

User's Manual

AudioCodes Mediant™ Family of Session Border Controllers

Mediant Software SBC

Virtual Edition (VE) & Server Edition (SE)

Version 7.2



Table of Contents

1	Introduction	21
1.1	Product Overview	21
1.2	Typographical Conventions.....	21
1.3	Getting Familiar with Configuration Concepts and Terminology	22
1.3.1	SBC Application.....	22
Getting Started with Initial Connectivity.....		27
2	Introduction	29
3	Default OAMP IP Address.....	31
4	Installing the Software	33
5	Changing Default IP Address to Suit your Network Addressing Scheme....	35
6	Licensing the Device.....	37
Management Tools		39
7	Introduction	41
8	Web-Based Management.....	43
8.1	Getting Acquainted with the Web Interface.....	43
8.1.1	Computer Requirements.....	43
8.1.2	Accessing the Web Interface.....	44
8.1.3	Areas of the GUI	45
8.1.4	Accessing Configuration Pages from Navigation Tree.....	47
8.1.5	Configuring Stand-alone Parameters	49
8.1.6	Configuring Table Parameters.....	50
8.1.6.1	Adding Table Rows	51
8.1.6.2	Modifying Table Rows.....	52
8.1.6.3	Deleting Table Rows	53
8.1.6.4	Invalid Value Indications	53
8.1.6.5	Viewing Table Rows.....	55
8.1.6.6	Sorting Tables by Column.....	55
8.1.6.7	Changing Index Position of Table Rows	56
8.1.6.8	Searching Table Entries.....	57
8.1.7	Searching for Configuration Parameters	57
8.1.8	Creating a Login Welcome Message.....	59
8.1.9	Getting Help.....	59
8.1.10	Logging Off the Web Interface.....	60
8.2	Configuring Management User Accounts	60
8.3	Displaying Login Information upon Login	64
8.4	Viewing Logged-In User Information.....	65
8.5	Configuring Web Session and Access Settings	66
8.6	Changing Login Password for Administrator and Monitor Users	67
8.7	Configuring Secured (HTTPS) Web.....	68
8.8	Web Login Authentication using Smart Cards	68
8.9	Configuring Web and Telnet Access List	69

9	CLI-Based Management.....	71
9.1	Getting Familiar with CLI.....	71
9.1.1	Understanding Configuration Modes.....	71
9.1.2	Using CLI Shortcuts.....	72
9.1.3	Common CLI Commands.....	73
9.1.4	Configuring Tables through CLI.....	74
9.1.5	Understanding CLI Error Messages.....	75
9.2	Enabling CLI.....	76
9.2.1	Enabling Telnet for CLI.....	76
9.2.2	Enabling SSH with RSA Public Key for CLI.....	76
9.3	Configuring Maximum Telnet/SSH Sessions.....	78
9.4	Establishing a CLI Session.....	79
9.5	Viewing Current CLI Sessions.....	80
9.6	Terminating a User's CLI Session.....	80
9.7	Configuring Displayed Output Lines in CLI Terminal Window.....	80
10	SNMP-Based Management.....	83
10.1	Enabling SNMP.....	83
10.2	Configuring SNMP Community Strings.....	83
10.3	Configuring SNMP Trap Destinations with IP Addresses.....	85
10.4	Configuring an SNMP Trap Destination with FQDN.....	87
10.5	Configuring SNMP Trusted Managers.....	87
10.6	Enabling SNMP Traps for Web Activity.....	88
10.7	Configuring SNMP V3 Users.....	88
11	INI File-Based Management.....	91
11.1	INI File Format.....	91
11.1.1	Configuring Individual ini File Parameters.....	91
11.1.2	Configuring Table ini File Parameters.....	91
11.1.3	General ini File Formatting Rules.....	93
11.2	Configuring an ini File.....	93
11.3	Loading an ini File to the Device.....	94
11.4	Secured Encoded ini File.....	94
11.5	Configuring Password Display in ini File.....	94
11.6	INI Viewer and Editor Utility.....	96
General System Settings.....		97
12	Configuring SSL/TLS Certificates.....	99
12.1	Configuring TLS Certificate Contexts.....	99
12.2	Assigning CSR-based Certificates to TLS Contexts.....	103
12.3	Viewing Certificate Information.....	105
12.4	Assigning Externally Created Private Keys to TLS Contexts.....	106
12.5	Generating Private Keys for TLS Contexts.....	107
12.6	Creating Self-Signed Certificates for TLS Contexts.....	109
12.7	Importing Certificates and Certificate Chain into Trusted Certificate Store.....	110
12.8	Configuring Mutual TLS Authentication.....	111
12.8.1	TLS for SIP Clients.....	111

