul> <p><b>Note:</b> The REGISTER-specific Contact header field value of "*" applies to all registrations, but it can only be used if the Expires header field is present with a value of "0".</p>
Web: Add Empty Authorization Header <b>[EmptyAuthorizationHeader]</b>	<p>Enables the inclusion of the SIP Authorization header in initial registration (REGISTER) requests sent by the device.</p> <ul style="list-style-type: none"> <li>▪ <b>[0] Disable (default)</b></li> </ul>



Parameter	Description
	<ul style="list-style-type: none"> <li>▪ <b>[1] Enable</b></li> </ul> <p>The Authorization header carries the credentials of a user agent (UA) in a request to a server. The sent REGISTER message populates the Authorization header with the following parameters:</p> <ul style="list-style-type: none"> <li>▪ username - set to the value of the private user identity</li> <li>▪ realm - set to the domain name of the home network</li> <li>▪ uri - set to the SIP URI of the domain name of the home network</li> <li>▪ nonce - set to an empty value</li> <li>▪ response - set to an empty value</li> </ul> <p>For example:</p> <pre>Authorization: Digest username=alice_private@homel.net, realm="homel.net", nonce="", response="e56131d19580cd833064787ecc"</pre> <p><b>Note:</b> This registration header is according to the IMS 3GPP TS24.229 and PKT-SP-24.220 specifications.</p>
Web: Add initial Route Header <b>[InitialRouteHeader]</b>	<p>Enables the inclusion of the SIP Route header in initial registration or re-registration (REGISTER) requests sent by the device.</p> <ul style="list-style-type: none"> <li>▪ <b>[0] Disable (default)</b></li> <li>▪ <b>[1] Enable</b></li> </ul> <p>When the device sends a REGISTER message, the Route header includes either the Proxy's FQDN, or IP address and port according to the configured Proxy Set, for example:</p> <pre>Route: &lt;sip:10.10.10.10;lr;transport=udp&gt;</pre> <p>or</p> <pre>Route: &lt;sip: pcscf- gm.ims.rr.com;lr;transport=udp&gt;</pre>
<b>[UsePingPongKeepAlive]</b>	<p>Enables the use of the carriage-return and line-feed sequences (CRLF) Keep-Alive mechanism, according to RFC 5626 "Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)" for reliable, connection-orientated transport types such as TCP.</p> <ul style="list-style-type: none"> <li>▪ <b>[0] Disable (default)</b></li> <li>▪ <b>[1] Enable</b></li> </ul> <p>The SIP user agent/client (i.e., device) uses a simple periodic message as a keep-alive mechanism to keep their flow to the proxy or registrar alive (used for example, to keep NAT bindings open). For connection-oriented transports such as TCP/TLS this is based on CRLF. This mechanism uses a client-to-server "ping" keep-alive and a corresponding server-to-client "pong" message. This ping-pong sequence allows the client, and optionally the server, to tell if its flow is still active and useful for SIP traffic. If the client does not receive a pong in response to its ping, it declares the flow "dead" and opens a new flow in its place. In the CRLF Keep-Alive mechanism the client periodically (defined by the PingPongKeepAliveTime parameter) sends a double-CRLF (the "ping") then waits to receive a single CRLF (the "pong"). If the client does not receive a "pong" within an appropriate amount of time, it</p>



Parameter	Description
	considers the flow failed. <b>Note:</b> The device sends a CRLF message to the Proxy Set only if the Proxy Keep-Alive feature (EnableProxyKeepAlive parameter) is enabled and its transport type is set to TCP or TLS. The device first sends a SIP OPTION message to establish the TCP/TLS connection and if it receives any SIP response, it continues sending the CRLF keep-alive sequences.
<b>[PingPongKeepAliveTime]</b>	Defines the periodic interval (in seconds) after which a "ping" (double-CRLF) keep-alive is sent to a proxy/registrar, using the CRLF Keep-Alive mechanism.  The default range is 5 to 2,000,000. The default is 120.  The device uses the range of 80-100% of this user-defined value as the actual interval. For example, if the parameter value is set to 200 sec, the interval used is any random time between 160 to 200 seconds. This prevents an "avalanche" of keep-alive by multiple SIP UAs to a specific server.

## 42.7.2 Network Application Parameters

The SIP network application parameters are described in the table below.

**Table 42-29: SIP Network Application Parameters**

Parameter	Description
<b>Signaling Routing Domain Table</b>	
Web: SRD Settings <b>[SRD]</b>	This table parameter configures the Signaling Routing Domain (SRD) table. The format of this parameter is as follows:  [SRD] FORMAT SRD_Index = SRD_Name, SRD_MediaRealm, SRD_IntraSRDMediaAnchoring, SRD_BlockUnRegUsers, SRD_MaxNumOfRegUsers, SRD_EnableUnAuthenticatedRegistrations; [SRD]  For example: SRD 1 = LAN1_SRD, Mrealm1, 0, 1, 15, 1; SRD 2 = LAN2_SRD, Mrealm2, 0, 1, 15, 1;  <b>Note:</b> For a detailed description of this table, see "Configuring SRD Table" on page 159.
<b>SIP Interface Table</b>	
Web: SIP Interface Table <b>[SIPInterface]</b>	This table parameter configures the SIP Interface table. The SIP Interface represents a SIP signaling entity, comprising ports (UDP, TCP, and TLS) and associated with a specific IP interface and an SRD ID. The format of this parameter is as follows:  [SIPInterface] FORMAT SIPInterface_Index = SIPInterface_NetworkInterface, SIPInterface_ApplicationType, SIPInterface_UDPPort, SIPInterface_TCPPort, SIPInterface_TLSPort, SIPInterface_SRD, SIPInterface_MessagePolicy, SIPInterface_TLSMutualAuthentication, SIPInterface_TCPKeepaliveEnable,



Parameter	Description
	<p>SIPInterface_ClassificationFailureResponseType; [\SIPInterface]</p> <p><b>Note:</b> For a detailed description of this table, see "Configuring SIP Interface Table" on page 161.</p>
<p>TCP Keep Alive Idle Time [TCPKeepAliveTime]</p>	<p>Defines the interval (in sec) between the last data packet sent and the first keep-alive probe to send. The valid value is 10 to 65,000. The default is 60.</p> <p>Notes:</p> <ul style="list-style-type: none"> <li>Simple ACKs such as keep-alives are not considered data packets.</li> <li>TCP keepalive is enabled per SIP Interface in the SIP Interface table.</li> </ul>
<p>TCP Keep Alive Interval Time [TCPKeepAliveInterval]</p>	<p>Defines the interval (in sec) between consecutive keep-alive probes, regardless of what the connection has exchanged in the meantime. The valid value is 10 to 65,000. The default is 10.</p> <p><b>Note:</b> TCP keepalive is enabled per SIP Interface in the SIP Interface table.</p>
<p>TCP Keep Alive Retry Number [TCPKeepAliveRetry]</p>	<p>Defines the number of unacknowledged keep-alive probes to send before considering the connection down. The valid value is 1 to 100. The default is 5.</p> <p><b>Note:</b> TCP keepalive is enabled per SIP Interface in the SIP Interface table.</p>
<b>NAT Translation Table</b>	
<p>Web: NAT Translation Table [NATTranslation]</p>	<p>This table parameter defines NAT rules for translating source IP addresses per VoIP interface (SIP control and RTP media traffic) into NAT IP addresses. This allows, for example, the separation of VoIP traffic between different ISTP's, and topology hiding (of internal IP addresses to the "public" network). Each IP interface (configured in the Multiple Interface table - InterfaceTable parameter) can be associated with a NAT rule in this table, translating the source IP address and port of the outgoing packet into the NAT address (IP address and port range). The format of this parameter is as follows:</p> <p>[ NATTranslation ]          FORMAT NATTranslation_Index =          NATTranslation_SourceIPInterfaceName,          NATTranslation_TargetIPAddress, NATTranslation_SourceStartPort,          NATTranslation_SourceEndPort, NATTranslation_TargetStartPort,          NATTranslation_TargetEndPort;          [ \NATTranslation ]</p> <p><b>Note:</b> For a detailed description of this table, see "Configuring NAT Translation per IP Interface" on page 110.</p>



## 42.8 General SIP Parameters

The general SIP parameters are described in the table below.

**Table 42-30: General SIP Parameters**

Parameter	Description
Web: SIP Remote Reset CLI: sip-remote-reset <b>[EnableSIPRemoteReset]</b>	<p>Enables a specific device action upon the receipt of a SIP NOTIFY request, where the action depends on the value received in the Event header.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <p>The action depends on the Event header value:</p> <ul style="list-style-type: none"> <li>'check-sync;reboot=false': triggers the regular Automatic Update feature (if Automatic Update has been enabled on the device)</li> <li>'check-sync;reboot=true': triggers a device reset</li> </ul> <p><b>Note:</b> The Event header value is proprietary to AudioCodes.</p>
Web: Max SIP Message Length <b>[KB]</b> <b>[MaxSIPMessageLength]</b>	<p>Defines the maximum size (in Kbytes) for each SIP message that can be sent over the network. The device rejects messages exceeding this user-defined size.</p> <p>The valid value range is 1 to 50. The default is 50.</p>
<b>[SIPForceRport]</b>	<p>Determines whether the device sends SIP responses to the UDP port from where SIP requests are received even if the 'rport' parameter is not present in the SIP Via header.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) Disabled. The device sends the SIP response to the UDP port defined in the Via header. If the Via header contains the 'rport' parameter, the response is sent to the UDP port from where the SIP request is received.</li> <li><b>[1]</b> = Enabled. SIP responses are sent to the UDP port from where SIP requests are received even if the 'rport' parameter is not present in the Via header.</li> </ul>
Web: Reject Cancel after Connect CLI: reject-cancel-after-connect <b>[RejectCancelAfterConnect]</b>	<p>Determines whether the device accepts or rejects a SIP CANCEL request received after the receipt of a 200 OK, during an established call.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) Accepts the CANCEL, by responding with a 200 OK and terminating the call session.</li> <li><b>[1]</b> = Rejects the CANCEL, by responding with a SIP 481 Call/Transaction Does Not Exist, and maintaining the call session.</li> </ul>
Web: Verify Received RequestURI CLI: verify-rcvd-requri <b>[VerifyReceeededRequestUri]</b>	<p>Enables the device to reject SIP requests (such as ACK, BYE, or re-INVITE) whose user part in the Request-URI is different from the user part received in the Contact header of the last sent SIP request.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) Even if the user is different, the device accepts the SIP request.</li> <li><b>[1]</b> Enable = If the user is different, the device rejects the SIP request (BYE is responded with 481; re-INVITE is responded with 404; ACK is ignored).</li> </ul>
Web: Max Number of Active Calls <b>[MaxActiveCalls]</b>	<p>Defines the maximum number of simultaneous active calls supported by the device. If the maximum number of calls is reached, new calls are not established.</p> <p>The valid range is 1 to the maximum number of supported channels. The default is the maximum available channels (i.e., no restriction on</p>



Parameter	Description
	the maximum number of calls).
Web: QoS statistics in SIP Release Call <b>[QoSStatistics]</b>	<p>Enables the device to include call quality of service (QoS) statistics in SIP BYE and SIP 200 OK response to BYE, using the proprietary SIP header X-RTP-Stat.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = Disable (default)</li> <li><b>[1]</b> = Enable</li> </ul> <p>The X-RTP-Stat header provides the following statistics:</p> <ul style="list-style-type: none"> <li>Number of received and sent voice packets</li> <li>Number of received and sent voice octets</li> <li>Received packet loss, jitter (in ms), and latency (in ms)</li> </ul> <p>The X-RTP-Stat header contains the following fields:</p> <ul style="list-style-type: none"> <li>PS=&lt;voice packets sent&gt;</li> <li>OS=&lt;voice octets sent&gt;</li> <li>PR=&lt;voice packets received&gt;</li> <li>OR=&lt;voice octets received&gt;</li> <li>PL=&lt;receive packet loss&gt;</li> <li>JL=&lt;jitter in ms&gt;</li> <li>LA=&lt;latency in ms&gt;</li> </ul> <p>Below is an example of the X-RTP-Stat header in a SIP BYE message:</p> <pre> BYE sip:302@10.33.4.125 SIP/2.0 Via: SIP/2.0/UDP 10.33.4.126;branch=z9hG4bKac2127550866 Max-Forwards: 70 From: &lt;sip:401@10.33.4.126;user=phone&gt;;tag=1c2113553324 To: &lt;sip:302@company.com&gt;;tag=1c991751121 Call-ID: 991750671245200001912@10.33.4.125 CSeq: 1 BYE <b>X-RTP-Stat:</b> <b>PS=207;OS=49680;;PR=314;OR=50240;PL=0;JI=600;LA=40;</b> Supported: em,timer,replaces,path,resource-priority Allow: REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK ,REFER,INFO,SUBSCRIBE,UPDATE User-Agent: Sip-Gateway-/v.6.2A.008.006 Reason: Q.850 ;cause=16 ;text="local" Content-Length: 0 </pre>
Web: PRACK Mode <b>[PrackMode]</b>	<p>Determines the PRACK (Provisional Acknowledgment) mechanism mode for SIP 1xx reliable responses.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable</li> <li><b>[1]</b> Supported (default)</li> <li><b>[2]</b> Required</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>The Supported and Required headers contain the '100rel' tag.</li> <li>The device sends PRACK messages if 180/183 responses are received with '100rel' in the Supported or Required headers.</li> </ul>
Web: Enable Early Media <b>[EnableEarlyMedia]</b>	<p>Enables the Early Media feature.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> </ul>



Parameter	Description
	<ul style="list-style-type: none"> <li>▪ <b>[1]</b> Enable</li> </ul> <p><b>Note:</b> This feature can also be configured as an IP Profile and/or Tel Profile.</p>
Web: 183 Message Behavior <b>[SIP183Behaviour]</b>	<ul style="list-style-type: none"> <li>▪ <b>[0]</b> Progress = (Default) .</li> <li>▪ <b>[1]</b> Alert =</li> </ul>
Web: Session-Expires Time <b>[SIPSessionExpires]</b>	<p>Defines the numerical value sent in the Session-Expires header in the first INVITE request or response (if the call is answered).</p> <p>The valid range is 1 to 86,400 sec. The default is 0 (i.e., the Session-Expires header is disabled).</p>
Web: Minimum Session-Expires <b>[MinSE]</b>	<p>Defines the time (in seconds) that is used in the Min-SE header. This header defines the minimum time that the user agent refreshes the session.</p> <p>The valid range is 10 to 100,000. The default is 90.</p>
Web/EMS: Session Expires Disconnect Time CLI: session-exp-disconnect-time <b>[SessionExpiresDisconnectTime]</b>	<p>Defines a session expiry timeout. The device disconnects the session (sends a SIP BYE) if the refresher does not send a refresh request before one-third (1/3) of the session expires time, or before the time configured by this parameter (the minimum of the two).</p> <p>The valid range is 0 to 32 (in seconds). The default is 32.</p>
Web: Session Expires Method <b>[SessionExpiresMethod]</b>	<p>Determines the SIP method used for session-timer updates.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Re-INVITE = (Default) Uses Re-INVITE messages for session-timer updates.</li> <li>▪ <b>[1]</b> UPDATE = Uses UPDATE messages.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ The device can receive session-timer refreshes using both methods.</li> <li>▪ The UPDATE message used for session-timer is excluded from the SDP body.</li> </ul>
<b>[RemoveToTagInFailureResponse]</b>	<p>Determines whether the device removes the 'to' header tag from final SIP failure responses to INVITE transactions.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = (Default) Do not remove tag.</li> <li>▪ <b>[1]</b> = Remove tag.</li> </ul>
<b>[EnableRTCPAttribute]</b>	<p>Enables the use of the 'rtcp' attribute in the outgoing SDP.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = Disable (default)</li> <li>▪ <b>[1]</b> = Enable</li> </ul>
<b>[OPTIONSUserPart]</b>	<p>Defines the user part value of the Request-URI for outgoing SIP OPTIONS requests. If no value is configured, the configuration parameter 'Username' value is used.</p> <p>A special value is 'empty', indicating that no user part in the Request-URI (host part only) is used.</p> <p>The valid range is a 30-character string. The default is an empty string ("").</p>
Web: Fax Signaling Method <b>[IsFaxUsed]</b>	<p>Determines the SIP signaling method for establishing and transmitting a fax session after a fax is detected.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> No Fax = (Default) No fax negotiation using SIP signaling. Fax transport method is according to the parameter FaxTransportMode.</li> </ul>