12.8.2	TLS for Remote Device Management	112
12.9	Configuring TLS Server Certificate Expiry Check	114
13	Date and Time.....	115
13.1	Configuring Automatic Date and Time using SNTP	115
13.2	Configuring Date and Time Manually	116
13.3	Configuring the Time Zone.....	116
13.4	Configuring Daylight Saving Time.....	117
General VoIP Configuration.....		119
14	Network.....	121
14.1	Building and Viewing your Network Topology.....	121
14.2	Configuring Physical Ethernet Ports	124
14.3	Configuring Ethernet Port Groups.....	126
14.4	Configuring Underlying Ethernet Devices	128
14.5	Configuring IP Network Interfaces	130
14.5.1	Assigning NTP Services to Application Types	134
14.5.2	IP Interfaces Table Configuration Guidelines.....	134
14.5.3	Networking Configuration Examples	135
14.5.3.1	One VoIP Interface for All Applications.....	135
14.5.3.2	VoIP Interface per Application Type.....	136
14.5.3.3	VoIP Interfaces for Combined Application Types	136
14.5.3.4	VoIP Interfaces with Multiple Default Gateways	137
14.6	Configuring Static IP Routes	138
14.6.1	Configuration Example of Static IP Routes	139
14.6.2	Troubleshooting the Static Routes Table	140
14.7	Network Address Translation Support	141
14.7.1	Device Located behind NAT.....	141
14.7.1.1	Configuring NAT Translation per IP Interface	142
14.7.2	Remote UA behind NAT	144
14.7.2.1	SIP Signaling Messages	144
14.7.2.2	Media (RTP/RTCP/T.38).....	144
14.8	Configuring Quality of Service.....	148
14.8.1	Configuring Class-of-Service QoS.....	148
14.8.2	Configuring DiffServ-to-VLAN Priority Mapping.....	150
14.9	Configuring ICMP Messages	151
14.10	DNS.....	152
14.10.1	Configuring the Internal DNS Table.....	152
14.10.2	Configuring the Internal SRV Table.....	153
14.11	Robust Receipt of Media Streams by Media Latching	155
14.12	Multiple Routers Support.....	156
15	Security.....	157
15.1	Configuring Firewall Settings	157
15.2	Configuring TLS for SIP	162
15.3	Intrusion Detection System	163
15.3.1	Enabling IDS.....	164
15.3.2	Configuring IDS Policies.....	164
15.3.3	Assigning IDS Policies.....	168

15.3.4	Viewing IDS Alarms	170
16	Media	173
16.1	Configuring Voice Settings	173
16.1.1	Configuring Voice Gain (Volume) Control	173
16.1.2	Silence Suppression (Compression)	173
16.1.3	Configuring Echo Cancellation	173
16.2	Fax and Modem Capabilities	175
16.2.1	Fax/Modem Operating Modes	176
16.2.2	Fax/Modem Transport Modes	176
16.2.2.1	T.38 Fax Relay Mode	176
16.2.2.2	G.711 Fax / Modem Transport Mode	179
16.2.2.3	Fax Fallback	179
16.2.2.4	Fax/Modem Bypass Mode	180
16.2.2.5	Fax / Modem NSE Mode	181
16.2.2.6	Fax / Modem Transparent with Events Mode	182
16.2.2.7	Fax / Modem Transparent Mode	182
16.2.2.8	RFC 2833 ANS Report upon Fax/Modem Detection	183
16.2.3	V.34 Fax Support	184
16.2.3.1	Bypass Mechanism for V.34 Fax Transmission	184
16.2.3.2	Relay Mode for T.30 and V.34 Faxes	184
16.2.4	V.152 Support	185
16.3	Configuring RTP/RTCP Settings	185
16.3.1	Configuring the Dynamic Jitter Buffer	186
16.3.2	Configuring RFC 2833 Payload	187
16.3.3	Configuring RTP Base UDP Port	187
16.4	Event Detection and Notification using X-Detect Header	188
16.4.1	Detecting Answering Machine Beeps	189
16.4.2	SIP Call Flow Examples of Event Detection and Notification	190
16.5	Answering Machine Detection (AMD)	192
16.5.1	Configuring AMD	195
16.6	Automatic Gain Control (AGC)	195
16.7	Configuring Media (SRTP) Security	196
16.7.1	SRTP using DTLS Protocol	199
17	Services	201
17.1	DHCP Server Functionality	201
17.1.1	Configuring the DHCP Server	201
17.1.2	Configuring the Vendor Class Identifier	206
17.1.3	Configuring Additional DHCP Options	207
17.1.4	Configuring Static IP Addresses for DHCP Clients	209
17.1.5	Viewing and Deleting DHCP Clients	210
17.2	SIP-based Media Recording	211
17.2.1	Enabling SIP-based Media Recording	215
17.2.2	Configuring SIP Recording Rules	215
17.2.3	Configuring SIP User Part for SRS	217
17.2.4	Interworking SIP-based Media Recording with Third-Party Vendors	217
17.2.4.1	Genesys	217
17.2.4.2	Avaya UCID	218
17.3	RADIUS-based Services	218
17.3.1	Enabling RADIUS Services	218
17.3.2	Configuring RADIUS Servers	219
17.3.3	Configuring Interface for RADIUS Communication	221
17.3.4	Configuring RADIUS Packet Retransmission	221

17.3.5	Configuring the RADIUS Vendor ID	222
17.3.6	RADIUS-based Management User Authentication	222
17.3.6.1	Setting Up a Third-Party RADIUS Server	223
17.3.6.2	Configuring RADIUS-based User Authentication.....	224
17.3.6.3	Securing RADIUS Communication	226
17.3.6.4	RADIUS-based User Authentication in URL	226
17.3.7	RADIUS-based CDR Accounting	226
17.4	LDAP-based Management and SIP Services	226
17.4.1	Enabling the LDAP Service	228
17.4.2	Enabling LDAP-based Web/CLI User Login Authentication....	228
17.4.3	Configuring LDAP Server Groups	228
17.4.4	Configuring LDAP Servers.....	231
17.4.5	Configuring LDAP DN's (Base Paths) per LDAP Server.....	234
17.4.6	Configuring the LDAP Search Filter Attribute	235
17.4.7	Configuring Access Level per Management Groups Attributes	236
17.4.8	Configuring the Device's LDAP Cache.....	238
17.4.8.1	Refreshing the LDAP Cache	240
17.4.8.2	Clearing the LDAP Cache	242
17.4.9	Configuring Local Database for Management User Authentication	242
17.4.10	LDAP-based Login Authentication Example.....	243
17.4.11	Enabling LDAP Searches for Numbers with Characters	248
17.4.12	AD-based Routing for Microsoft Skype for Business	248
17.4.12.1	Querying the AD and Routing Priority	249
17.4.12.2	Configuring AD-Based Routing Rules.....	252
17.5	Least Cost Routing.....	254
17.5.1	Overview	254
17.5.2	Configuring LCR	256
17.5.2.1	Configuring Cost Groups.....	256
17.5.2.2	Assigning Cost Groups to Routing Rules.....	259
17.6	Remote Web Services	259
17.6.1	Configuring Remote Web Services	259
17.6.1.1	Configuring Remote HTTP Hosts.....	263
17.6.2	Enabling Topology Status Services.....	265
17.6.3	Centralized Third-Party Routing Server.....	266
17.7	HTTP-based Proxy Services.....	268
17.7.1	Enabling the HTTP Proxy Application	269
17.7.2	Configuring HTTP Interfaces	270
17.7.3	Configuring HTTP Proxy Services.....	272
17.7.3.1	Configuring HTTP Proxy Hosts	273
17.7.4	Configuring an HTTP-based EMS Service	275
17.8	E9-1-1 Support for Microsoft Skype for Business	277
17.8.1	About E9-1-1 Services.....	277
17.8.2	Microsoft Skype for Business and E9-1-1	278
17.8.2.1	Gathering Location Information of Skype for Business Clients for 911 Calls	278
17.8.2.2	Adding ELINs to the Location Information Server.....	280
17.8.2.3	Passing Location Information to the PSTN Emergency Provider	281
17.8.3	AudioCodes ELIN Device for Skype for Business E9-1-1 Calls to PSTN	282
17.8.3.1	Detecting and Handling E9-1-1 Calls.....	283
17.8.3.2	Pre-empting Existing Calls for E9-1-1 Calls.....	285
17.8.3.3	PSAP Callback to Skype for Business Clients for Dropped E9-1-1 Calls	285
17.8.3.4	Selecting ELIN for Multiple Calls within Same ERL.....	286
17.8.4	Configuring AudioCodes ELIN Device.....	286
17.8.4.1	Enabling the E9-1-1 Feature	287