Parameter	Description
	<ul style="list-style-type: none"> <li>▪ <b>[1]</b> T.38 Relay = Initiates T.38 fax relay.</li> <li>▪ <b>[2]</b> G.711 Transport = Initiates fax/modem using the coder G.711 A-law/Mu-law with adaptations (see Note below).</li> <li>▪ <b>[3]</b> Fax Fallback = Initiates T.38 fax relay. If the T.38 negotiation fails, the device re-initiates a fax session using the coder G.711 A-law/<math>\mu</math>-law with adaptations (see the Note below).</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ Fax adaptations (for options 2 and 3): <ul style="list-style-type: none"> <li>✓ Echo Canceller = On</li> <li>✓ Silence Compression = Off</li> <li>✓ Echo Canceller Non-Linear Processor Mode = Off</li> <li>✓ Dynamic Jitter Buffer Minimum Delay = 40</li> <li>✓ Dynamic Jitter Buffer Optimization Factor = 13</li> </ul> </li> <li>▪ If the device initiates a fax session using G.711 (option 2 and possibly 3), a 'gpmid' attribute is added to the SDP in the following format: <ul style="list-style-type: none"> <li>✓ <b>For A-law:</b> 'a=gpmid:8 vbd=yes;ecan=on'</li> <li>✓ <b>For <math>\mu</math>-law:</b> 'a=gpmid:0 vbd=yes;ecan=on'</li> </ul> </li> <li>▪ When this parameter is set to 1, 2, or 3, the parameter FaxTransportMode is ignored.</li> <li>▪ When this parameter is set to 0, T.38 might still be used without the control protocol's involvement. To completely disable T.38, set FaxTransportMode to a value other than 1.</li> <li>▪ This parameter can also be configured per IP Profile (using the IPProfile parameter).</li> <li>▪ For more information on fax transport methods, see Fax/Modem Transport Modes.</li> </ul>
<b>[HandleG711asVBD]</b>	<p>Enables the handling of G.711 as G.711 VBD coder.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = (Default) Disable. The device negotiates G.711 as a regular audio coder and sends an answer only with G.729 coder. For example, if the device is configured with G.729 and G.711 VBD coders and it receives an INVITE with an SDP offer containing G.729 and "regular" G.711 coders, it sends an SDP answer containing only the G.729 coder.</li> <li>▪ <b>[1]</b> = Enable. The device assumes that the G.711 coder received in the INVITE SDP offer is a VBD coder. For example, if the device is configured with G.729 and G.711 VBD coders and it receives an INVITE with an SDP offer containing G.729 and "regular" G.711 coders, it sends an SDP answer containing G.729 and G.711 VBD coders, allowing a subsequent bypass (passthrough) session if fax/modem signals are detected during the call.</li> </ul> <p><b>Note:</b> This parameter is applicable only if G.711 VBD coder(s) with regular G.711 payload types 0 or 8 are configured for the device (using the CodersGroup parameter).</p>
<b>[FaxVBDBehavior]</b>	<p>Determines the device's fax transport behavior when G.711 VBD coder is negotiated at call start.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = (Default) If the device is configured with a VBD coder (see the CodersGroup parameter) and is negotiated OK at call start, then both fax and modem signals are sent over RTP using the bypass payload type (and no mid-call VBD or T.38 Re-INVITEs occur).</li> <li>▪ <b>[1]</b> = If the IsFaxUsed parameter is set to 1, the channel opens with the FaxTransportMode parameter set to 1 (relay). This is required to detect mid-call fax tones and to send T.38 Re-INVITE messages</li> </ul>



Parameter	Description
	<p>upon fax detection. If the remote party supports T.38, the fax is relayed over T.38.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>If VBD coder negotiation fails at call start and if the IsFaxUsed parameter is set to 1 (or 3), then the channel opens with the FaxTransportMode parameter set to 1 (relay) to allow future detection of fax tones and sending of T.38 Re-INVITES. In such a scenario, the FaxVBDBehavior parameter has no effect.</li> <li>This feature can be used only if the remote party supports T.38 fax relay; otherwise, the fax fails.</li> </ul>
<b>[NoAudioPayloadType]</b>	<p>Defines the payload type of the outgoing SDP offer.</p> <p>The valid value range is 96 to 127 (dynamic payload type). The default is 0 (i.e. NoAudio is not supported). For example, if set to 120, the following is added to the INVITE SDP:</p> <pre>a=rtptime:120 NoAudio/8000\r\n</pre> <p><b>Note:</b> For incoming SDP offers, NoAudio is always supported.</p>
Web: SIP Transport Type <b>[SIPTransportType]</b>	<p>Determines the default transport layer for outgoing SIP calls initiated by the device.</p> <ul style="list-style-type: none"> <li><b>[0]</b> UDP (default)</li> <li><b>[1]</b> TCP</li> <li><b>[2]</b> TLS (SIPS)</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>It's recommended to use TLS for communication with a SIP Proxy and not for direct device-to-device communication.</li> <li>For received calls (i.e., incoming), the device accepts all these protocols.</li> <li>The value of this parameter is also used by the SAS application as the default transport layer for outgoing SIP calls.</li> </ul>
Web: SIP UDP Local Port <b>[LocalSIPPort]</b>	<p>Defines the local UDP port for SIP messages.</p> <p>The valid range is 1 to 65534. The default is 5060.</p>
Web: SIP TCP Local Port <b>[TCPLocalSIPPort]</b>	<p>Defines the local TCP port for SIP messages.</p> <p>The valid range is 1 to 65535. The default is 5060.</p>
Web: SIP TLS Local Port <b>[TLSTLocalSIPPort]</b>	<p>Defines the local TLS port for SIP messages.</p> <p>The valid range is 1 to 65535. The default is 5061.</p> <p><b>Note:</b> The value of this parameter must be different from the value of the parameter TCPLocalSIPPort.</p>
Web: Enable SIPS <b>[EnableSIPS]</b>	<p>Enables secured SIP (SIPS URI) connections over multiple hops.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <p>When the SIPTransportType parameter is set to 2 (i.e., TLS) and the parameter EnableSIPS is disabled, TLS is used for the next network hop only. When the parameter SIPTransportType is set to 2 or 1 (i.e., TCP or TLS) and EnableSIPS is enabled, TLS is used through the entire connection (over multiple hops).</p> <p><b>Note:</b> If this parameter is enabled and the parameter SIPTransportType is set to 0 (i.e., UDP), the connection fails.</p>
Web: Enable TCP	<p>Enables the reuse of the same TCP connection for all calls to the same</p>



Parameter	Description
Connection Reuse <b>[EnableTCPConnectionReuse]</b>	<p>destination.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = Uses a separate TCP connection for each call.</li> <li><b>[1]</b> Enable = (Default) Uses the same TCP connection for all calls.</li> </ul> <p><b>Note:</b> For the SAS application, this feature is configured using the SASConnectionReuse parameter.</p>
Web: Fake TCP alias <b>[FakeTCPalias]</b>	<p>Enables the re-use of the same TCP/TLS connection for sessions with the same user, even if the "alias" parameter is not present in the SIP Via header of the first INVITE.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) TCP/TLS connection reuse is done only if the "alias" parameter is present in the Via header of the first INVITE.</li> <li><b>[1]</b> Enable</li> </ul> <p><b>Note:</b> To enable TCP/TLS connection re-use, set the EnableTCPConnectionReuse parameter to 1.</p>
Web: Reliable Connection Persistent Mode <b>[ReliableConnectionPersistentMode]</b>	<p>Enables setting of all TCP/TLS connections as persistent and therefore, not released.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) Disable. All TCP connections (except those that are set to a proxy IP) are released if not used by any SIP dialog/transaction.</li> <li><b>[1]</b> = Enable - TCP connections to all destinations are persistent and not released unless the device reaches 70% of its maximum TCP resources.</li> </ul> <p>While trying to send a SIP message connection, reuse policy determines whether live connections to the specific destination are re-used.</p> <p>Persistent TCP connection ensures less network traffic due to fewer setting up and tearing down of TCP connections and reduced latency on subsequent requests due to avoidance of initial TCP handshake. For TLS, persistent connection may reduce the number of costly TLS handshakes to establish security associations, in addition to the initial TCP connection set up.</p> <p><b>Note:</b> If the destination is a Proxy server, the TCP/TLS connection is persistent regardless of the settings of this parameter.</p>
Web: TCP Timeout <b>[SIPTCPTimeout]</b>	<p>Defines the Timer B (INVITE transaction timeout timer) and Timer F (non-INVITE transaction timeout timer), as defined in RFC 3261, when the SIP Transport Type is TCP.</p> <p>The valid range is 0 to 40 sec. The default is 64 multiplied by the SipT1Rtx parameter value. For example, if SipT1Rtx is set to 500 msec, then the default of SIPTCPTimeout is 32 sec.</p>
Web: SIP Destination Port <b>[SIPDestinationPort]</b>	<p>Defines the SIP destination port for sending initial SIP requests. The valid range is 1 to 65534. The default port is 5060.</p> <p><b>Note:</b> SIP responses are sent to the port specified in the Via header.</p>
Web: Use user=phone in SIP URL <b>[IsUserPhone]</b>	<p>Determines whether the 'user=phone' string is added to the SIP URI and SIP To header.</p> <ul style="list-style-type: none"> <li><b>[0]</b> No = 'user=phone' string is not added.</li> <li><b>[1]</b> Yes = (Default) 'user=phone' string is part of the SIP URI and SIP To header.</li> </ul>
Web: Use user=phone in From Header <b>[IsUserPhoneInFrom]</b>	<p>Determines whether the 'user=phone' string is added to the From and Contact SIP headers.</p> <ul style="list-style-type: none"> <li><b>[0]</b> No = (Default) Doesn't add 'user=phone' string.</li> <li><b>[1]</b> Yes = 'user=phone' string is part of the From and Contact</li> </ul>



Parameter	Description											
	headers.											
Web: Use Tel URI for Asserted Identity <b>[UseTelURIForAssertedID]</b>	<p>Determines the format of the URI in the P-Asserted-Identity and P-Preferred-Identity headers.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) 'sip:'</li> <li><b>[1]</b> Enable = 'tel:'</li> </ul>											
Web: Tel to IP No Answer Timeout <b>[IPAlertTimeout]</b>	<p>Defines the time (in seconds) that the device waits for a 200 OK response from the called party (IP side) after sending an INVITE message. If the timer expires, the call is released.</p> <p>The valid range is 0 to 3600. The default is 180.</p>											
Web: Enable Remote Party ID <b>[EnableRPIheader]</b>	<p>Enables Remote-Party-Identity headers for calling and called numbers for Tel-to-IP calls.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default).</li> <li><b>[1]</b> Enable = Remote-Party-Identity headers are generated in SIP INVITE messages for both called and calling numbers.</li> </ul>											
Web: Enable History-Info Header <b>[EnableHistoryInfo]</b>	<p>Enables usage of the History-Info header.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <p><b>User Agent Client (UAC) Behavior:</b></p> <ul style="list-style-type: none"> <li>Initial request: The History-Info header is equal to the Request-URI. If a PSTN Redirect number is received, it is added as an additional History-Info header with an appropriate reason.</li> <li>Upon receiving the final failure response, the device copies the History-Info as is, adds the reason of the failure response to the last entry, and concatenates a new destination to it (if an additional request is sent). The order of the reasons is as follows: <ol style="list-style-type: none"> <li>Q.850 Reason</li> <li>SIP Reason</li> <li>SIP Response code</li> </ol> </li> <li>Upon receiving the final response (success or failure), the device searches for a Redirect reason in the History-Info (i.e., 3xx/4xx SIP reason). If found, it is passed to ISDN according to the following table:</li> </ul> <table border="1"> <thead> <tr> <th>SIP Reason Code</th><th>ISDN Redirecting Reason</th></tr> </thead> <tbody> <tr> <td>302 - Moved Temporarily</td><td>Call Forward Universal (CFU)</td></tr> <tr> <td>408 - Request Timeout</td><td rowspan="3">Call Forward No Answer (CFNA)</td></tr> <tr> <td>480 - Temporarily Unavailable</td></tr> <tr> <td>487 - Request Terminated</td></tr> <tr> <td>486 - Busy Here</td><td rowspan="2">Call Forward Busy (CFB)</td></tr> <tr> <td>600 - Busy Everywhere</td></tr> </tbody> </table> <ul style="list-style-type: none"> <li>If history reason is a Q.850 reason, it is translated to the SIP reason (according to the SIP-ISDN tables) and then to ISDN Redirect reason according to the table above.</li> </ul> <p><b>User Agent Server (UAS) Behavior:</b></p> <ul style="list-style-type: none"> <li>The History-Info header is sent only in the final response.</li> <li>Upon receiving a request with History-Info, the UAS checks the policy in the request. If a 'session', 'header', or 'history' policy tag is found, the (final) response is sent without History-Info; otherwise, it is copied from the request.</li> </ul>	SIP Reason Code	ISDN Redirecting Reason	302 - Moved Temporarily	Call Forward Universal (CFU)	408 - Request Timeout	Call Forward No Answer (CFNA)	480 - Temporarily Unavailable	487 - Request Terminated	486 - Busy Here	Call Forward Busy (CFB)	600 - Busy Everywhere
SIP Reason Code	ISDN Redirecting Reason											
302 - Moved Temporarily	Call Forward Universal (CFU)											
408 - Request Timeout	Call Forward No Answer (CFNA)											
480 - Temporarily Unavailable												
487 - Request Terminated												
486 - Busy Here	Call Forward Busy (CFB)											
600 - Busy Everywhere												



Parameter	Description
Web: Enable GRUU <b>[EnableGRUU]</b>	<p>Determines whether the Globally Routable User Agent URIs (GRUU) mechanism is used, according to RFC 5627. This is used for obtaining a GRUU from a registrar and for communicating a GRUU to a peer within a dialog.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul> <p>A GRUU is a SIP URI that routes to an instance-specific UA and can be reachable from anywhere. There are a number of contexts in which it is desirable to have an identifier that addresses a single UA (using GRUU) rather than the group of UA's indicated by an Address of Record (AOR). For example, in call transfer where user A is talking to user B, and user A wants to transfer the call to user C. User A sends a REFER to user C:</p> <pre>REFER sip:C@domain.com SIP/2.0 From: sip:A@domain.com;tag=99asd To: sip:C@domain.com Refer-To: (URI that identifies B's UA)</pre> <p>The Refer-To header needs to contain a URI that user C can use to place a call to user B. This call needs to route to the specific UA instance that user B is using to talk to user A. User B should provide user A with a URI that has to be usable by anyone. It needs to be a GRUU.</p> <ul style="list-style-type: none"> <li>▪ Obtaining a GRUU: The mechanism for obtaining a GRUU is through registrations. A UA can obtain a GRUU by generating a REGISTER request containing a Supported header field with the value "gruu". The UA includes a "+sip.instance" Contact header parameter of each contact for which the GRUU is desired. This Contact parameter contains a globally unique ID that identifies the UA instance. The global unique ID is created from one of the following: <ul style="list-style-type: none"> <li>✓ If the REGISTER is per the device's client (endpoint), it is the MAC address concatenated with the phone number of the client.</li> <li>✓ If the REGISTER is per device, it is the MAC address only.</li> <li>✓ When using TP, "User Info" can be used for registering per endpoint. Thus, each endpoint can get a unique id – its phone number. The globally unique ID in TP is the MAC address concatenated with the phone number of the endpoint.</li> </ul> </li> </ul> <p>If the remote server doesn't support GRUU, it ignores the parameters of the GRUU. Otherwise, if the remote side also supports GRUU, the REGISTER responses contain the "gruu" parameter in each Contact header. This parameter contains a SIP or SIPS URI that represents a GRUU corresponding to the UA instance that registered the contact. The server provides the same GRUU for the same AOR and instance-id when sending REGISTER again after registration expiration. RFC 5627 specifies that the remote target is a GRUU target if its' Contact URL has the "gr" parameter with or without a value.</p> <ul style="list-style-type: none"> <li>▪ Using GRUU: The UA can place the GRUU in any header field that can contain a URI. It must use the GRUU in the following messages: INVITE request, its 2xx response, SUBSCRIBE request, its 2xx response, NOTIFY request, REFER request and its 2xx response.</li> </ul>
<b>[IsCiscoSCEMode]</b>	<p>Determines whether a Cisco gateway exists at the remote side.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = (Default) No Cisco gateway exists at the remote side.</li> <li>▪ <b>[1]</b> = A Cisco gateway exists at the remote side.</li> </ul> <p>When a Cisco gateway exists at the remote side, the device must set the value of the 'annexb' parameter of the fmtp attribute in the SDP to</p>



Parameter	Description
	<p>'no'. This logic is used if the parameter EnableSilenceCompression is set to 2 (enable without adaptation). In this case, Silence Suppression is used on the channel but not declared in the SDP.</p> <p><b>Note:</b> The IsCiscoSCEMode parameter is applicable only when the selected coder is G.729.</p>
Web: User-Agent Information <b>[UserAgentDisplayInfo]</b>	<p>Defines the string that is used in the SIP User-Agent and Server response headers. When configured, the string &lt;UserAgentDisplayInfo value&gt;/software version' is used, for example:</p> <pre>User-Agent: myproduct/v.6.40.010.006</pre> <p>If not configured, the default string, &lt;AudioCodes product-name&gt;/software version' is used, for example:</p> <pre>User-Agent: Audiocodes-Sip-Gateway-Mediant Software E-SBC/v.6.40.010.006</pre> <p>The maximum string length is 50 characters.</p> <p><b>Note:</b> The software version number and preceding forward slash (/) cannot be modified. Therefore, it is recommended not to include a forward slash in the parameter's value (to avoid two forward slashes in the SIP header, which may cause problems).</p>
Web: SDP Session Owner <b>[SIPSDPSessionOwner]</b>	<p>Defines the value of the Owner line ('o' field) in outgoing SDP messages.</p> <p>The valid range is a string of up to 39 characters. The default is 'AudiocodesGW'.</p> <p>For example:</p> <pre>o=AudiocodesGW 1145023829 1145023705 IN IP4 10.33.4.126</pre>
<b>[EnableSDPVersionNegotiation]</b>	<p>Enables the device to ignore new SDP re-offers (from the media negotiation perspective) in certain scenarios (such as session expires). According to RFC 3264, once an SDP session is established, a new SDP offer is considered a new offer only when the SDP origin value is incremented. In scenarios such as session expires, SDP negotiation is irrelevant and thus, the origin field is not changed.</p> <p>Even though some SIP devices don't follow this behavior and don't increment the origin value even in scenarios where they want to re-negotiate, the device can assume that the remote party operates according to RFC 3264, and in cases where the origin field is not incremented, the device does not re-negotiate SDP capabilities.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable = (Default) The device negotiates any new SDP re-offer, regardless of the origin field.</li> <li>▪ <b>[1]</b> Enable = The device negotiates only an SDP re-offer with an incremented origin field.</li> </ul>
Web: Subject <b>[SIPSubject]</b>	<p>Defines the Subject header value in outgoing INVITE messages. If not specified, the Subject header isn't included (default).</p> <p>The maximum length is up to 50 characters.</p>



Parameter	Description
Web: Multiple Packetization Time Format <b>[MultiPtimeFormat]</b>	<p>Determines whether the 'mptime' attribute is included in the outgoing SDP.</p> <ul style="list-style-type: none"> <li><b>[0]</b> None = (Default) Disabled.</li> <li><b>[1]</b> PacketCable = Includes the 'mptime' attribute in the outgoing SDP - PacketCable-defined format.</li> </ul> <p>The 'mptime' attribute enables the device to define a separate packetization period for each negotiated coder in the SDP. The 'mptime' attribute is only included if this parameter is enabled even if the remote side includes it in the SDP offer. Upon receipt, each coder receives its 'ptime' value in the following precedence: from 'mptime' attribute, from 'ptime' attribute, and then from default value.</p>
<b>[EnablePtime]</b>	<p>Determines whether the 'ptime' attribute is included in the SDP.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = Remove the 'ptime' attribute from SDP.</li> <li><b>[1]</b> = (Default) Include the 'ptime' attribute in SDP.</li> </ul>
Web: 3xx Behavior <b>[3xxBehavior]</b>	<p>Determines the device's behavior regarding call identifiers when a 3xx response is received for an outgoing INVITE request. The device can either use the same call identifiers (Call-ID, To, and From tags) or change them in the new initiated INVITE.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Forward = (Default) Use different call identifiers for a redirected INVITE message.</li> <li><b>[1]</b> Redirect = Use the same call identifiers.</li> </ul>
Web: Enable P-Charging Vector <b>[EnablePChargingVector]</b>	<p>Enables the inclusion of the P-Charging-Vector header to all outgoing INVITE messages.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul>
Web: Retry-After Time <b>[RetryAfterTime]</b>	<p>Defines the time (in seconds) used in the Retry-After header when a 503 (Service Unavailable) response is generated by the device.</p> <p>The time range is 0 to 3,600. The default is 0.</p>
Web: Fake Retry After <b>[sec]</b> <b>[FakeRetryAfter]</b>	<p>Determines whether the device, upon receipt of a SIP 503 response without a Retry-After header, behaves as if the 503 response included a Retry-After header and with the period (in seconds) specified by this parameter.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li>Any positive value (in seconds) for defining the period</li> </ul> <p>When enabled, this feature allows the device to operate with Proxy servers that do not include the Retry-After SIP header in SIP 503 (Service Unavailable) responses to indicate an unavailable service.</p> <p>The Retry-After header is used with the 503 (Service Unavailable) response to indicate how long the service is expected to be unavailable to the requesting SIP client. The device maintains a list of available proxies, by using the Keep-Alive mechanism. The device checks the availability of proxies by sending SIP OPTIONS every keep-alive timeout to all proxies.</p> <p>If the device receives a SIP 503 response to an INVITE, it also marks that the proxy is out of service for the defined "Retry-After" period.</p>
Web: Enable P-Associated-URI Header <b>[EnablePAssociatedURIHeader]</b>	<p>Determines the device usage of the P-Associated-URI header. This header can be received in 200 OK responses to REGISTER requests. When enabled, the first URI in the P-Associated-URI header is used in subsequent requests as the From/P-Asserted-Identity headers value.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> </ul>



Parameter	Description
	<ul style="list-style-type: none"> <li>▪ <b>[1]</b> Enable</li> </ul> <p><b>Note:</b> P-Associated-URIs in registration responses is handled only if the device is registered per endpoint (using the User Information file).</p>
Web: Source Number Preference <b>[SourceNumberPreference]</b>	<p>Determines from which SIP header the source (calling) number is obtained in incoming INVITE messages.</p> <ul style="list-style-type: none"> <li>▪ If not configured (i.e., empty string) or if any string other than "From" or "Pai2" is configured, the calling number is obtained from a specific header using the following logic: <ul style="list-style-type: none"> <li>a. P-Preferred-Identity header.</li> <li>b. If the above header is not present, then the first P-Asserted-Identity header is used.</li> <li>c. If the above header is not present, then the Remote-Party-ID header is used.</li> <li>d. If the above header is not present, then the From header is used.</li> </ul> </li> <li>▪ "From" = The calling number is obtained from the From header.</li> <li>▪ "Pai2" = The calling number is obtained using the following logic: <ul style="list-style-type: none"> <li>a. If a P-Preferred-Identity header is present, the number is obtained from it.</li> <li>b. If no P-Preferred-Identity header is present and two P-Asserted-Identity headers are present, the number is obtained from the second P-Asserted-Identity header.</li> <li>c. If only one P-Asserted-Identity header is present, the calling number is obtained from it.</li> </ul> </li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ The "From" and "Pai2" values are not case-sensitive.</li> <li>▪ Once a URL is selected, all the calling party parameters are set from this header. If P-Asserted-Identity is selected and the Privacy header is set to 'id', the calling number is assumed restricted.</li> </ul>
<b>[SelectSourceHeaderForCalledNumber]</b>	<p>Determines the SIP header used for obtaining the called number (destination) for IP-to-Tel calls.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Request-URI header = (Default) Obtains the destination number from the user part of the Request-URI.</li> <li>▪ <b>[1]</b> To header = Obtains the destination number from the user part of the To header.</li> <li>▪ <b>[2]</b> P-Called-Party-ID header = Obtains the destination number from the P-Called-Party-ID header.</li> </ul>
Web: Forking Handling Mode <b>[ForkingHandlingMode]</b>	<p>Determines how the device handles the receipt of multiple SIP 18x forking responses for Tel-to-IP calls. The forking 18x response is the response with a different SIP to-tag than the previous 18x response. These responses are typically generated (initiated) by Proxy / Application servers that perform call forking, sending the device's originating INVITE (received from SIP clients) to several destinations, using the same CallID.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Parallel handling = (Default) If SIP 18x with SDP is received, the device opens a voice stream according to the received SDP and disregards any subsequently received 18x forking responses (with or without SDP). If the first response is 180 without SDP, the device responds according to the PlayRBTone2TEL parameter and disregards the subsequent forking 18x responses.</li> <li>▪ <b>[1]</b> Sequential handling = If 18x with SDP is received, the device opens a voice stream according to the received SDP. The device re-</li> </ul>



Parameter	Description
	<p>opens the stream according to subsequently received 18x responses with SDP, or plays a ringback tone if 180 response without SDP is received. If the first received response is 180 without SDP, the device responds according to the PlayRBTone2TEL parameter and processes the subsequent 18x forking responses.</p> <p><b>Note:</b> Regardless of this parameter setting, once a SIP 200 OK response is received, the device uses the RTP information and re-opens the voice stream, if necessary.</p>
Web: Forking Timeout <b>[ForkingTimeout]</b>	<p>Defines the timeout (in seconds) that is started after the first SIP 2xx response has been received for a User Agent when a Proxy server performs call forking (Proxy server forwards the INVITE to multiple SIP User Agents). The device sends a SIP ACK and BYE in response to any additional SIP 2xx received from the Proxy within this timeout. Once this timeout elapses, the device ignores any subsequent SIP 2xx.</p> <p>The number of supported forking calls per channel is 20. In other words, for an INVITE message, the device can receive up to 20 forking responses from the Proxy server.</p> <p>The valid range is 0 to 30. The default is 30.</p>
Web: Tel2IP Call Forking Mode <b>[Tel2IPCallForkingMode]</b>	<p>Enables Tel-to-IP call forking, whereby a Tel call can be routed to multiple IP destinations.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <p><b>Note:</b> Once enabled, routing rules must be assigned Forking Groups in the Outbound IP Routing table.</p>
Web: Enable Reason Header <b>[EnableReasonHeader]</b>	<p>Enables the usage of the SIP Reason header.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable</li> <li><b>[1]</b> Enable (default)</li> </ul>
Web/EMS: Gateway Name CLI: gw-name <b>[SIPGatewayName]</b>	<p>Defines a name for the device (e.g., device123.com). This name is used as the host part of the SIP URI in the From header. If not specified, the device's IP address is used instead (default).</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>Ensure that the parameter value is the one with which the Proxy has been configured with to identify the device.</li> <li>This parameter can also be configured for an IP Group (in the IP Group table).</li> </ul>
<b>[ZeroSDPHandling]</b>	<p>Determines the device's response to an incoming SDP that includes an IP address of 0.0.0.0 in the SDP's Connection Information field (i.e., "c=IN IP4 0.0.0.0").</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) Sets the IP address of the outgoing SDP's c= field to 0.0.0.0.</li> <li><b>[1]</b> = Sets the IP address of the outgoing SDP c= field to the IP address of the device. If the incoming SDP doesn't contain the "a=inactive" line, the returned SDP contains the "a=recvonly" line.</li> </ul>
Web: Enable Delayed Offer <b>[EnableDelayedOffer]</b>	<p>Determines whether the device sends the initial INVITE message with or without an SDP. Sending the first INVITE without SDP is typically done by clients for obtaining the far-end's full list of capabilities before sending their own offer. (An alternative method for obtaining the list of supported capabilities is by using SIP OPTIONS, which is not supported by every SIP agent.)</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) The device sends the initial INVITE message</li> </ul>



Parameter	Description
	<p>with an SDP.</p> <ul style="list-style-type: none"> <li><b>[1]</b> Enable = The device sends the initial INVITE message without an SDP.</li> </ul>
<b>[DisableCryptoLifeTimeInSDP]</b>	<p>Enables the device to send "a=crypto" lines without the lifetime parameter in the SDP. For example, if the SDP contains "a=crypto:12 AES_CM_128_HMAC_SHA1_80 inline:hhQe10yZRCrclFPkH5xYY9R1de37ogh9G1MpvNp 2^31", it removes the lifetime parameter "2^31".</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul>
Web: Enable Contact Restriction <b>[EnableContactRestriction]</b>	<p>Determines whether the device sets the Contact header of outgoing INVITE requests to 'anonymous' for restricted calls.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul>
<b>[AnonymousMode]</b>	<p>Determines whether the device's IP address is used as the URI host part instead of "anonymous.invalid" in the INVITE's From header for Tel-to-IP calls.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) If the device receives a call from the Tel with blocked caller ID, it sends an INVITE with From: "anonymous"&lt;anonymous@anonymous.invalid&gt;</li> <li><b>[1]</b> = The device's IP address is used as the URI host part instead of "anonymous.invalid".</li> </ul> <p>This parameter may be useful, for example, for service providers who identify their SIP Trunking customers by their source phone number or IP address, reflected in the From header of the SIP INVITE. Therefore, even customers blocking their Caller ID can be identified by the service provider. Typically, if the device receives a call with blocked Caller ID from the PSTN side (e.g., Trunk connected to a PBX), it sends an INVITE to the IP with a From header as follows: From: "anonymous"&lt;anonymous@anonymous.invalid&gt;. This is in accordance with RFC 3325. However, when this parameter is set to 1, the device replaces the "anonymous.invalid" with its IP address.</p>
<b>[PAssertedUserName]</b>	<p>Defines a 'representative number' (up to 50 characters) that is used as the user part of the Request-URI in the P-Asserted-Identity header of an outgoing INVITE for Tel-to-IP calls.</p> <p>The default is null.</p>
<b>[UseAORInReferToHeader]</b>	<p>Defines the source for the SIP URI set in the Refer-To header of outgoing REFER messages.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) Use SIP URI from Contact header of the initial call.</li> <li><b>[1]</b> = Use SIP URI from To/From header of the initial call.</li> </ul>
Web: Enable User-Information Usage <b>[EnableUserInfoUsage]</b>	<p>Enables the usage of the User Information, which is loaded to the device in the User Information auxiliary file. For a description on User Information, see "Loading Auxiliary Files" on page 311.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
<b>[HandleReasonHeader]</b>	<p>Determines whether the device uses the value of the incoming SIP Reason header for Release Reason mapping.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = Disregard Reason header in incoming SIP messages.</li> </ul>



Parameter	Description
	<ul style="list-style-type: none"> <li><b>[1]</b> = (Default) Use the Reason header value for Release Reason mapping.</li> </ul>
<b>[EnableSilenceSuppInSDP]</b>	<p>Determines the device's behavior upon receipt of SIP Re-INVITE messages that include the SDP's 'silencesupp:off' attribute.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) Disregard the 'silencesupp' attribute.</li> <li><b>[1]</b> = Handle incoming Re-INVITE messages that include the 'silencesupp:off' attribute in the SDP as a request to switch to the Voice-Band-Data (VBD) mode. In addition, the device includes the attribute 'a=silencesupp:off' in its SDP offer.</li> </ul> <p><b>Note:</b> This parameter is applicable only if the G.711 coder is used.</p>
<b>[EnableRport]</b>	<p>Enables the usage of the 'rport' parameter in the Via header.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = Disabled (default)</li> <li><b>[1]</b> = Enabled</li> </ul> <p>The device adds an 'rport' parameter to the Via header of each outgoing SIP message. The first Proxy that receives this message sets the 'rport' value of the response to the actual port from where the request was received. This method is used, for example, to enable the device to identify its port mapping outside a NAT.</p> <p>If the Via header doesn't include the 'rport' parameter, the destination port of the response is obtained from the host part of the Via header. If the Via header includes the 'rport' parameter without a port value, the destination port of the response is the source port of the incoming request.</p> <p>If the Via header includes 'rport' with a port value (e.g., rport=1001), the destination port of the response is the port indicated in the 'rport' parameter.</p>
<b>[XChannelHeader]</b>	<p>Determines whether the SIP X-Channel header is added to SIP messages for providing information on the physical channel on which the call is received or placed.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) X-Channel header is not used.</li> <li><b>[1]</b> Enable = X-Channel header is generated by the device and sent in INVITE messages and 180, 183, and 200 OK SIP responses. The header includes the channel, and the device's IP address. For example, 'x-channel: DS/DS1-8;IP=192.168.13.1', where: <ul style="list-style-type: none"> <li>✓ 'DS/DS-1' is a constant string</li> <li>✓ '8' is the channel</li> <li>✓ 'IP=192.168.13.1' is the device's IP address</li> </ul> </li> </ul>
<b>[EnableRekeyAfter181]</b>	<p>Enables the device to send a re-INVITE with a new (different) SRTP key (in the SDP) if a SIP 181 response is received ("call is being forwarded"). The re-INVITE is sent immediately upon receipt of the 200 OK (when the call is answered).</p> <ul style="list-style-type: none"> <li><b>[0]</b> = Disable (default)</li> <li><b>[1]</b> = Enable</li> </ul> <p><b>Note:</b> This parameter is applicable only if SRTP is used.</p>
<b>[NumberOfActiveDialogs]</b>	<p>Defines the maximum number of concurrent, outgoing SIP REGISTER dialogs. This parameter is used to control the registration rate. The valid range is 1 to 20. The default is 20.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>Once a 200 OK is received in response to a REGISTER message, the REGISTER message is not considered in this maximum count</li> </ul>