17.8.4.2	Configuring the E9-1-1 Callback Timeout	287
17.8.4.3	Configuring SBC IP-to-IP Routing Rule for E9-1-1	287
17.8.4.4	Viewing the ELIN Table	288
18	Quality of Experience.....	289
18.1	Reporting Voice Quality of Experience to SEM.....	289
18.1.1	Configuring the SEM Server	289
18.1.2	Configuring Clock Synchronization between Device and SEM	290
18.1.3	Enabling RTCP XR Reporting to SEM	290
18.2	Configuring Quality of Experience Profiles.....	291
18.3	Configuring Bandwidth Profiles	296
18.4	Configuring Quality of Service Rules	300
19	Control Network	303
19.1	Configuring Media Realms.....	303
19.1.1	Configuring Remote Media Subnets.....	306
19.1.2	Configuring Media Realm Extensions	309
19.2	Configuring SRDs	311
19.2.1	Filtering Tables in Web Interface by SRD	317
19.2.2	Multiple SRDs for Multi-tenant Deployments.....	317
19.2.3	Cloning SRDs	320
19.2.4	Color-Coding of SRDs in Web Interface.....	321
19.2.5	Automatic Configuration based on SRD.....	321
19.3	Configuring SIP Interfaces	321
19.4	Configuring IP Groups.....	329
19.5	Configuring Proxy Sets	341
19.6	Building and Viewing SIP Entities in Topology View.....	350
20	SIP Definitions.....	355
20.1	Configuring Registration Accounts.....	355
20.1.1	Regular Registration Mode.....	358
20.1.2	Single Registration for Multiple Phone Numbers using GIN.....	358
20.2	Configuring Proxy and Registration Parameters.....	359
20.2.1	SIP Message Authentication Example	360
20.3	Configuring SIP Message Manipulation	362
20.4	Configuring SIP Message Policy Rules.....	367
20.5	Configuring Call Setup Rules.....	370
20.5.1	Call Setup Rule Examples	375
21	Coders and Profiles	379
21.1	Configuring Coder Groups	379
21.1.1	Supported Audio Coders	382
21.1.2	Configuring Various Codec Attributes	383
21.2	Configuring Allowed Audio Coder Groups	384
21.3	Configuring Allowed Video Coder Groups	387
21.4	Configuring IP Profiles	388
Session Border Controller Application.....		419

22 SBC Overview	421
22.1 Feature List	421
22.2 B2BUA and Stateful Proxy Operating Modes	422
22.3 Call Processing of SIP Dialog Requests	425
22.4 User Registration	427
22.4.1 Initial Registration Request Processing	427
22.4.2 Classification and Routing of Registered Users	428
22.4.3 General Registration Request Processing	429
22.4.4 Registration Refreshes	429
22.4.5 Registration Restriction Control	430
22.4.6 Deleting Registered Users	430
22.5 Media Handling	430
22.5.1 Media Anchoring	431
22.5.2 Direct Media	432
22.5.3 Restricting Audio Coders	434
22.5.4 Coder Transcoding	435
22.5.5 Transcoding Mode	438
22.5.6 Prioritizing Coder List in SDP Offer	438
22.5.7 SRTP-RTP and SRTP-SRTP Transcoding	439
22.5.8 Multiple RTP Media Streams per Call Session	439
22.5.9 Interworking Miscellaneous Media Handling	440
22.5.9.1 Interworking DTMF Methods	440
22.5.9.2 Interworking RTP Redundancy	440
22.5.9.3 Interworking RTP-RTCP Multiplexing	440
22.5.9.4 Interworking RTCP Attribute in SDP	440
22.5.9.5 Interworking Crypto Lifetime Field	441
22.5.9.6 Interworking Media Security Protocols	441
22.5.9.7 Interworking ICE Lite for NAT Traversal	441
22.6 Fax Negotiation and Transcoding	441
22.7 Limiting SBC Call Duration	442
22.8 SBC Authentication	442
22.8.1 SIP Authentication Server Functionality	442
22.8.2 User Authentication based on RADIUS	443
22.9 Interworking SIP Signaling	443
22.9.1 Interworking SIP 3xx Redirect Responses	444
22.9.1.1 Resultant INVITE Traversing Device	444
22.9.1.2 Local Handling of SIP 3xx	445
22.9.2 Interworking SIP Diversion and History-Info Headers	446
22.9.3 Interworking SIP REFER Messages	446
22.9.4 Interworking SIP PRACK Messages	447
22.9.5 Interworking SIP Session Timer	447
22.9.6 Interworking SIP Early Media	447
22.9.7 Interworking SIP re-INVITE Messages	450
22.9.8 Interworking SIP UPDATE Messages	450
22.9.9 Interworking SIP re-INVITE to UPDATE	451
22.9.10 Interworking Delayed Offer	451
22.9.11 Interworking Call Hold	451
22.9.12 Interworking SIP Via Headers	451
22.9.13 Interworking SIP User-Agent Headers	452
22.9.14 Interworking SIP Record-Route Headers	452
22.9.15 Interworking SIP To-Header Tags in Multiple SDP Answers	452
22.9.16 Interworking In-dialog SIP Contact and Record-Route Headers	452