Parameter	Description
	<p>limit.</p> <ul style="list-style-type: none"> <li>This parameter applies only to outgoing REGISTER messages (i.e., incoming is unlimited).</li> </ul>
Web: Default Release Cause <b>[DefaultReleaseCause]</b>	<p>Defines the default Release Cause (sent to IP) for IP-to-Tel calls when the device initiates a call release and an explicit matching cause for this release is not found.</p> <p>The default release cause is NO_ROUTE_TO_DESTINATION (3). Other common values include NO_CIRCUIT_AVAILABLE (34), DESTINATION_OUT_OF_ORDER (27), etc.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>The default release cause is described in the Q.931 notation and is translated to corresponding SIP 40x or 50x values (e.g., 3 to SIP 404, and 34 to SIP 503).</li> <li>For a list of SIP responses-Q.931 release cause mapping, see Alternative Routing to Trunk upon Q.931 Call Release Cause Code.</li> </ul>
Web: Enable Microsoft Extension <b>[EnableMicrosoftExt]</b>	<p>Enables the modification of the called and calling number for numbers received with Microsoft's proprietary "ext=xxx" parameter in the SIP INVITE URI user part. Microsoft Office Communications Server sometimes uses this proprietary parameter to indicate the extension number of the called or calling party.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <p>For example, if a calling party makes a call to telephone number 622125519100 Ext. 104, the device receives the SIP INVITE (from Microsoft's application) with the URI user part as INVITE sip:622125519100;ext=104@10.1.1.10 (or INVITE tel:622125519100;ext=104). If the parameter EnableMicrosofExt is enabled, the device modifies the called number by adding an "e" as the prefix, removing the "ext=" parameter, and adding the extension number as the suffix (e.g., <b>e622125519100104</b>). Once modified, the device can then manipulate the number further, using the Number Manipulation tables to leave only the last 3 digits (for example) for sending to a PBX.</p>
<b>[UseSIPURIForDiversionHeader]</b>	<p>Defines the URI format in the SIP Diversion header.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = 'tel:' (default)</li> <li><b>[1]</b> = 'sip:'</li> </ul>
<b>[TimeoutBetween100And18x]</b>	<p>Defines the timeout (in msec) between receiving a 100 Trying response and a subsequent 18x response. If a 18x response is not received within this timeout period, the call is disconnected.</p> <p>The valid range is 0 to 180,000 (i.e., 3 minutes). The default is 32000 (i.e., 32 sec).</p>
<b>[IgnoreRemoteSDPMKI]</b>	<p>Determines whether the device ignores the Master Key Identifier (MKI) if present in the SDP received from the remote side.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul>
Web: Comfort Noise Generation Negotiation <b>[ComfortNoiseNegotiation]</b>	<p>Enables negotiation and usage of Comfort Noise (CN).</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable</li> <li><b>[1]</b> Enable (default)</li> </ul> <p>The use of CN is indicated by including a payload type for CN on the media description line of the SDP. The device can use CN with a codec whose RTP time stamp clock rate is 8,000 Hz (G.711/G.726). The static</p>



Parameter	Description
	<p>payload type 13 is used. The use of CN is negotiated between sides. Therefore, if the remote side doesn't support CN, it is not used. Regardless of the device's settings, it always attempts to adapt to the remote SIP UA's request for CNG, as described below.</p> <p>To determine CNG support, the device uses the ComfortNoiseNegotiation parameter and the codec's SCE (silence suppression setting) using the CodersGroup parameter.</p> <p>If the ComfortNoiseNegotiation parameter is enabled, then the following occurs:</p> <ul style="list-style-type: none"> <li>▪ If the device is the initiator, it sends a "CN" in the SDP only if the SCE of the codec is enabled. If the remote UA responds with a "CN" in the SDP, then CNG occurs; otherwise, CNG does not occur.</li> <li>▪ If the device is the receiver and the remote SIP UA does not send a "CN" in the SDP, then no CNG occurs. If the remote side sends a "CN", the device attempts to be compatible with the remote side and even if the codec's SCE is disabled, CNG occurs.</li> </ul> <p>If the ComfortNoiseNegotiation parameter is disabled, then the device does not send "CN" in the SDP. However, if the codec's SCE is enabled, then CNG occurs.</p>
<b>[SDPEcanFormat]</b>	<p>Defines the echo canceller format in the outgoing SDP. The 'ecan' attribute is used in the SDP to indicate the use of echo cancellation.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = (Default) The 'ecan' attribute appears on the 'a=gpmid' line.</li> <li>▪ <b>[1]</b> = The 'ecan' attribute appears as a separate attribute.</li> <li>▪ <b>[2]</b> = The 'ecan' attribute is not included in the SDP.</li> <li>▪ <b>[3]</b> = The 'ecan' attribute and the 'vbd' parameter are not included in the SDP.</li> </ul> <p><b>Note:</b> This parameter is applicable only when the IsFaxUsed parameter is set to 2, and for re-INVITE messages generated by the device as result of modem or fax tone detection.</p>
Web: First Call Ringback Tone ID <b>[FirstCallIRBTId]</b>	<p>Defines the index of the first ringback tone in the CPT file. This option enables an Application server to request the device to play a distinctive ringback tone to the calling party according to the destination of the call. The tone is played according to the Alert-Info header received in the 180 Ringing SIP response (the value of the Alert-Info header is added to the value of this parameter).</p> <p>The valid range is -1 to 1,000. The default is -1 (i.e., play standard ringback tone).</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ It is assumed that all ringback tones are defined in sequence in the CPT file.</li> <li>▪ In case of an MLPP call, the device uses the value of this parameter plus 1 as the index of the ringback tone in the CPT file (e.g., if this value is set to 1, then the index is 2, i.e., 1 + 1).</li> </ul>
Web: RTP Only Mode <b>[RTPOnlyMode]</b>	<p>Enables the device to send and receive RTP packets to and from remote endpoints without the need to establish a SIP session. The remote IP address is determined according to the Outbound IP Routing table (Prefix parameter). The port is the same port as the local RTP port (configured by the BaseUDPPort parameter and the channel on which the call is received).</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Transmit &amp; Receive = Send and receive RTP packets.</li> <li>▪ <b>[2]</b> Transmit Only= Send RTP packets only.</li> </ul>



Parameter	Description
	<ul style="list-style-type: none"> <li><b>[3]</b> Receive Only= Receive RTP packets only.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>To configure the RTP Only mode per trunk, use the RTPOnlyModeForTrunk_ID parameter.</li> <li>If per trunk configuration (using the RTPOnlyModeForTrunk_ID parameter) is set to a value other than the default, the RTPOnlyMode parameter value is ignored.</li> </ul>
Web/EMS: Media IP Version Preference <b>[MediaIPVersionPreference]</b>	<p>Determines the preferred RTP media IP addressing version for outgoing SIP calls. This is indicated in the "c=" field (Connection Information) of the SDP.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Only IPv4 = (Default) offer includes only IPv4 media IP addresses.</li> <li><b>[1]</b> Only IPv6 = offer includes only IPv6 media IPs addresses.</li> <li><b>[2]</b> Prefer IPv4 = offer includes both IPv4 and IPv6 media IP addresses, but the first media is IPv4.</li> <li><b>[3]</b> Prefer IPv6 = offer includes both IPv4 and IPv6 media IP addresses, but the first media is IPv6.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This parameter is applicable only when the device offers an SDP.</li> <li>The IP addressing version is determined according to the first SDP "m=" field.</li> <li>This parameter can be configured per IP Profile, using the parameter IPProfile (see Configuring IP Profiles on page 189).</li> </ul>
<b>Retransmission Parameters</b>	
Web: SIP T1 Retransmission Timer <b>[msec]</b> <b>[SipT1Rtx]</b>	<p>Defines the time interval (in msec) between the first transmission of a SIP message and the first retransmission of the same message. The default is 500.</p> <p><b>Note:</b> The time interval between subsequent retransmissions of the same SIP message starts with SipT1Rtx. For INVITE requests, it is multiplied by two for each new retransmitted message. For all other SIP messages, it is multiplied by two until SipT2Rtx. For example, assuming SipT1Rtx = 500 and SipT2Rtx = 4000:</p> <ul style="list-style-type: none"> <li>The first retransmission is sent after 500 msec.</li> <li>The second retransmission is sent after 1000 (2*500) msec.</li> <li>The third retransmission is sent after 2000 (2*1000) msec.</li> <li>The fourth retransmission and subsequent retransmissions until SIPMaxRtx are sent after 4000 (2*2000) msec.</li> </ul>
Web: SIP T2 Retransmission Timer <b>[msec]</b> <b>[SipT2Rtx]</b>	<p>Defines the maximum interval (in msec) between retransmissions of SIP messages (except for INVITE requests). The default is 4000.</p> <p><b>Note:</b> The time interval between subsequent retransmissions of the same SIP message starts with SipT1Rtx and is multiplied by two until SipT2Rtx.</p>
Web: SIP Maximum RTX <b>[SIPMaxRtx]</b>	<p>Defines the maximum number of UDP transmissions of SIP messages (first transmission plus retransmissions). The range is 1 to 30. The default is 7.</p>



Parameter	Description
Web: Number of RTX Before Hot-Swap <b>[HotSwapRtx]</b>	<p>Defines the number of retransmitted INVITE/REGISTER messages before the call is routed (hot swap) to another Proxy/Registrar.</p> <p>The valid range is 1 to 30. The default is 3.</p> <p><b>Note:</b> This parameter is also used for alternative routing. If a domain name in the SBC IP-to-IP Routing table is resolved into two IP addresses, and if there is no response for HotSwapRtx retransmissions to the INVITE message that is sent to the first IP address, the device immediately initiates a call to the second IP address.</p>
<b>SIP Message Manipulations Table</b>	
Web: Message Manipulations <b>[MessageManipulations]</b>	<p>This table parameter defines manipulation rules for SIP header messages.</p> <p>The format of this parameter is as follows:</p> <pre>[ MessageManipulations] FORMAT MessageManipulations_Index = MessageManipulations_ManSetID, MessageManipulations_MessageType, MessageManipulations_Condition, MessageManipulations_ActionSubject, MessageManipulations_ActionType, MessageManipulations_ActionValue, MessageManipulations_RowRole; [MessageManipulations]</pre> <p>For example, the below configuration changes the user part of the SIP From header to 200:</p> <pre>MessageManipulations 1 = 0, Invite.Request, , Header.From.Url.User, 2, 200, 0;</pre> <p><b>Note:</b> For a detailed description of this table, see "Configuring SIP Message Manipulation" on page <a href="#">182</a>.</p>
<b>Message Policy Table</b>	
Web: Message Policy Table <b>[MessagePolicy]</b>	<p>This table parameter configures SIP message policy rules for blocking (blacklist) unwanted incoming SIP messages or allowing (whitelist) receipt of desired messages. The format of this parameter is as follows:</p> <pre>[MessagePolicy] FORMAT MessagePolicy_Index = MessagePolicy_Policy, MessagePolicy_MaxMessageLength, MessagePolicy_MaxHeaderLength, MessagePolicy_MaxBodyLength, MessagePolicy_MaxNumHeaders, MessagePolicy_MaxNumBodies, MessagePolicy_SendRejection, MessagePolicy_MethodListType, MessagePolicy_MethodList, MessagePolicy_BodyListType, MessagePolicy_BodyList; [/MessagePolicy]</pre> <p><b>Note:</b> For a detailed description of this table, see "Configuring SIP Message Policy Rules".</p>



## 42.9 Profile Parameters

The profile parameters are described in the table below.

**Table 42-31: Profile Parameters**

Parameter	Description
<b>IP Profile Table</b>	
Web: IP Profile Settings [IPProfile]	<p>This table parameter configures the IP Profile table. Each IP Profile ID includes a set of parameters (which are typically configured separately using their individual "global" parameters). You can later assign these IP Profiles to outbound IP routing rules (Prefix parameter), inbound IP routing rules and IP Groups.</p> <p>The format of this parameter is as follows: [IPProfile] FORMAT IpProfile_Index = IpProfile_ProfileName, IpProfile_IpPreference, IpProfile_CodersGroupID, IpProfile_IsFaxUsed, IpProfile_JitterBufMinDelay, IpProfile_JitterBufOptFactor, IpProfile_IPDiffServ, IpProfile_SigIPDiffServ, IpProfile_SCE, IpProfile_RTPRedundancyDepth, IpProfile_RemoteBaseUDPPort, IpProfile_CNGmode, IpProfile_VxxTransportType, IpProfile_NSEMode, IpProfile_IsDTMFUsed, IpProfile_PlayRBTone2IP, IpProfile_EnableEarlyMedia, IpProfile_ProgressIndicator2IP, IpProfile_EnableEchoCanceller, IpProfile_CopyDest2RedirectNumber, IpProfile_MediaSecurityBehaviour, IpProfile_CallLimit, IpProfile_DisconnectOnBrokenConnection, IpProfile_FirstTxDtmfOption, IpProfile_SecondTxDtmfOption, IpProfile_RxDTMFOption, IpProfile_EnableHold, IpProfile_InputGain, IpProfile_VoiceVolume, IpProfile_AddIEInSetup, IpProfile_SBCExtensionCodersGroupID, IpProfile_MediaIPVersionPreference, IpProfile_TranscodingMode, IpProfile_SBCAllowedCodersGroupID, IpProfile_SBCAllowedCodersMode, IpProfile_SBCMediaSecurityBehaviour, IpProfile_SBCRFC2833Behavior, IpProfile_SBCAlternativeDTMFMethod, IpProfile_SBCAssertIdentity, IpProfile_AMDSensitivityParameterSuit, IpProfile_AMDSensitivityLevel, IpProfile_AMDMaxGreetingTime, IpProfile_AMDMaxPostSilenceGreetingTime, IpProfile_SBCDiversionsMode, IpProfile_SBCHistoryInfoMode, IpProfile_EnableQSIGTunneling, IpProfile_SBCFaxCodersGroupID, IpProfile_SBCFaxBehavior, IpProfile_SBCFaxOfferMode, IpProfile_SBCFaxAnswerMode, IpProfile_SbcPrackMode, IpProfile_SBCSessionExpiresMode, IpProfile_SBCRemoteUpdateSupport, IpProfile_SBCRemoteReinviteSupport, IpProfile_SBCRemoteDelayedOfferSupport, IpProfile_SBCRemoteReferBehavior, IpProfile_SBCRemote3xxBehavior, IpProfile_SBCRemoteMultiple18xSupport, IpProfile_SBCRemoteEarlyMediaResponseType, IpProfile_SBCRemoteEarlyMediaSupport, IpProfile_EnableSymmetricMKI, IpProfile_MKISize, IpProfile_SBCEnforceMKISize, IpProfile_SBCRemoteEarlyMediaRTP, IpProfile_SBCRemoteSupportsRFC3960, IpProfile_SBCRemoteCanPlayRingback, IpProfile_EnableEarly183, IpProfile_EarlyAnswerTimeout, IpProfile_SBC2833DTMFPayloadType, IpProfile_SBCUserRegistrationTime,</p>



Parameter	Description
	<p>IpProfile_ResetSRTPStateUponRekey, IpProfile_AmdMode, IpProfile_SBCReliableHeldToneSource, IpProfile_SBCPlayHeldTone, IpProfile_SBCRemoteHoldFormat, IpProfile_DelayTimeForInvite; [IPProfile]</p> <p><b>Note:</b> For a description of this table, see "Configuring IP Profiles" on page 189.</p>

## 42.10 Channel Parameters

This subsection describes the device's channel parameters.

### 42.10.1 RTP, RTCP and T.38 Parameters

The RTP, RTCP and T.38 parameters are described in the table below.

**Table 42-32: RTP/RTCP and T.38 Parameters**

Parameter	Description
<p>Web: RTP Base UDP Port EMS: Base UDP Port <b>[BaseUDPport]</b></p>	<p>Defines the lower boundary of the UDP port used for RTP, RTCP (RTP port + 1) and T.38 (RTP port + 2). For example, if the Base UDP Port is set to 6000, then one channel may use the ports RTP 6000, RTCP 6001, and T.38 6002, while another channel may use RTP 6010, RTCP 6011, and T.38 6012, and so on.</p> <p>The range of possible UDP ports is 6,000 to 64,000. The default base UDP port is 6000.</p> <p>Once this parameter is configured, the UDP port range (lower to upper boundary) is calculated as follows:</p> <ul style="list-style-type: none"> <li>BaseUDPport to BaseUDPport + 4000*10</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>The UDP ports are allocated randomly to channels.</li> <li>You can define a UDP port range per Media Realm (see Configuring Media Realms on page 130).</li> <li>If RTP Base UDP Port is not a factor of 10, the following message is generated: 'invalid local RTP port'.</li> </ul>
<p>EMS: No Op Enable <b>[NoOpEnable]</b></p>	<p>Enables the transmission of RTP or T.38 No-Op packets.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = Disable (default)</li> <li><b>[1]</b> = Enable</li> </ul> <p>This mechanism ensures that the NAT binding remains open during RTP or T.38 silence periods.</p>
<p>EMS: No Op Interval <b>[NoOpInterval]</b></p>	<p>Defines the time interval in which RTP or T.38 No-Op packets are sent in the case of silence (no RTP/T.38 traffic) when No-Op packet transmission is enabled.</p> <p>The valid range is 20 to 65,000 msec. The default is 10,000.</p> <p><b>Note:</b> To enable No-Op packet transmission, use the NoOpEnable parameter.</p>



Parameter	Description
EMS: No Op Payload Type <b>[RTPNoOpPayloadType]</b>	<p>Defines the payload type of No-Op packets.</p> <p>The valid range is 96 to 127 (for the range of Dynamic RTP Payload Type for all types of non hard-coded RTP Payload types, refer to RFC 3551). The default is 120.</p> <p><b>Note:</b> When defining this parameter, ensure that it doesn't cause collision with other payload types.</p>
<b>[RTCPActivationMode]</b>	<p>Disables RTCP traffic when there is no RTP traffic. This feature is useful, for example, to stop RTCP traffic that is typically sent when calls are put on hold (by an INVITE with 'a=inactive' in the SDP).</p> <ul style="list-style-type: none"> <li><b>[0]</b> Active Always = (Default) RTCP is active even during inactive RTP periods, i.e., when the media is in 'recvonly' or 'inactive' mode.</li> <li><b>[1]</b> Inactive Only If RTP Inactive = No RTCP is sent when RTP is inactive.</li> </ul>
<b>RTP Control Protocol Extended Reports (RTCP XR) Parameters</b>	
Web: Enable RTCP XR EMS: RTCP XR Enable <b>[VQMonEnable]</b>	<p>Enables voice quality monitoring and RTCP XR, according to Internet-Draft draft-ietf-sipping-rtcp-summary-13.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
Web: Minimum Gap Size EMS: GMin <b>[VQMonGMin]</b>	<p>Defines the voice quality monitoring - minimum gap size (number of frames).</p> <p>The default is 16.</p>
Web/EMS: Burst Threshold <b>[VQMonBurstHR]</b>	<p>Defines the voice quality monitoring - excessive burst alert threshold.</p> <p>The default is -1 (i.e., no alerts are issued).</p>
Web/EMS: Delay Threshold <b>[VQMonDelayTHR]</b>	<p>Defines the voice quality monitoring - excessive delay alert threshold.</p> <p>The default is -1 (i.e., no alerts are issued).</p>
Web: R-Value Delay Threshold EMS: End of Call Rval Delay Threshold <b>[VQMonEOCRValTHR]</b>	<p>Defines the voice quality monitoring - end of call low quality alert threshold.</p> <p>The default is -1 (i.e., no alerts are issued).</p>
Web: RTCP XR Packet Interval EMS: Packet Interval <b>[RTCPInterval]</b>	<p>Defines the time interval (in msec) between adjacent RTCP reports.</p> <p>The valid value range is 0 to 65,535. The default is 5,000.</p>
Web: Disable RTCP XR Interval Randomization EMS: Disable Interval Randomization <b>[DisableRTCPRandomize]</b>	<p>Determines whether RTCP report intervals are randomized or whether each report interval accords exactly to the parameter RTCPInterval.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) Randomize</li> <li><b>[1]</b> Enable = No Randomize</li> </ul>
EMS: RTCP XR Collection Server Transport Type <b>[RTCPXRESCTransportType]</b>	<p>Defines the transport layer used for outgoing SIP dialogs initiated by the device to the RTCP XR Collection Server.</p> <ul style="list-style-type: none"> <li><b>[-1]</b> Not Configured (default)</li> <li><b>[0]</b> UDP</li> <li><b>[1]</b> TCP</li> </ul>



Parameter	Description
	<ul style="list-style-type: none"> <li><b>[2]</b> TLS</li> </ul> <p><b>Note:</b> When set to <b>[-1]</b>, the value of the SIPTransportType parameter is used.</p>
Web: RTCP XR Collection Server EMS: Esc IP <b>[RTCPXREscIP]</b>	Defines the IP address of the Event State Compositor (ESC). The device sends RTCP XR reports to this server, using SIP PUBLISH messages. The address can be configured as a numerical IP address or as a domain name.
Web: RTCP XR Report Mode EMS: Report Mode <b>[RTCPXRReportMode]</b>	<p>Determines whether RTCP XR reports are sent to the Event State Compositor (ESC) and defines the interval at which they are sent.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) RTCP XR reports are not sent to the ESC.</li> <li><b>[1]</b> End Call = RTCP XR reports are sent to the ESC at the end of each call.</li> <li><b>[2]</b> End Call &amp; Periodic = RTCP XR reports are sent to the ESC at the end of each call and periodically according to the RTCPInterval parameter.</li> </ul>

## 42.11 Least Cost Routing Parameters

The Least Cost Routing (LCR) parameters are described in the table below.

**Table 42-33: LCR Parameters**

Parameter	Description
Web: Routing Rule Groups Table <b>[RoutingRuleGroups]</b>	<p>This table parameter enables the LCR feature and configures the average call duration and default call cost. The default call cost determines whether routing rules that are not configured with a Cost Group are considered as a higher or lower cost route compared to other matching routing rules that are assigned Cost Groups.</p> <p>[ RoutingRuleGroups ]            FORMAT RoutingRuleGroups_Index =            RoutingRuleGroups_LCREnable,            RoutingRuleGroups_LCRAverageCallLength,            RoutingRuleGroups_LCRDefaultCost;            [ \RoutingRuleGroups ]</p> <p><b>Note:</b> For a detailed description of this table, see "Enabling LCR and Configuring Default LCR" on page 152.</p>
Web: Cost Group Table <b>[CostGroupTable]</b>	<p>This table parameter configures the Cost Groups for LCR, where each Cost Group is configured with a name, fixed call connection charge, and a call rate (charge per minute).</p> <p>[ CostGroupTable ]            FORMAT CostGroupTable_Index =            CostGroupTable_CostGroupName,            CostGroupTable_DefaultConnectionCost,            CostGroupTable_DefaultMinuteCost;            [ \CostGroupTable ]</p> <p>For example: CostGroupTable 2 = "Local Calls", 2, 1;</p> <p><b>Note:</b> For a detailed description of this table, see "Configuring Cost Groups" on page 153.</p>



Parameter	Description
Web: Cost Group > Time Band Table <b>[CostGroupTimebands]</b>	<p>This table parameter configures time bands and associates them with Cost Groups.</p> <p><b>[CostGroupTimebands]</b>            FORMAT CostGroupTimebands_TimebandIndex =            CostGroupTimebands_StartTime, CostGroupTimebands_EndTime,            CostGroupTimebands_ConnectionCost,            CostGroupTimebands_MinuteCost;  <b>[\\CostGroupTimebands]</b></p> <p><b>Note:</b> For a detailed description of this table, see "Configuring Time Bands for Cost Groups" on page 154.</p>

## 42.12 LDAP Parameters

The Lightweight Directory Access Protocol (LDAP) parameters are described in the table below. For more information on routing based on LDAP, see "Routing Based on LDAP Active Directory Queries" on page 141.

**Table 42-34: LDAP Parameters**

Parameter	Description
Web: LDAP Service <b>[LDAPServiceEnable]</b>	<p>Enables the LDAP feature.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
Web: LDAP Server IP <b>[LDAPServerIP]</b>	<p>Defines the LDAP server's address as an IP address (in dotted-decimal notation, e.g., 192.10.1.255). The default is 0.0.0.0.</p>
Web: LDAP Server Port <b>[LDAPServerPort]</b>	<p>Defines the LDAP server's port number. The valid value range is 0 to 65535. The default port number is 389.</p>
Web: LDAP Server Domain Name <b>[LDAPServerDomainName]</b>	<p>Defines the host name (FQDN) of the LDAP server. The device tries to connect to the LDAP server according to the IP address list received in the DNS query. If there is no connection to the LDAP server or the connection to the LDAP server fails, the device tries to connect to the LDAP server with the next IP address in the DNS query list.</p> <p><b>Note:</b> The 'LDAP Server IP' parameter takes precedence over this parameter. Thus, if you want to use an FQDN, keep the 'LDAP Server IP' parameter empty.</p>
Web: LDAP Password <b>[LDAPPassword]</b>	<p>Defines the LDAP server's user password.</p>
Web: LDAP Bind DN <b>[LDAPBindDN]</b>	<p>Defines the LDAP server's bind Distinguished Name (DN). This is used as the username during connection and binding to the server.</p> <p>For example: LDAPBindDN = "CN=Search user,OU=Labs,DC=OCSR2,DC=local"</p> <p><b>Note:</b> The DN is used to uniquely name an Active Directory</p>



Parameter	Description
	object.
Web: LDAP Search Dn <b>[LDAPSearchDN]</b>	<p>Defines up to three search DN's for LDAP search queries. These are the DN subtrees where the search is done. This parameter is mandatory for the search.</p> <p>The format of this parameter is as follows:</p> <pre>[LdapSearchDNs ] FORMAT LdapSearchDNs_Index = LdapSearchDNs_Base_Path; [ \LdapSearchDNs ]</pre> <p>For example:</p> <pre>LdapSearchDNs 0 = "CN=Search user,OU=NY,DC=OCSR2,DC=local"; LdapSearchDNs 1 = "CN=Search user,OU=SF,DC=OCSR2,DC=local";</pre> <p>In this example, the DN path is defined by the LDAP names, cn (common name), ou (organizational unit) and dc (domain component).</p> <p><b>Note:</b> If you configure multiple DN's, you can specify whether the search is done sequentially or in parallel, using the LDAPSearchDNsinParallel parameter.</p>
<b>[LDAPSearchDNsinParallel]</b>	<p>Defines the LDAP query DN search method in the AD database if multiple search DN's are configured, using the LDAPSearchDNs parameter.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Sequential = If the first DN search fails, the search is done on the next configured DN, and so on.</li> <li><b>[1]</b> Parallel (Default)</li> </ul>
Web: LDAP Server Max Respond Time <b>[LDAPServerMaxRespondTime]</b>	<p>Defines the time (in seconds) that the device waits for LDAP server responses.</p> <p>The valid value range is 0 to 86400. The default is 3000.</p>
<b>[LDAPDebugMode]</b>	<p>Determines whether to enable the LDAP task debug messages. This is used for providing debug information regarding LDAP tasks.</p> <p>The valid value range is 0 to 3. The default is 0.</p>
Web: MS LDAP OCS Number attribute name <b>[MSLDAPOCSNumAttributeName]</b>	<p>Defines the name of the attribute that represents the user OCS number in the Microsoft AD database.</p> <p>The valid value is a string of up to 49 characters. The default is "msRTCSIP-PrimaryUserAddress".</p>
Web: MS LDAP PBX Number attribute name <b>[MSLDAPPBXNumAttributeName]</b>	<p>Defines the name of the attribute that represents the user PBX number in the Microsoft AD database.</p> <p>The valid value is a string of up to 49 characters. The default is "telephoneNumber".</p>
Web: MS LDAP MOBILE Number attribute name <b>[MSLDAPMobileNumAttributeName]</b>	<p>Defines the name of the attribute that represents the user Mobile number in the Microsoft AD database.</p> <p>The valid value is a string of up to 49 characters. The default is "mobile".</p>



Parameter	Description
<b>[MSLDAPPrivateNumAttributeName]</b>	Defines the name of the attribute that represents the user's private number in the AD. If this value equals the value of the MSLDAPPrimaryKey or MSLDAPSecondaryKey parameter, then the device queries the AD for the destination number in this private attribute name; otherwise, this parameter is not used as a search key. The default is "msRTCSIP-PrivateLine".
<b>[MSLDAPPrimaryKey]</b>	Defines the name of the attribute used as a query search key for the destination number in the AD. This is used instead of the "PBX" attribute name (configured by the MSLDAPPBXNumAttributeName parameter). The default is not configured.
<b>[MSLDAPSecondaryKey]</b>	Defines the name of the attribute used as the second query search key for the destination number in the AD, if the primary search key or PBX search is not found.
LDAP Cache Service <b>[LDAPCacheEnable]</b>	Enables the LDAP cache service. <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <b>Notes:</b> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>For more information on LDAP caching, see "Configuring the Device's LDAP Cache" on page 142.</li> </ul>
LDAP Cache Entry Timeout <b>[LDAPCacheEntryTimeout]</b>	Defines the duration (in minutes) that an entry in the LDAP cache is valid. If the timeout expires, the cached entry is only used if there is no connectivity with the LDAP server. The default is 1200.
LDAP Cache Entry Removal Timeout <b>[LDAPCacheEntryRemovalTimeout]</b>	Defines the duration (in hours) after which the LDAP entry is removed from the cache. The default is 0.

## 42.13 SBC Parameters

The SBC parameters are described in the table below.

**Table 42-35: SBC Parameters**

Parameter	Description
Web: Enable SBC <b>[EnableSBCApplication]</b>	Enables the Session Border Control (SBC) application. <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default)</li> <li><b>[1]</b> Enable</li> </ul> <b>Notes:</b> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>In addition to enabling this parameter, the number of maximum SBC/IP-to-IP sessions must be defined in the Software License Key.</li> </ul>
Web: Allow Unclassified Calls	Determines whether incoming calls that cannot be classified (i.e.



Parameter	Description
<b>[AllowUnclassifiedCalls]</b>	<p>classification process fails) to a Source IP Group are rejected or processed.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Reject = Call is rejected if classification fails.</li> <li>▪ <b>[1]</b> Allow = (Default) If classification fails, the incoming packet is assigned to a source IP Group (and subsequently processed) as follows: <ul style="list-style-type: none"> <li>✓ The source SRD is determined according to the SIP Interface to where the SIP-initiating dialog request is sent. The source IP Group is set to the default IP Group associated with this SRD.</li> <li>✓ If the source SRD is ID 0, then source IP Group ID 0 is chosen. In case of any other SRD, then the first IP Group associated with this SRD is chosen as the source IP Group or the call. If no IP Group is associated with this SRD, the call is rejected.</li> </ul> </li> </ul>
Web: SBC No Answer Timeout <b>[SBCAlertTimeout]</b>	<p>Defines the timeout (in seconds) for SBC outgoing (outbound IP routing) SIP INVITE messages. If the called IP party does not answer the call within this user-defined interval, the device disconnects the session. The device starts the timeout count upon receipt of a SIP 180 Ringing response from the called party. If no other SIP response (for example, 200 OK) is received thereafter within this timeout, the call is released.</p> <p>The valid range is 0 to 3600 seconds. the default is 600.</p>
Web: SBC Max Forwards Limit <b>[SBCMaxForwardsLimit]</b>	<p>Defines the Max-Forwards SIP header value. The Max-Forwards header is used to limit the number of servers (such as proxies) that can forward the SIP request. The Max-Forwards value indicates the remaining number of times this request message is allowed to be forwarded. This count is decremented by each server that forwards the request.</p> <p>This parameter affects the Max-Forwards header in the received message as follows:</p> <ul style="list-style-type: none"> <li>▪ If the received header's original value is 0, the message is not passed on and is rejected.</li> <li>▪ If the received header's original value is less than this parameter's value, the header's value is decremented before being sent on.</li> <li>▪ If the received header's original value is greater than the parameter's value, the header's value is replaced by the user-defined parameter's value.</li> </ul> <p>The valid value range is 1-70. The default is 10.</p>
Web: SBC Session-Expires <b>[SBCSessionExpires]</b>	<p>Defines the SBC session refresh timer (in seconds) in the Session-Expires header of outgoing INVITE messages.</p> <p>The valid value range is 90 (according to RFC 4028) to 86400. The default is 180.</p>
Web: Minimum Session-Expires <b>[SBCMinSE]</b>	<p>Defines the minimum amount of time (in seconds) between session refresh requests in a dialog before the session is considered timed out. This value is conveyed in the SIP Min-SE header.</p> <p>The valid range is 0 (default) to 1,000,000 (where 0 means that the device does not limit Session-Expires).</p>
Web: Handle P-Asserted-Identity <b>[SBCAssertIdentity]</b>	<p>Determines the device's privacy handling of the P-Asserted-Identity header. This indicates how the outgoing SIP message</p>



Parameter	Description
	<p>asserts identity.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Don't Care = (Default) P-Asserted Identity header is not affected.</li> <li>▪ <b>[1]</b> Add P-Asserted-Identity Header = Adds a P-Asserted-Identity header. The header's values are taken from the source URL.</li> <li>▪ <b>[2]</b> Remove P-Asserted-Identity Header = Removes the P-Asserted-Identity header.</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ This parameter affects only the initial INVITE request.</li> <li>▪ The configuration of privacy handling in the IP Group table takes precedence over the settings of this global parameter. <ul style="list-style-type: none"> <li>✓ If in the IP Group this parameter is set to 'Don't care', then the settings of this global parameter is used.</li> <li>✓ If this global parameter and the IP Group are set to 'Don't care', the device uses the same P-Asserted-Identity header (if present) in the incoming message for the outgoing message.</li> </ul> </li> <li>▪ This parameter can also be configured in an IP Profile.</li> </ul>
Web: Keep original user in Register <b>[SBCKeepContactUserinRegister]</b>	<p>Determines whether the device replaces the Contact user with a unique Contact user in the outgoing message in response to a REGISTER request.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable = (Default) The device replaces the original Contact user with a unique Contact user, for example: <ul style="list-style-type: none"> <li>✓ Received Contact: &lt;sip:123@domain.com&gt;</li> <li>✓ Outgoing (unique) Contact: &lt;sip:FEU1_7_1@SBC&gt;</li> </ul> </li> <li>▪ <b>[1]</b> Enable = The original Contact user is retained and used in the outgoing REGISTER request.</li> </ul> <p><b>Note:</b> This parameter is applicable only to REGISTER messages received from User-type IP Groups and that are sent to Server-type IP Groups.</p>
Web: SBC Remote Refer Behavior <b>[SBCReferBehavior]</b>	<p>Determines the device's handling of REFER requests.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Transparent = (Default) Refer-To header is unchanged and the device forwards the REFER as is.</li> <li>▪ <b>[1]</b> DB URL = Changes the Refer-To header so that the re-routed INVITE is sent through the SBC: <ul style="list-style-type: none"> <li>d. Before forwarding the REFER request, the device changes the host part to the device's IP address and adds a special prefix ("T-&amp;R_") to the Contact user part.</li> <li>e. The incoming INVITE is identified as a REFER-resultant INVITE according to this special prefix.</li> <li>f. The device replaces the host part in the Request-URI with the host from the REFER contact. The special prefix remains in the user part for regular classification, manipulation, and routing. The special prefix can also be used for specific routing rules for REFER-resultant INVITEs.</li> <li>g. The special prefix is removed before the resultant INVITE is sent to the destination.</li> </ul> </li> <li>▪ <b>[2]</b> IP Group Name = Sets the host part in the REFER message to the name defined for the IP Group (in the IP Group table).</li> </ul>