23	Enabling the SBC Application.....	453
24	Configuring General SBC Settings	455
24.1	Interworking Dialog Information in SIP NOTIFY Messages	455
25	Configuring Admission Control.....	457
26	Routing SBC	461
26.1	Configuring Classification Rules	461
26.1.1	Classification Based on URI of Selected Header Example.....	468
26.2	Configuring Message Condition Rules.....	469
26.3	Configuring SBC IP-to-IP Routing.....	470
26.4	Configuring SIP Response Codes for Alternative Routing Reasons.....	482
26.5	Configuring SBC Routing Policy Rules	484
26.6	Configuring IP Group Sets	487
27	SBC Manipulations.....	491
27.1	Configuring IP-to-IP Inbound Manipulations	493
27.2	Configuring IP-to-IP Outbound Manipulations.....	497
28	Configuring Dial Plans.....	503
28.1	Importing and Exporting Dial Plans.....	507
28.2	Creating Dial Plan Files.....	510
28.3	Using Dial Plan Tags for IP-to-IP Routing.....	511
28.3.1	Dial Plan Backward Compatibility.....	512
28.4	Using Dial Plan Tags for Outbound Manipulation	514
28.5	Using Dial Plan Tags for Call Setup Rules.....	515
28.6	Using Dial Plan Tags for Message Manipulation	516
29	Configuring Malicious Signatures	517
30	Advanced SBC Features.....	519
30.1	Configuring Call Preemption for SBC Emergency Calls	519
30.2	Emergency Call Routing using LDAP to Obtain ELIN.....	520
30.3	Enabling Interworking of SIP and SIP-I Endpoints.....	522
30.4	WebRTC	524
30.4.1	SIP over WebSocket.....	526
30.4.2	Configuring WebRTC.....	528
30.5	Call Forking	531
30.5.1	Initiating SIP Call Forking	531
30.5.2	Configuring SIP Forking Initiated by SIP Proxy	531
30.5.3	Configuring Call Forking-based IP-to-IP Routing Rules	532
30.6	Call Survivability.....	532
30.6.1	Enabling Auto-Provisioning of Subscriber-Specific Information of BroadWorks Server for Survivability.....	532
30.6.2	Configuring BroadSoft's Shared Phone Line Call Appearance for Survivability	533
30.6.3	Configuring Call Survivability for Call Centers.....	535
30.6.4	Enabling Survivability Display on Aastra IP Phones	537
30.7	Alternative Routing on Detection of Failed SIP Response.....	538
30.8	VolPerfect	538

Cloud Resilience Package	543
31 CRP Overview	545
32 CRP Configuration	547
32.1 Enabling the CRP Application	547
32.2 Configuring Call Survivability Mode	547
32.3 Pre-Configured IP Groups.....	549
32.4 Pre-Configured IP-to-IP Routing Rules	550
32.4.1 Normal Mode	550
32.4.2 Emergency Mode.....	551
32.4.3 Auto Answer to Registrations	551
32.5 Configuring PSTN Fallback.....	552
High Availability System	553
33 HA Overview	555
33.1 Connectivity and Synchronization between Devices.....	556
33.2 Device Switchover upon Failure.....	557
33.3 Viewing HA Status on Monitor Web Page.....	558
34 HA Configuration.....	561
34.1 Initial HA Configuration	561
34.1.1 Network Topology Types and Rx/Tx Ethernet Port Group Settings.....	561
34.1.2 Configuring the HA Devices	563
34.1.2.1 Step 1: Configure the First Device	563
34.1.2.2 Step 2: Configure the Second Device	565
34.1.2.3 Step 3: Initialize HA on the Devices	566
34.2 Configuration while HA is Operational	566
34.3 Configuring Firewall Allowed Rules.....	567
34.4 Monitoring IP Entity and HA Switchover upon Ping Failure	568
35 HA Maintenance	571
35.1 Maintenance of Redundant Device	571
35.2 Replacing a Failed Device	571
35.3 Initiating an HA Switchover	571
35.4 Resetting the Redundant Unit	572
35.5 Software Upgrade	572
35.6 Rescue Options.....	573
35.6.1 Taking a Snapshot.....	573
35.6.2 Viewing Available Snapshots	573
35.6.3 Changing the Default Snapshot.....	574
35.6.4 Deleting a Snapshot	574
35.6.5 Manual Recovery.....	574
35.6.5.1 Returning to the Default Snapshot	574
35.6.5.2 Fixing the Current Installation	575
35.6.5.3 Returning to an Arbitrary Snapshot.....	575
35.6.5.4 Returning to a Factory Snapshot	575
35.6.6 Automatic Recovery.....	576