Parameter	Description
	<ul style="list-style-type: none"> <li>▪ <b>[3] Handle Locally</b> = Handles the incoming REFER request itself without forwarding the REFER. The device generates a new INVITE to the alternative destination according to the rules in the IP-to-IP Routing table (the 'Call Trigger' field must be set to <b>REFER</b>).</li> </ul> <p><b>Note:</b> This parameter can be configured in an IP Profile.</p>
<b>[SBCXferPrefix]</b>	<p>When the SBCReferBehavior is set to 1, the device, while interworking the SIP REFER message, adds the prefix "T~&amp;R-" to the user part of the URI in the Refer-To header. After this, the device can receive an INVITE with such a prefix (the INVITE is sent by the UA that receives the REFER message or 302 response). If the device receives an INVITE with such a prefix, it replaces the prefix with the value defined for the SBCXferPrefix parameter.</p> <p>The default is empty ("").</p> <p><b>Note:</b> This feature is also applicable to 3xx redirect responses. The device adds the prefix "T~&amp;R-" to the URI user part in the Contact header if the SBC3xxBehavior parameter is set to 1.</p>
<b>[SBC3xxBehavior]</b>	<p>Determines the device's handling of SIP 3xx responses. When enabled, the device handles SIP redirections between different subnets (e.g., between LAN and WAN sides). This is required where the new address provided by the redirector (Redirect sever) may not be reachable by the far-end user (FEU) located in another subnet. For example, a far-end user (FEU) in the WAN sends a SIP request via the device to a Redirect server in the LAN, and the Redirect server replies with a SIP 3xx response to a PBX in the LAN in the Contact header. If the device sends this response as is (i.e., with the original Contact header), the FEU is unable to reach the new destination.</p> <ul style="list-style-type: none"> <li>▪ <b>[0] Transparent</b> = (Default) The device forwards the received SIP 3xx response as is, without changing the Contact header (i.e., transparent handling).</li> <li>▪ <b>[1] DB URL</b> = The device changes the Contact header so that the re-route request is sent through the the device. The device changes the URI in the Contact header of the received SIP 3xx response to its own URI and adds a special user prefix ("T~&amp;R_"), which is then sent to the FEU. The FEU then sends a new INVITE to the device, which the device then sends to the correct destination.</li> <li>▪ <b>[2] Handle Locally</b> = The device handles SIP 3xx responses on behalf of the dialog-initiating UA and retries the request (e.g., INVITE) using one or more alternative URIs included in the 3xx response. The device sends the new request to the alternative destination according to the IP-to-IP Routing table (the 'Call Trigger' field must be set to <b>3xx</b>).</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ When this parameter is changed from 1 to 0, new 3xx Contact headers remain unchanged. However, requests with the special prefix continue using the device's database to locate the new destination.</li> <li>▪ Only one database entry is supported for the same host, port, and transport combination. For example, the following URLs cannot be distinguished by the device: <ul style="list-style-type: none"> <li>✓ sip:10.10.10.10:5060;transport=tcp;param=a</li> </ul> </li> </ul>



Parameter	Description
	<ul style="list-style-type: none"> <li>✓ sip:10.10.10.10:5060;transport=tcp;param=b</li> <li>▪ The database entry expires two hours after the last use.</li> <li>▪ The maximum number of destinations (i.e., database entries) is 50.</li> <li>▪ This parameter can also be configured as an IP Profile.</li> <li>▪ For more information on SIP 3xx Redirect response handling, see "Handling SIP 3xx Redirect Responses" on page 212.</li> </ul>
Web: Enforce Media Order <b>[SBCEnforceMediaOrder]</b>	<p>Enables the device to arrange media lines ('m=' line) in the SDP offer according to the previous offer-answer exchange (RFC 3264).</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable</li> <li>▪ <b>[1]</b> Enable (default)</li> </ul>
Web: Lifetime of the nonce in seconds <b>[AuthNonceDuration]</b>	<p>Defines the lifetime (in seconds) that the current nonce is valid for server-based authentication. The device challenges a message that attempts to use a server nonce beyond this period. This parameter is used to provide replay protection (i.e., ensures that old communication streams are not used in replay attacks). The valid value range is 30 to 600. The default is 300.</p>
Web: Authentication Challenge Method <b>[AuthChallengeMethod]</b>	<p>Defines the type of server-based authentication challenge.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> 0 = (Default) Send SIP 401 "Unauthorized" with a WWW-Authenticate header as the authentication challenge response.</li> <li>▪ <b>[1]</b> 1 = Send SIP 407 "Proxy Authentication Required" with a Proxy-Authenticate header as the authentication challenge response.</li> </ul>
Web: Authentication Quality of Protection <b>[AuthQOP]</b>	<p>Defines the authentication and integrity level of quality of protection (QoP) for digest authentication offered to the client. When the device challenges a SIP request (e.g., INVITE), it sends a SIP 401 response with the Proxy-Authenticate header or WWW-Authenticate header containing the 'qop' parameter. The QoP offered in the 401 response can be 'auth', 'auth-int', both 'auth' and 'auth-int', or the 'qop' parameter can be omitted from the 401 response. In response to the 401, the client needs to send the device another INVITE with the MD5 hash of the INVITE message and indicate the selected auth type.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> 0 = The device sends 'qop=auth' in the SIP response, requesting authentication (i.e., validates user by checking user name and password). This option does not authenticate the message body (i.e., SDP).</li> <li>▪ <b>[1]</b> 1 = The device sends 'qop=auth-int' in the SIP response, indicating required authentication and authentication with integrity (e.g., checksum). This option restricts the client to authenticating the entire SIP message, including the body, if present.</li> <li>▪ <b>[2]</b> 2 = (Default) The device sends 'qop=auth, auth-int' in the SIP response, indicating either authentication or integrity. This enables the client to choose 'auth' or 'auth-int'. If the client chooses 'auth-int', then the body is included in the authentication. If the client chooses 'auth', then the body is not authenticated.</li> <li>▪ <b>[3]</b> 3 = No 'qop' parameter is offered by the device in the SIP 401 challenge message.</li> </ul>



Parameter	Description
Web: SBC User Registration Time <b>[SBCUserRegistrationTime]</b>	<p>Defines the duration (in seconds) of the periodic registrations between the user and the device (the device responds with this value to the user). When set to 0, the device does not change the Expires header's value received in the user's REGISTER request. If no Expires header is received in the REGISTER message and the SBCUserRegistrationTime parameter is set to 0, then by default, the Expires header's value is set to 180 seconds.</p> <p>The valid range is 0 to 2,000,000 seconds. The default is 0.</p> <p><b>Note:</b> This parameter can also be configured for an IP Profile (in the IP Profile table).</p>
Web: SBC Proxy Registration Time <b>[SBCProxyRegistrationTime]</b>	<p>Defines the duration (in seconds) for which the user is registered in the proxy database (after the device forwards the REGISTER message). When set to 0, the device sends the Expires header's value as received from the user to the proxy.</p> <p>The valid range is 0 to 2,000,000 seconds. The default is 0.</p>
Web: SBC Survivability Registration Time <b>[SBCSurvivabilityRegistrationTime]</b>	<p>Defines the duration of the periodic registrations between the user and the device, when the device is in survivability state (i.e., when REGISTER requests cannot be forwarded to the proxy and are terminated by the device). When set to 0, the device uses the value set by the SBCUserRegistrationTime parameter for the device's response.</p> <p>The valid range is 0 to 2,000,000 seconds. The default is 0.</p>
<b>[SBCEnableAASTRASurvivabilityNotice]</b>	<p>Enables the device to notify Aastra IP phones that the device is currently operating in Survivability mode. When this occurs, the Aastra IP phones display the message, "Stand Alone Mode" on their LCD screens. Survivability mode occurs when connectivity with the WAN fails and as a result, the device enables communication between IP phone users within the LAN enterprise.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = Disable</li> <li><b>[1]</b> = Enable</li> </ul> <p>When this feature is enabled and the SBC device is in Survivability mode, it responds to SIP REGISTER messages from the IP phones with a SIP 200 OK containing the following XML body:</p> <pre>Content-Type: application/xml &lt;?xml version="1.0" encoding="utf-8"?&gt; &lt;LMIDocument version="1.0"&gt;   &lt;LocalModeStatus&gt;     &lt;LocalModeActive&gt;true&lt;/LocalModeActive&gt;     &lt;LocalModeDisplay&gt;StandAlone Mode&lt;/LocalModeDisplay&gt;   &lt;/LocalModeStatus&gt; &lt;/LMIDocument&gt;</pre>
Web: SBC GRUU Mode <b>[SBCGruuMode]</b>	<p>Determines the Globally Routable User Agent (UA) URI (GRUU) support, according to RFC 5627.</p> <ul style="list-style-type: none"> <li><b>[0]</b> None = No GRUU is supplied to users.</li> <li><b>[1]</b> As Proxy = (Default) The device provides same GRUU types as the proxy provided the device's GRUU clients.</li> <li><b>[2]</b> Temporary only = Supply only temporary GRUU to users. (Currently not supported.)</li> </ul>



Parameter	Description
	<ul style="list-style-type: none"> <li>▪ <b>[3]</b> Public only = The device provides only public GRUU to users.</li> <li>▪ <b>[4]</b> Both = The device provides temporary and public GRUU to users. (Currently not supported.)</li> </ul> <p>This parameter allows the device to act as a GRUU server for its SIP UA clients, providing them with public GRUU's, according to RFC 5627. The public GRUU provided to the client is denoted in the SIP Contact header parameters, "pub-gruu". Public GRUU remains the same over registration expirations. On the other SBC leg communicating with the Proxy/Registrar, the device acts as a GRUU client.</p> <p>The device creates a GRUU value for each of its registered clients, which is mapped to the GRUU value received from the Proxy server. In other words, the created GRUU value is only used between the device and its clients (endpoints).</p> <p>Public-GRUU: sip:userA@domain.com;gr=unique-id</p>
Web: Bye Authentication <b>[SBCEnableByeAuthentication]</b>	<p>Enables authenticating a SIP BYE request before disconnecting the call. This feature prevents, for example, a scenario in which the SBC SIP client receives a BYE request from a third-party imposer assuming the identity of a participant in the call and as a consequence, the call between the first and second parties is inappropriately disconnected.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable = The device forwards the SIP authentication response (for the BYE request) to the request sender and waits for the user to authenticate it. The call is disconnected only if the authenticating server responds with a 200 OK.</li> </ul>
<b>[SBCExtensionsProvisioningMode]</b>	<p>Enables SBC user registration for interoperability with BroadSoft's BroadWorks server, to provide call survivability in case of connectivity failure with the BroadWorks server.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = (Default) Normal processing of REGISTER messages.</li> <li>▪ <b>[1]</b> = Registration method for BroadWorks server. In a failure scenario with BroadWorks, the device acts as a backup SIP proxy server, maintaining call continuity between the enterprise LAN users (subscribers) and between the subscribers and the PSTN (if provided).</li> </ul> <p><b>Note:</b> For a detailed description of this feature, see "Auto-Provisioning of Subscriber-Specific Information for BroadWorks Server" on page 218.</p>
Web: SBC Direct Media <b>[SBCDirectMedia]</b>	<p>Enables the No Media Anchoring feature (i.e., direct media) for all SBC calls. No Media Anchoring uses SIP signaling capabilities without handling the RTP/SRTP (media) flow between remote SIP user agents (UA). The RTP packets do not traverse the device, instead, the two SIP UAs establish a direct RTP/SRTP flow between one another. Signaling continues to traverse the device with minimal intermediation and involvement to enable certain SBC abilities such as routing</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable = (Default) All SRD calls via SBC are not direct media - internal SRD calls are according to SRD configuration.</li> <li>▪ <b>[1]</b> Enable = All SBC calls use the No Media Anchoring feature (i.e., direct media).</li> </ul> <p><b>Notes:</b></p>



Parameter	Description
	<ul style="list-style-type: none"> <li>For more information on No Media Anchoring, see "No Media Anchoring (Anti Tromboning)" on page 207.</li> <li>When No Media Anchoring is enabled: <ul style="list-style-type: none"> <li>✓ Manipulation is not done on SDP data (offer/answer transaction) such as ports and IP addresses.</li> <li>✓ Opening voice channels and allocation of IP media ports are not required.</li> <li>✓ Forced Transcoding and Extension Coders features are disabled for No Media Anchoring calls.</li> <li>✓ The Coder Restriction feature (Allowed Coders List) operates simultaneously with No Media Anchoring calls. Restricted coders are removed from the SDP offer message.</li> </ul> </li> <li>No Media Anchoring is typically implemented in the following scenarios: <ul style="list-style-type: none"> <li>✓ SBC device is located in the LAN.</li> <li>✓ Calls between two SIP UAs in the same LAN and signals are sent to a SIP proxy server that is located in the WAN.</li> <li>✓ SBC device does not do NAT traversal (for media) and all the users are in the same domain.</li> </ul> </li> <li>The benefits of implementing the No Media Anchoring feature includes the following: saves network bandwidth, reduces CPU usage (no RTP/SRTP handling), and avoids interference in SDP negotiation and header manipulation on RTP/SRTP.</li> <li>The process for handling the No Media Anchoring feature is as follows: <ul style="list-style-type: none"> <li>✓ Identifying a No Media Anchoring call according to configuration and the call's properties (such as source, destination, IP Group, and SRD).</li> <li>✓ Handling the identified No Media Anchoring call.</li> </ul> </li> <li>You can enable No Media Anchoring per SRD (using the IntraSRDMediaAnchoring parameter), whereby calls between two UAs that pertain to the same SRD (source and destination) are handled as a No Media Anchoring (direct media) call.</li> <li>Chosen configuration can't handle call from any UA to a foreign UA (vice versa) but both UAs belong to the same SRD and the parameter IntraSRDMediaAnchoring for that specific SRD is &gt; 0.</li> <li>When this parameter is disabled, No Media Anchoring calls between two UAs that belong to separate SRDs cannot be configured. No Media Anchoring calls between two UAs that belong to the same SRD is configurable only (in this case).</li> </ul>
Web: SBC Send Invite To All Contacts CLI: sbc-send-invite-to-all-contacts <b>[SBCSendInviteToAllContacts]</b>	<p>Enables call forking of INVITE message received with a Request-URI for a specific contact registered in the device's database, to all users under the same AOR as the contact.</p> <ul style="list-style-type: none"> <li><b>[0]</b> Disable (default) = Sends the INVITE only to the contact of the received Request-URI.</li> <li><b>[1]</b> Enable</li> </ul> <p><b>Note:</b> To configure call forking initiated by the device, see Initiating SIP Call Forking.</p>



Parameter	Description
Web: SBC Shared Line Registration Mode CLI: sbc-shared-line-reg-mode <b>[SBCSharedLineRegMode]</b>	Enables the termination on the device of SIP REGISTER messages from secondary lines pertaining to the Shared Line feature. <ul style="list-style-type: none"> <li><b>[0]</b> Disable = (Default) Device forwards the REGISTER messages as is (i.e., not terminated on the device).</li> <li><b>[1]</b> Enable = REGISTER messages of secondary lines are terminated on the device.</li> </ul> <b>Note:</b> The device always forwards REGISTER messages of the primary line.
Web: SBC Forking Handling Mode <b>[SBCForkingHandlingMode]</b>	Defines the handling of SIP 18x responses received due to call forking of an INVITE. <ul style="list-style-type: none"> <li><b>[0]</b> Latch On First = (Default) Only the first 18x is forwarded to the INVITE-initiating UA. If SIP 18x with SDP is received, the device opens a voice stream according to the received SDP and disregards any subsequent 18x forking responses (with or without SDP). If the first response is 180 without SDP, the device responds according to the PlayRBTone2TEL parameter and disregards the subsequent forking 18x responses.</li> <li><b>[1]</b> Sequential = All 18x responses are forwarded, one at a time (sequentially) to the INVITE-initiating UA. If a 18x arrives with an offer only, then only the first offer is forwarded to the INVITE-initiating UA and subsequent 18x responses are discarded.</li> </ul>
<b>[EnableSBCMediaSync]</b>	Enables SBC media synchronization process for calls established from SIP forking that is initiated by external proxy servers. It is possible that a call is established with the media not synchronized between the SBC legs. Media synchronization resolves this issue. <ul style="list-style-type: none"> <li><b>[0]</b> Disable</li> <li><b>[1]</b> Enable (default)</li> </ul>
<b>Admission Control Table</b>	
Web: Admission Control EMS: Call Admission Control <b>[SBCAdmissionControl]</b>	This table parameter defines limitations on the number of allowed concurrent calls (SIP dialogs). This is useful for controlling bandwidth utilization between Voice and Data traffic. The format of this parameter is as follows: <b>[SBCAdmissionControl]</b> FORMAT SBCAdmissionControl_Index = SBCAdmissionControl_LimitType, SBCAdmissionControl_IPGroupID, SBCAdmissionControl_SRDID, SBCAdmissionControl_RequestType, SBCAdmissionControl_RequestDirection, SBCAdmissionControl_Limit, SBCAdmissionControl_LimitPerUser, SBCAdmissionControl_Rate, SBCAdmissionControl_MaxBurst; <b>[SBCAdmissionControl]</b> For example, the below configuration allows a maximum of 10 concurrent SIP INVITEs for IP Group 1: SBCAdmissionControl 1 = 0, 1, -1, 1, 0, 10, -1, 0, 0; <b>Note:</b> For a detailed description of this table, see "Configuring Admission Control" on page 226.