Maintenance	577
36 Basic Maintenance	579
36.1 Resetting the Device	579
36.2 Remotely Resetting Device using SIP NOTIFY	580
36.3 Locking and Unlocking the Device	581
36.4 Saving Configuration.....	582
37 Channel Maintenance	583
37.1 Disconnecting Active Calls.....	583
38 Software Upgrade	585
38.1 Auxiliary Files	585
38.1.1 Loading Auxiliary Files.....	585
38.1.1.1 Loading Auxiliary Files through Web Interface	586
38.1.1.2 Loading Auxiliary Files through CLI	587
38.1.2 Deleting Auxiliary Files	587
38.1.3 Call Progress Tones File	587
38.1.4 Prerecorded Tones File	590
38.1.5 Dial Plan File.....	591
38.1.5.1 Creating a Dial Plan File.....	591
38.1.5.2 Obtaining IP Destination from Dial Plan File	592
38.1.5.3 Viewing Information of Installed Dial Plan File	592
38.1.6 User Information File	593
38.1.6.1 Enabling the User Info Table.....	593
38.1.6.2 User Information File for SBC User Database	593
38.1.6.3 Viewing the Installed User Info File Name	597
38.1.7 AMD Sensitivity File.....	597
38.2 License Key.....	597
38.2.1 Viewing the License Key.....	598
38.2.2 Entering the Product Key.....	598
38.2.3 Obtaining License Key for Initial Activation	599
38.2.4 Obtaining License Key for Feature Upgrade	599
38.2.5 Installing the License Key	600
38.2.5.1 Installing License Key through Web Interface.....	600
38.2.5.2 Installing License Key through CLI.....	602
38.3 Upgrading SBC Capacity Licenses by License Pool Manager Server.....	602
38.4 Software Upgrade Wizard	604
38.4.1 Post-Upgrade from Version 7.0 Procedure	610
39 Backing Up and Loading Configuration File	613
40 Automatic Provisioning	615
40.1 Automatic Configuration Methods	615
40.1.1 DHCP-based Provisioning.....	615
40.1.2 HTTP-based Provisioning.....	616
40.1.3 FTP-based Provisioning	617
40.1.4 Provisioning using AudioCodes EMS	617
40.2 HTTP/S-Based Provisioning using the Automatic Update Feature	617
40.2.1 Files Provisioned by Automatic Update.....	618
40.2.2 File Location for Automatic Update	618
40.2.3 MAC Address Placeholder in Configuration File Name.....	619
40.2.4 File Template for Automatic Provisioning.....	620
40.2.5 Triggers for Automatic Update.....	621

40.2.6	Access Authentication with HTTP Server.....	622
40.2.7	Querying Provisioning Server for Updated Files	622
40.2.8	File Download Sequence.....	625
40.2.9	Cyclic Redundancy Check on Downloaded Configuration Files	626
40.2.10	Automatic Update Configuration Examples.....	626
40.2.10.1	Automatic Update for Single Device	627
40.2.10.2	Automatic Update from Remote Servers	628
40.2.10.3	Automatic Update for Mass Deployment.....	629
41	Restoring Factory Defaults	633
41.1	Restoring Factory Defaults through CLI.....	633
41.2	Restoring Factory Defaults through Web Interface	633
41.3	Restoring Defaults through ini File	634
Status, Performance Monitoring and Reporting		635
42	System Status	637
42.1	Viewing Device Information.....	637
42.2	Viewing Device Status on Monitor Page	637
43	Reporting DSP Utilization through SNMP MIB.....	641
44	Viewing Carrier-Grade Alarms	643
44.1	Viewing Active Alarms.....	643
44.2	Viewing History Alarms	644
45	Viewing Management User Activity Logs	647
46	Viewing Performance Monitoring	649
46.1	Viewing Call Success and Failure Ratio	649
46.2	Viewing Average Call Duration	650
46.3	Configuring Performance Profiles	651
47	Viewing VoIP Status.....	657
47.1	Viewing SBC Registered Users	657
47.2	Viewing Call Routing Status.....	658
47.3	Viewing Registration Status	658
47.4	Viewing CDR Test Calls.....	659
47.5	Viewing SBC CDR History	660
48	Viewing Network Status.....	663
48.1	Viewing Active IP Interfaces.....	663
48.2	Viewing Ethernet Device Status.....	663
48.3	Viewing Ethernet Port Information	663
48.4	Viewing Static Routes Status	664
49	Reporting Information to External Party	665
49.1	Configuring RTCP XR	665
49.2	Generating Call Detail Records.....	669
49.2.1	CDR Field Description	670
49.2.1.1	CDR Fields for SBC Signaling	670

49.2.1.2	CDR Fields for SBC Media	675
49.2.1.3	CDR Fields for SBC Local Storage	677
49.2.2	Customizing CDRs for SBC Calls.....	678
49.2.3	Configuring CDR Reporting	682
49.2.4	Storing CDRs on the Device.....	683
49.3	Configuring RADIUS Accounting	685
Diagnosics		691
50	Syslog and Debug Recording	693
50.1	Configuring Log Filter Rules.....	693
50.1.1	Filtering IP Network Traces	697
50.2	Configuring Syslog.....	698
50.2.1	Syslog Message Format.....	698
50.2.1.1	Event Representation in Syslog Messages	700
50.2.1.2	Identifying AudioCodes Syslog Messages using Facility Levels	702
50.2.1.3	Syslog Fields for Answering Machine Detection (AMD)	702
50.2.1.4	SNMP Alarms in Syslog Messages.....	703
50.2.2	Enabling Syslog	703
50.2.3	Configuring the Syslog Server Address.....	703
50.2.4	Configuring Syslog Debug Level	704
50.2.5	Configuring Reporting of Management User Activities.....	705
50.2.6	Viewing Syslog Messages	706
50.3	Configuring Debug Recording.....	707
50.3.1	Configuring the Debug Recording Server Address	708
50.3.2	Collecting Debug Recording Messages	708
50.3.3	Debug Capturing on Physical VoIP Interfaces	709
51	Creating Core Dump and Debug Files upon Device Crash	711
52	Testing SIP Signaling Calls	713
52.1	Configuring Test Call Endpoints.....	713
52.2	Starting and Stopping Test Calls.....	717
52.3	Viewing Test Call Status	718
52.4	Viewing Test Call Statistics	718
52.5	Configuring DTMF Tones for Test Calls.....	720
52.6	Configuring SBC Test Call with External Proxy	721
52.7	Test Call Configuration Examples.....	722
53	Pinging a Remote Host or IP Address.....	725
Appendix		727
54	Dialing Plan Notation for Routing and Manipulation.....	729
55	Configuration Parameters Reference	733
55.1	Management Parameters.....	733
55.1.1	General Parameters	733
55.1.2	Web Parameters.....	734
55.1.3	Telnet Parameters	737
55.1.4	ini File Parameters.....	737
55.1.5	SNMP Parameters.....	738
55.1.6	Serial Parameters	741

55.1.7	Auxiliary and Configuration File Name Parameters	742
55.1.8	Automatic Update Parameters	743
55.2	Networking Parameters.....	747
55.2.1	Ethernet Parameters.....	747
55.2.2	Multiple VoIP Network Interfaces and VLAN Parameters	748
55.2.3	Routing Parameters.....	749
55.2.4	Quality of Service Parameters.....	750
55.2.5	NAT Parameters	751
55.2.6	DNS Parameters.....	752
55.2.7	DHCP Parameters	753
55.2.8	NTP and Daylight Saving Time Parameters.....	755
55.3	Debugging and Diagnostics Parameters.....	756
55.3.1	General Parameters	756
55.3.2	SIP Test Call Parameters	757
55.3.3	Syslog, CDR and Debug Parameters.....	758
55.3.4	Resource Allocation Indication Parameters.....	763
55.4	HA Parameters.....	764
55.5	Security Parameters.....	766
55.5.1	General Security Parameters	766
55.5.2	HTTPS Parameters	768
55.5.3	SRTP Parameters.....	769
55.5.4	TLS Parameters.....	771
55.5.5	SSH Parameters.....	773
55.5.6	IDS Parameters	774
55.5.7	OCSP Parameters	775
55.6	Quality of Experience Parameters	775
55.7	Control Network Parameters.....	778
55.7.1	IP Group, Proxy, Registration and Authentication Parameters	778
55.7.2	Network Application Parameters	785
55.8	General SIP Parameters	788
55.9	Coders and Profile Parameters.....	802
55.10	Channel Parameters	804
55.10.1	Voice Parameters	804
55.10.2	Coder Parameters	807
55.10.3	DTMF Parameters	808
55.10.4	RTP, RTCP and T.38 Parameters.....	809
55.11	SBC Parameters	813
55.11.1	Supplementary Services.....	829
55.12	IP Media Parameters	830
55.13	Services	834
55.13.1	SIP-based Media Recording Parameters.....	834
55.13.2	RADIUS and LDAP Parameters	834
55.13.2.1	General Parameters	834
55.13.2.2	RADIUS Parameters	835
55.13.2.3	LDAP Parameters	837
55.13.3	Least Cost Routing Parameters	840
55.13.4	Call Setup Rules Parameters	841
55.13.5	HTTP-based Services.....	841
55.13.6	HTTP Proxy Parameters.....	842
56	Channel Capacity	845
56.1	Mediant VE SBC	847
56.1.1	Mediant VE SBC for KVM and VMware Hypervisors	847

56.1.1.1	2-vCPU Mediant VE SBC.....	847
56.1.1.2	4-vCPU Mediant VE SBC.....	848
56.1.1.3	Amazon AWS EC2.....	850
56.1.1.4	8-vCPU Mediant VE SBC.....	851
56.1.2	Mediant VE SBC for Hyper-V Hypervisor.....	853
56.1.2.1	2-vCPU Mediant VE SBC.....	853
56.1.2.2	4-vCPU Mediant VE SBC.....	855
56.2	Mediant SE SBC.....	856
57	Technical Specifications	857

Notice

This document describes AudioCodes Mediant Server Edition and Mediant Virtual Edition Session Border Controllers (SBCs).