Parameter	Description
<b>Allowed Audio Coders Table</b>	
Web: Allowed Audio Coders <b>[AllowedCodersGroup0]</b> <b>[AllowedCodersGroup1]</b> <b>[AllowedCodersGroup2]</b> <b>[AllowedCodersGroup3]</b> <b>[AllowedCodersGroup4]</b>	<p>This table parameter configures Allowed Coders Groups, which determines the coders that can be used for a specific SBC leg. Coders excluded from the Allowed Coders Group are removed from the SDP offer (only coders common between SDP offered coders and Allowed Coders are used). In addition, coders defined in top entries in the Allowed Coders Group are assigned higher priority than those entered in lower entries.</p> <p>[AllowedCodersGroupx]  FORMAT AllowedCodersGroup_Index =  AllowedCodersGroup_Name;  [AllowedCodersGroup]</p> <p>For example, below represents two configured Allowed Coders Groups. Group 0 has two coders; Group 1 has one coder. The highest priority coder is G.723.1.</p> <p>[ AllowedCodersGroup0 ]  FORMAT AllowedCodersGroup0_Index =  AllowedCodersGroup0_Name;  AllowedCodersGroup0 0 = g7231;  AllowedCodersGroup0 1 = g711Alaw64k;  [ \AllowedCodersGroup0 ]</p> <p>[ AllowedCodersGroup1 ]  FORMAT AllowedCodersGroup1_Index =  AllowedCodersGroup0_Name;  AllowedCodersGroup1 0 = g711Ulaw64k;  [ \AllowedCodersGroup1 ]</p> <p><b>Note:</b> For a detailed description of this table, see "Configuring Allowed Coder Groups" on page <a href="#">228</a>.</p>
<b>Classification Table</b>	
Web: Classification Table <b>[Classification]</b>	<p>This table parameter configures the Classification table. This table classifies incoming SIP dialogs to Source IP Groups. The format of this parameter is as follows:</p> <p>[ Classification ]  FORMAT Classification_Index =  Classification_MessageCondition, Classification_SrcSRDID,  Classification_SrcAddress, Classification_SrcPort,  Classification_SrcTransportType,  Classification_SrcUsernamePrefix, Classification_SrcHost,  Classification_DestUsernamePrefix, Classification_DestHost,  Classification_ActionType, Classification_SrcIPGroupID;  [ \Classification ]</p> <p>For example:  Classification 1 = 1, , 10.8.6.15, 5060, 2, *, *, *, *, 1, 4;</p> <p><b>Note:</b> For a detailed description of this table, see "Configuring Classification Rules" on page <a href="#">230</a>.</p>
<b>Condition Table</b>	



Parameter	Description
Web: Condition Table <b>[ConditionTable]</b>	<p>This table parameter configures Condition rules for SIP messages using the same syntax as used in the SIP Message Manipulation table. These Condition rules are later assigned to Classification rules in the Classification table for enhancing the process of classifying incoming SIP dialogs to an IP Groups.</p> <p>[ ConditionTable ]            FORMAT ConditionTable_Index = ConditionTable_Condition, ConditionTable_Description;            [ \ConditionTable ]</p> <p><b>Note:</b> For a detailed description of this table, see "Configuring Condition Rules" on page <a href="#">235</a>.</p>
<b>SBC IP-to-IP Routing Table</b>	
Web: IP-to-IP Routing Table <b>[IP2IPRouting]</b>	<p>This table parameter configures the SBC IP-to-IP Routing table for routing incoming SIP messages such as INVITE messages to an IP destination. The format of this parameter is as follows:</p> <p>[IP2IPRouting]            FORMAT IP2IPRouting_Index = IP2IPRouting_SrcIPGroupID, IP2IPRouting_SrcUsernamePrefix, IP2IPRouting_SrcHost, IP2IPRouting_DestUsernamePrefix, IP2IPRouting_DestHost, IP2IPRouting_RequestType, IP2IPRouting_MessageCondition, IP2IPRouting_ReRouteIPGroupID, IP2IPRouting_Trigger, IP2IPRouting_DestType, IP2IPRouting_DestIPGroupID, IP2IPRouting_DestSRDID, IP2IPRouting_DestAddress, IP2IPRouting_DestPort, IP2IPRouting_DestTransportType, IP2IPRouting_AltRouteOptions, IP2IPRouting_CostGroup;            [ \IP2IPRouting ]</p> <p>For example:            IP2IPRouting 1 = -1, *, *, *, *, 0, , -1, 0, 0, 1, , , 0, -1, 0,;</p> <p><b>Note:</b> For a detailed description of this table, see "Configuring SBC IP-to-IP R'outing" on page <a href="#">236</a>.</p>
<b>SBC Alternative Routing Reasons Table</b>	
Web: SBC Alternative Routing Reasons <b>[SBCAlternativeRoutingReasons]</b>	<p>This table parameter configures the SBC Alternative Routing Reasons table. This table is used for alternative IP-to-IP routing. If 4xx, 5xx, or 6xx SIP responses are received as a result of outgoing SIP dialog-initiating methods (e.g., INVITE, OPTIONS, and SUBSCRIBE messages), the device re-sends the messages to an alternative route if the response is defined in this table and if there are alternative routes configured in the IP-to-IP Routing table.</p> <p>The format of this parameter is as follows:</p> <p>[ SBCAlternativeRoutingReasons ]            FORMAT SBCAlternativeRoutingReasons_Index = SBCAlternativeRoutingReasons_ReleaseCause;            [ \SBCAlternativeRoutingReasons ]</p> <p>For example:            SBCAlternativeRoutingReasons 0 = 403;            SBCAlternativeRoutingReasons 1 = 404;</p> <p><b>Note:</b> For a detailed description of this table, see "Configuring Alternative Routing Reasons" on page <a href="#">243</a>.</p>
<b>IP to IP Inbound Manipulation Table</b>	



Parameter	Description
Web: IP to IP Inbound Manipulation <b>[IPInboundManipulation]</b>	<p>This table parameter configures the IP to IP Inbound Manipulation table. This table allows you to manipulate the SIP URI user part (source and/or destination) of the inbound SIP dialog message. The format of this parameter is as follows:</p> <p>[IPInboundManipulation]  FORMAT IPInboundManipulation_Index =  IPInboundManipulation_IsAdditionalManipulation,  IPInboundManipulation_ManipulatedURI,  IPInboundManipulation_ManipulationPurpose,  IPInboundManipulation_SrcIPGroupID,  IPInboundManipulation_SrcUsernamePrefix,  IPInboundManipulation_SrcHost,  IPInboundManipulation_DestUsernamePrefix,  IPInboundManipulation_DestHost,  IPInboundManipulation_RequestType,  IPInboundManipulation_RemoveFromLeft,  IPInboundManipulation_RemoveFromRight,  IPInboundManipulation_LeaveFromRight,  IPInboundManipulation_Prefix2Add,  IPInboundManipulation_Suffix2Add;  [IPInboundManipulation]</p> <p>For example:  IPInboundManipulation 1 = 0, 0, 0, -1, *, abc, *, *, 0, 0, 0, 255, , ;</p> <p><b>Note:</b> For a detailed description of this table, see "Configuring IP-to-IP Inbound Manipulations" on page <a href="#">246</a>.</p>
<b>IP to IP Outbound Manipulation Table</b>	
Web: IP to IP Outbound Manipulation <b>[IPOutboundManipulation]</b>	<p>This table parameter configures the IP to IP Outbound Manipulation table. This table allows you to manipulate the SIP URI user part (source and/or destination) of the outbound SIP dialog message. The format of this parameter is as follows:</p> <p>FORMAT IPOutboundManipulation_Index =  IPOutboundManipulation_IsAdditionalManipulation,  IPOutboundManipulation_SrcIPGroupID,  IPOutboundManipulation_DestIPGroupID,  IPOutboundManipulation_SrcUsernamePrefix,  IPOutboundManipulation_SrcHost,  IPOutboundManipulation_DestUsernamePrefix,  IPOutboundManipulation_DestHost,  IPOutboundManipulation_RequestType,  IPOutboundManipulation_ReRouteIPGroupID,  IPOutboundManipulation_Trigger,  IPOutboundManipulation_ManipulatedURI,  IPOutboundManipulation_RemoveFromLeft,  IPOutboundManipulation_RemoveFromRight,  IPOutboundManipulation_LeaveFromRight,  IPOutboundManipulation_Prefix2Add,  IPOutboundManipulation_Suffix2Add,  IPOutboundManipulation_PrivacyRestrictionMode;</p> <p>For example:  IPOutboundManipulation 1 = 0, 2, 4, "", "", "", "", 0, -1, 0, 0, 0, 0, 255, "", "", 0;</p> <p><b>Note:</b> For a detailed description of this table, see "Configuring IP-to-IP Outbound Manipulations" on page <a href="#">249</a>.</p>



## 42.14 Standalone Survivability Parameters

The Stand-alone Survivability (SAS) parameters are described in the table below.

**Table 42-36: SAS Parameters**

Parameter	Description
Web: Enable SAS <b>[EnableSAS]</b>	<p>Enables the Stand-Alone Survivability (SAS) feature.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul> <p>When enabled, the device receives the registration requests from different SIP entities in the local network and then forwards them to the defined proxy. If the connection to the proxy fails ('Emergency Mode'), the device serves as a proxy by allowing calls internal to the local network or outgoing to PSTN.</p> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
Web: SAS Local SIP UDP Port <b>[SASLocalSIPUDPPort]</b>	<p>Defines the local UDP port for sending and receiving SIP messages for SAS. The SIP entities in the local network need to send the registration requests to this port. When forwarding the requests to the proxy ('Normal Mode'), this port serves as the source port.</p> <p>The valid range is 1 to 65,534. The default is 5080.</p>
Web: SAS Default Gateway IP <b>[SASDefaultGatewayIP]</b>	<p>Defines the Default Gateway used in SAS 'Emergency Mode'. When an incoming SIP INVITE is received and the destination Address-Of-Record is not included in the SAS database, the request is immediately sent to this default gateway.</p> <p>The address can be configured as an IP address (dotted-decimal notation) or as a domain name (up to 49 characters). You can also configure the IP address with a destination port, e.g., "10.1.2.3:5060". The default is a null string, i.e., the local IP address of the gateway.</p>
Web: SAS Registration Time <b>[SASRegistrationTime]</b>	<p>Defines the value of the SIP Expires header that is sent in a 200 OK response to an incoming REGISTER message when in SAS 'Emergency Mode'.</p> <p>The valid range is 10 to 2,000,000. The default is 20.</p>
Web: SAS Local SIP TCP Port <b>[SASLocalSIPTCPPort]</b>	<p>Defines the local TCP port used to send/receive SIP messages for the SAS application. The SIP entities in the local network need to send the registration requests to this port. When forwarding the requests to the proxy ('Normal Mode'), this port serves as the source port.</p> <p>The valid range is 1 to 65,534. The default is 5080.</p>
Web: SAS Local SIP TLS Port <b>[SASLocalSIPTLSPort]</b>	<p>Defines the local TLS port used to send/receive SIP messages for the SAS application. The SIP entities in the local network need to send the registration requests to this port. When forwarding the requests to the proxy ('Normal Mode'), this port serves as the source port.</p> <p>The valid range is 1 to 65,534. The default is 5081.</p>
Web: SAS Connection Reuse <b>[SASConnectionReuse]</b>	<p>Enables the re-use of the same TCP connection for sessions with the same user in the SAS application.</p>



Parameter	Description
	<ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable</li> <li>▪ <b>[1]</b> Enable (default)</li> </ul> <p>The device can use the same TCP connection for multiple SIP requests / responses for a specific 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 the following:</p> <ul style="list-style-type: none"> <li>▪ User A sends a REGISTER message to SAS with transport=TCP.</li> <li>▪ User B sends an INVITE message to A using SAS.</li> </ul> <p>In this scenario, the SAS application forwards the INVITE request using the TCP connection that User A initially opened with the REGISTER message.</p>
Web: Enable Record-Route <b>[SASEnableRecordRoute]</b>	<p>Determines whether the device's SAS application adds the SIP Record-Route header to SIP requests. This ensures that SIP messages traverse the device's SAS agent by including the SAS IP address in the Record-Route header.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul> <p>The Record-Route header is inserted in a request by a SAS proxy to force future requests in the dialog session to be routed through the SAS agent. Each traversed proxy in the path can insert this header, causing all future dialogs in the session to pass through it as well.</p> <p>When this feature is enabled, the SIP Record-Route header includes the URI "lr" parameter, indicating loose routing, for example:</p> <pre>Record-Route: &lt;sip:server10.biloxi.com;lr&gt;</pre>
Web: SAS Proxy Set <b>[SASProxySet]</b>	<p>Defines the Proxy Set (index number) used in SAS Normal mode to forward REGISTER and INVITE requests from users that are served by the SAS application.</p> <p>The valid range is 0 to 5. The default is 0 (i.e., default Proxy Set).</p>
Web: Redundant SAS Proxy Set <b>[RedundantSASProxySet]</b>	<p>Defines the Proxy Set (index number) used in SAS Emergency mode for fallback when the user is not found in the Registered Users database. Each time a new SIP request arrives, the SAS application checks whether the user is listed in the registration database. If the user is located in the database, the request is sent to the user. If the user is not found, the request is forwarded to the next redundant SAS defined in the Redundant SAS Proxy Set. If that SAS Proxy IP appears in the Via header of the request, it is not forwarded (thereby, preventing loops in the request's course). If no such redundant SAS exists, the SAS sends the request to its default gateway (configured by the parameter SASDefaultGatewayIP).</p> <p>The valid range is -1 to 5. The default is -1 (i.e., no redundant Proxy Set).</p>
Web: SAS Block Unregistered Users <b>[SASBlockUnRegUsers]</b>	<p>Determines whether the device rejects SIP INVITE requests received from unregistered SAS users. This applies to SAS Normal and Emergency modes.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Un-Block = (Default) Allow INVITE from unregistered SAS users.</li> </ul>



Parameter	Description
	<ul style="list-style-type: none"> <li>▪ <b>[1]</b> Block = Reject dialog-establishment requests from un-registered SAS users.</li> </ul>
<b>[SASEnableContactReplace]</b>	<p>Enables the device to change the SIP Contact header so that it points to the SAS host and therefore, the top-most SIP Via header and the Contact header point to the same host.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> (default) = Disable - when relaying requests, the SAS agent adds a new Via header (with the SAS IP address) 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.</li> <li>▪ <b>[1]</b> = Enable - the device 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.</li> </ul> <p><b>Note:</b> Operating in this mode causes all incoming dialog requests to traverse the SAS, which may cause load problems.</p>
Web: SAS Survivability Mode <b>[SASSurvivabilityMode]</b>	<p>Determines the Survivability mode used by the SAS application.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Standard = (Default) Incoming INVITE and REGISTER requests are forwarded to the defined Proxy list of SASProxySet in Normal mode and handled by the SAS application in Emergency mode.</li> <li>▪ <b>[1]</b> Always Emergency = The SAS application does not use Keep-Alive messages towards the SASProxySet, instead it always operates in Emergency mode (as if no Proxy in the SASProxySet is available).</li> <li>▪ <b>[2]</b> Ignore Register = Use regular SAS Normal/Emergency logic (same as option <b>[0]</b>), but when in Normal mode incoming REGISTER requests are ignored.</li> <li>▪ <b>[3]</b> Auto-answer REGISTER = When in Normal mode, the device responds to received REGISTER requests by sending a SIP 200 OK (instead of relaying the registration requests to a Proxy), and enters the registrations in its SAS database.</li> <li>▪ <b>[4]</b> Use Routing Table only in Normal mode = The device uses the IP-to-IP Routing table to route IP-to-IP SAS calls only when in SAS Normal mode (and is unavailable when SAS is in Emergency mode). This allows routing of SAS IP-to-IP calls to different destinations (and not only to the SAS Proxy Set).</li> </ul>
Web: SAS Subscribe Response <b>[SASSubscribeResponse]</b>	<p>Defines the SIP response upon receipt of a SUBSCRIBE message when SAS is in Emergency mode. For example, if this parameter is set to "200", then SAS sends a SIP 200 OK in response to a SUBSCRIBE message, when in Emergency mode.</p> <p>The valid value is 200 to 699. The default is 489.</p>
Web: Enable ENUM <b>[SASEnableENUM]</b>	<p>Enables SAS to perform ENUM (E.164 number to URI mapping) queries when receiving INVITE messages in SAS emergency mode.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> Disable (default)</li> <li>▪ <b>[1]</b> Enable</li> </ul>
Web: SAS Binding Mode <b>[SASBindingMode]</b>	<p>Determines the SAS application database binding mode.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> URI = (Default) If the incoming AoR in the INVITE requests is using a 'tel:' URI or 'user=phone' is defined, the</li> </ul>



Parameter	Description
	<p>binding is performed according to the user part of the URI only. Otherwise, the binding is according to the entire URI, i.e., User@Host.</p> <ul style="list-style-type: none"> <li><b>[1]</b> User Part only = The binding is always performed according to the User Part only.</li> </ul>
Web: SAS Emergency Numbers <b>[SASEmergencyNumbers]</b>	<p>Defines emergency numbers for the device's SAS application. When the device's SAS agent receives a SIP INVITE (from an IP phone) that includes one of the emergency numbers (in the SIP user part), it forwards the INVITE to the default gateway (configured by the parameter SASDefaultGatewayIP), i.e., the device itself, which sends the call directly to the PSTN. This is important for routing emergency numbers such as 911 (in North America) directly to the PSTN. This is applicable to SAS operating in Normal and Emergency modes.</p> <p>Up to four emergency numbers can be defined, where each number can be up to four digits.</p>
<b>[SASEmergencyPrefix]</b>	<p>Defines a prefix that is added to the Request-URI user part of the INVITE message that is sent by the device's SAS agent when in Emergency mode to the default gateway or to any other destination (using the IP-to-IP Routing table). This parameter is required to differentiate between normal SAS calls routed to the default gateway and emergency SAS calls. Therefore, this allows you to define different manipulation rules for normal and emergency calls.</p> <p>This valid value is a character string. The default is an empty "" string.</p>
Web: SAS Entering Emergency Mode <b>[SASEnteringEmergencyMode]</b>	<p>Determines for which sent SIP message types the device enters SAS Emergency mode if no response is received for them from the proxy server.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) SAS enters Emergency mode only if no response is received from sent SIP OPTIONS messages.</li> <li><b>[1]</b> = SAS enters Emergency mode if no response is received from sent SIP OPTIONS, INVITE, or REGISTER messages.</li> </ul> <p><b>Note:</b> If the keep-alive mechanism is disabled for the Proxy Set (in the Proxy Set table) and this parameter is set to [1], SAS enters Emergency mode only if no response is received from sent INVITE or REGISTER messages.</p>
Web: SAS Inbound Manipulation Mode <b>[SASInboundManipulationMode]</b>	<p>Enables destination number manipulation of incoming INVITE messages when SAS is in Emergency mode. The manipulation rule is done in the IP to IP Inbound Manipulation table.</p> <ul style="list-style-type: none"> <li><b>[0]</b> None (default)</li> <li><b>[1]</b> Emergency Only</li> </ul> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>Inbound manipulation applies only to INVITE requests.</li> <li>For more information on SAS inbound manipulation, see "Manipulating Destination Number of Incoming INVITE" on page 274.</li> </ul>
<b>SAS Registration Manipulation Table</b>	
Web: SAS Registration Manipulation <b>[SASRegistrationManipulation]</b>	<p>This table parameter configures the SAS Registration Manipulation table. This table is used by the SAS application to manipulate the SIP Request-URI user part of incoming INVITE</p>



Parameter	Description
	<p>messages and of incoming REGISTER request AoR (To header), before saving it to the registered users database. The format of this table parameter is as follows:</p> <p>[SASRegistrationManipulation]            FORMAT SASRegistrationManipulation_Index =            SASRegistrationManipulation_RemoveFromRight,            SASRegistrationManipulation_LeaveFromRight;            [\SASRegistrationManipulation]</p> <p>For example, the manipulation rule below routes an INVITE with Request-URI header "sip:7184002@10.33.4.226" to user "4002@10.33.4.226" (i.e., keep only four digits from right of user part):</p> <pre>SASRegistrationManipulation 0 = 0, 4;</pre> <p><b>Note:</b> For a detailed description of this table, see 'Manipulating URI user part of Incoming REGISTER' on page <a href="#">273</a>.</p>
<b>Web: SAS IP-to-IP Routing Table</b>	
[IP2IPRouting]	<p>This table parameter configures the IP-to-IP Routing table for SAS routing rules. The format of this parameter is as follows:</p> <p>[IP2IPRouting]            FORMAT IP2IPRouting_Index = IP2IPRouting_SrcIPGroupID,            IP2IPRouting_SrcUsernamePrefix, IP2IPRouting_SrcHost,            IP2IPRouting_DestUsernamePrefix, IP2IPRouting_DestHost,            IP2IPRouting_DestType, IP2IPRouting_DestIPGroupID,            IP2IPRouting_DestSRDID, IP2IPRouting_DestAddress,            IP2IPRouting_DestPort, IP2IPRouting_DestTransportType,            IP2IPRouting_AltRouteOptions;            [\IP2IPRouting]</p> <p>For example:            IP2IPRouting 1 = -1, *, *, *, *, 0, -1, -1, , 0, -1, 0;</p> <p><b>Note:</b> For a detailed description of this table parameter, see "SAS Routing Based on IP-to-IP Routing Table" on page <a href="#">277</a>.</p>

## 42.15 IP Media Parameters

The IP media parameters are described in the table below.

**Table 42-37: IP Media Parameters**

Parameter	Description
Web: Number of Media Channels <b>[MediaChannels]</b>	<p>Defines the maximum number of DSP channels allocated for various functionalities).</p> <p>The default is 0.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>The SBC application does not require DSP channels. The SBC application uses DSP channels only if media transcoding is needed, where two DSP channels are used per transcoding session.</li> </ul>



## 42.16 Auxiliary and Configuration File Name Parameters

The configuration files (i.e., auxiliary files) can be loaded to the device using the Web interface. For loading these files using the *ini* file, you need to configure these files in the *ini* file and configured whether they must be stored in the non-volatile memory. The table below lists the *ini* file parameters associated with these auxiliary files. For more information on the auxiliary files, see "Loading Auxiliary Files" on page 311.

**Table 42-38: Auxiliary and Configuration File Parameters**

Parameter	Description
<b>General Parameters</b>	
<b>[SetDefaultOnIniFileProcess]</b>	<p>Determines if all the device's parameters are set to their defaults before processing the updated <i>ini</i> file.</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = Disable - parameters not included in the downloaded <i>ini</i> file are not returned to default settings (i.e., retain their current settings).</li> <li>▪ <b>[1]</b> = Enable (default).</li> </ul> <p><b>Note:</b> This parameter is applicable only for automatic HTTP update or Web <i>ini</i> file upload (not applicable if the <i>ini</i> file is loaded using BootP).</p>
<b>[SaveConfiguration]</b>	<p>Determines if the device's configuration (parameters and files) is saved to flash (non-volatile memory).</p> <ul style="list-style-type: none"> <li>▪ <b>[0]</b> = Configuration isn't saved to flash memory.</li> <li>▪ <b>[1]</b> = (Default) Configuration is saved to flash memory.</li> </ul>
<b>Auxiliary and Configuration File Name Parameters</b>	
Web: Call Progress Tones File <b>[CallProgressTonesFilename]</b>	<p>Defines the name of the file containing the Call Progress Tones definitions. For more information on how to create and load this file, refer to <i>DConvert Utility User's Guide</i>.</p> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
Web: Dial Plan File EMS: Dial Plan File Name <b>[DialPlanFileName]</b>	<p>Defines the name (and path) of the Dial Plan file. This file should be created using AudioCodes DConvert utility (refer to <i>DConvert Utility User's Guide</i>).</p>
<b>[UserInfoFileName]</b>	<p>Defines the name (and path) of the file containing the User Information data.</p>



## 42.17 Automatic Update Parameters

The automatic update of software and configuration files parameters are described in the table below.

**Table 42-39: Automatic Update of Software and Configuration Files Parameters**

Parameter	Description
<b>General Automatic Update Parameters</b>	
<b>[AutoUpdateCmpFile]</b>	<p>Enables the Automatic Update mechanism for the <i>cmp</i> file.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) The Automatic Update mechanism doesn't apply to the <i>cmp</i> file.</li> <li><b>[1]</b> = The Automatic Update mechanism includes the <i>cmp</i> file.</li> </ul> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
<b>[AutoUpdateFrequency]</b>	<p>Defines the number of minutes that the device waits between automatic updates. The default is 0 (i.e., the update at fixed intervals mechanism is disabled).</p> <p><b>Note:</b> For this parameter to take effect, a device reset is required.</p>
<b>[AutoUpdatePredefinedTime]</b>	<p>Defines schedules (time of day) for automatic updates. The format of this parameter is: 'HH:MM', where <i>HH</i> denotes the hour and <i>MM</i> the minutes, for example, 20:18.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>The actual update time is randomized by five minutes to reduce the load on the Web servers.</li> </ul>
EMS: AUPD Verify Certificates <b>[AUPDVerifyCertificates]</b>	<p>Determines whether the Automatic Update mechanism verifies server certificates when using HTTPS.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = Disable (default)</li> <li><b>[1]</b> = Enable</li> </ul>
<b>[AUPDCheckIfIniChanged]</b>	<p>Determines whether the Automatic Update mechanism performs CRC checking to determine if the <i>ini</i> file has changed prior to processing.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) Do not check CRC. The <i>ini</i> file is loaded whenever the server provides it.</li> <li><b>[1]</b> = Check CRC for the entire file. Any change, including line order, causes the <i>ini</i> file to be re-processed.</li> <li><b>[2]</b> = Check CRC for individual lines. Use this option when the HTTP server scrambles the order of lines in the provided <i>ini</i> file.</li> </ul>
<b>[ResetNow]</b>	<p>Invokes an immediate device reset. This option can be used to activate offline (i.e., not on-the-fly) parameters that are loaded using the parameter <i>IniFileUrl</i>.</p> <ul style="list-style-type: none"> <li><b>[0]</b> = (Default) The immediate restart mechanism is disabled.</li> <li><b>[1]</b> = The device immediately resets after an <i>ini</i> file with this parameter set to 1 is loaded.</li> </ul>
<b>Software/Configuration File URL Path for Automatic Update Parameters</b>	
<b>[CmpFileURL]</b>	<p>Defines the name of the <i>cmp</i> file and the path to the server (IP address or FQDN) from where the device can load the <i>cmp</i> file and update itself. The <i>cmp</i> file can be loaded using HTTP/HTTPS. For example: <code>http://192.168.0.1/filename</code></p>



Parameter	Description
	<b>Notes:</b> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>When this parameter is configured, the device always loads the <i>cmp</i> file after it is reset.</li> <li>The <i>cmp</i> file is validated before it's burned to flash. The checksum of the <i>cmp</i> file is also compared to the previously burnt checksum to avoid unnecessary resets.</li> <li>The maximum length of the URL address is 255 characters.</li> </ul>
[IniFileURL]	<p>Defines the name of the <i>ini</i> file and the path to the server (IP address or FQDN) on which it is located. The <i>ini</i> file can be loaded using HTTP/HTTPS.</p> <p>For example:  http://192.168.0.1/filename  http://192.8.77.13/config&lt;MAC&gt;  https://&lt;username&gt;:&lt;password&gt;@&lt;IP address&gt;/&lt;file name&gt;</p> <b>Notes:</b> <ul style="list-style-type: none"> <li>For this parameter to take effect, a device reset is required.</li> <li>When using HTTP or HTTPS, the date and time of the <i>ini</i> file are validated. Only more recently dated <i>ini</i> files are loaded.</li> <li>The optional string &lt;MAC&gt; is replaced with the device's MAC address. Therefore, the device requests an <i>ini</i> file name that contains its MAC address. This option allows the loading of specific configurations for specific devices.</li> <li>The maximum length of the URL address is 99 characters.</li> </ul>
[CptFileURL]	<p>Defines the name of the CPT file and the path to the server (IP address or FQDN) on which it is located.</p> <p>For example: http://server_name/file, https://server_name/file.</p> <b>Note:</b> The maximum length of the URL address is 99 characters.
[TLSTrustFileUrl]	<p>Defines the name of the TLS trusted root certificate file and the URL from where it can be downloaded.</p> <b>Note:</b> For this parameter to take effect, a device reset is required.
[TLSCertFileUrl]	<p>Defines the name of the TLS certificate file and the URL from where it can be downloaded.</p> <b>Note:</b> For this parameter to take effect, a device reset is required.
[TLSPkeyFileUrl]	<p>Defines the URL for downloading a TLS private key file using the Automatic Update facility.</p>
[UserInfoFileURL]	<p>Defines the name of the User Information file and the path to the server (IP address or FQDN) on which it is located.</p> <p>For example: http://server_name/file, https://server_name/file</p> <b>Note:</b> The maximum length of the URL address is 99 characters.



## 43 Specifications

The device's technical specifications are listed in the table below.



### Notes:

- All specifications in this document are subject to change without prior notice.
- The compliance and regulatory information can be downloaded from AudioCodes Web site at <http://www.audiocodes.com/library>.

**Table 43-1: Technical Specifications**

Function	Specification
<b>Capacity</b>	
<b>SBC Sessions</b>	<ul style="list-style-type: none"> <li>▪ RTP-RTP: 1,000</li> <li>▪ SRTP-RTP: 500</li> </ul>
<b>Registered Users (SBC, SAS)</b>	20,000
<b>Networking Interfaces</b>	
<b>LAN</b>	<ul style="list-style-type: none"> <li>▪ Up to 6 physical Gigabit Ethernet (1000Base-T) port interfaces.</li> <li>▪ Up to 3 groups of Ethernet port pairs, where each port-pair behaves as active-standby for 1+1 port redundancy. Up to 6 Ethernet port groups if each group is assigned only a single port.</li> <li>▪ Physical port separation by selecting port group per network interface</li> </ul>
<b>High Availability (HA)</b>	
<b>Full HA</b>	Two deployed devices for 1+1 high availability, communicating through a Maintenance network interface. Upon failure of the active device, all functionality is switched over to the redundant device
<b>Media Processing</b>	
<b>IP Transport</b>	VoIP (RTP/RTCP) per IETF RFC 3550 and 3551, IPv6
<b>Control and Management</b>	
<b>Control Protocols</b>	<ul style="list-style-type: none"> <li>▪ SIP-TCP, UDP, TLS and MSCML</li> <li>▪ Stand Alone Survivability (SAS) for service continuity</li> </ul>
<b>Operations &amp; Management</b>	<ul style="list-style-type: none"> <li>▪ Embedded HTTP Web Server, Telnet, SNMP V2/V3</li> <li>▪ Remote configuration and software download via TFTP, HTTP, HTTPS, DHCP</li> <li>▪ RADIUS, Syslog (for events, alarms and CDRs)</li> </ul>
<b>IP/VoIP Quality of Service</b>	
	<ul style="list-style-type: none"> <li>▪ IEEE 802.1p, TOS, DiffServ</li> <li>▪ IEEE 802.1Q VLAN tagging</li> <li>▪ Shaping, Policing, Queuing, Bandwidth Reservation</li> </ul>
<b>Stand Alone Survivability (SAS) Application</b>	
	SAS ensures call continuity between LAN SIP clients upon connectivity failure with IP Centrex services (e.g., WAN IP PBX).



Function	Specification
<b>Session Border Controller</b>	
	<ul style="list-style-type: none"> <li>▪ SIP Header conversion: IP to IP Routing translations of SIP, UDP, TCP, TLS.</li> <li>▪ Translation of RTP, SRTP; Support SIP trunk with multi-ITSP (Registrations to ITSPs is invoked independently); Topology hiding; Call Admission Control; Call Black/White list.</li> <li>▪ Intrusion detection/prevention (NIDS); Anti SPIT &amp; SPAM mechanisms.</li> </ul>
<b>Hardware Specifications</b>	
Recommended Platform	<ul style="list-style-type: none"> <li>▪ Server Edition - x86 server based platform: <ul style="list-style-type: none"> <li>✓ Platform: HP ProLiant DL120 G7 or HP ProLiant DL320e G8</li> <li>✓ Processor: Intel Xeon E3-1220 or E3-1220v2 (4 cores, 3.1 GHz, 8M Cache) Intel Xeon E3-1220 (8M Cache, 3.10 GHz), 4 Cores</li> <li>✓ Memory: 4 GB</li> <li>✓ Disk space: 72 GB or more</li> <li>✓ Installation from CD/DVD drive</li> <li>✓ Installation interface: VGA Monitor and Keyboard</li> </ul> </li> <li>▪ Virtual Edition - installed and hosted in a virtual machine environment: <ul style="list-style-type: none"> <li>✓ Host OS: VMware ESXi version 5.0 or later</li> <li>✓ Processor: 2 Cores or more.</li> <li>✓ Memory: 4 GB or more</li> <li>✓ Disk space: 60 GB or more</li> <li>✓ Network: At least two virtual networks preconfigured</li> </ul> </li> </ul>



## Reader's Notes





## User's Manual Ver. 6.6