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 2016 AudioCodes Ltd. All rights reserved.

This document is subject to change without notice.

Date Published: October-06-2016

Trademarks

AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice and CloudBond 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.

Related Documentation

Manual Name
SIP Release Notes
Mediant Server Edition SBC Installation Manual
Mediant Virtual Edition SBC Installation Manual
Complementary Guides
CLI Reference Guide
SNMP User's Guide
SBC Design Guide
Recommended Security Guidelines Configuration Note
SIP Message Manipulations Quick Reference Guide
Utility Guides
INI Viewer & Editor Utility User's Guide
AcBootP Utility User's Guide
CLI Wizard User's Guide

Notes and Warnings



Note: The device is an indoor unit and therefore, must be installed only **INDOORS**. In addition, Ethernet port interface cabling must be routed only indoors and must not exit the building.



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, refer to AudioCodes *Recommended Security Guidelines* document.



Note: Throughout this manual, unless otherwise specified, the term *device* refers to your AudioCodes product.



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

**Note:**

- 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).



Note: Some of the features listed in this document are available only if the relevant License Key has been purchased from AudioCodes and installed on the device. For a list of License Keys that can be purchased, please consult your AudioCodes sales representative.



Note: OPEN SOURCE SOFTWARE. Portions of the software may be open source software and may be governed by and distributed under open source licenses, such as the terms of the GNU General Public License (GPL), the terms of the Lesser General Public License (LGPL), BSD and LDAP, which terms are located at: <http://www.audiocodes.com/support> and all are incorporated herein by reference. If any open source software is provided in object code, and its accompanying license requires that it be provided in source code as well, Buyer may receive such source code by contacting AudioCodes, by following the instructions available on AudioCodes website.

Document Revision Record

LTRT	Description
41863	Initial document release for Version 7.2.
41864	<ul style="list-style-type: none"> ▪ Updated for patch version 7.20A.001. ▪ Updated sections: Licensing the Device; First Incoming Packet Mechanism; Configuring the Device's LDAP Cache; Centralized Third-Party Routing Server; Configuring the SEM Server (port removed); Configuring Call Setup Rules (Dial Plan queries); Call Setup Rule Examples; Registration Refreshes; Using Dial Plan Tags for IP-to-IP Routing; Enabling Interworking of SIP and SIP-I Endpoints (SPIROU and SIP header X-AC-Action); Computer Requirements (supported browsers); Configuring BroadSoft's Shared Phone Line Call Appearance for Survivability (example); Configuring RTCP XR (IP Group); Enabling Same Call Session ID over Multiple Devices (removed). ▪ New sections: Using Dial Plan Tags for Message Manipulation; Using Dial Plan Tags for Message Manipulation; VolPerfect; Configuring Test Call Endpoints. ▪ New parameters: WebLoginBlockAutoComplete; EnforcePasswordComplexity; IPGroup_SBCKeepOriginalCallID; IPGroup_SBCDialPlanName; IPGroup_CallSetupRulesSetId; CallSetupRules_QueryType; CallSetupRules_QueryTarget; IpProfile_SBCVoiceQualityEnhancement; IpProfile_SBCMaxOpusBW; IpProfile_SBCISUPVariant; PublicationIPGroupID; GeneratedRegistersInterval. ▪ Updated parameters: InterfaceTable_InterfaceName; Web password;

LTRT	Description
	<p>IPGroup_MediaRealm (Web name); CallSetupRules_AttributesToQuery (Web name and description); CallSetupRules_ActionValue; CallSetupRules_ActionSubject; CallSetupRules_Condition; CallSetupRules_AttributesToQuery; IPProfile_SBCRTCPFeedback (values); IpProfile_MediaIPVersionPreference; ConditionTable_Name; Test_Call_RouteBy (default); Test_Call_SIPInterfaceName; CLIPrivPass; NATMode (values); SendAcSessionIDHeader (removed); InboundMediaLatchMode (Note); QOEPort (removed); MaxGeneratedRegistersRate; RTPOnlyMode (removed); SBCUserRegistrationGraceTime; SBCKeepOriginalCallId.</p> <ul style="list-style-type: none"> ▪ Channel Capacity: Hyper-V 1/2/4 vCPU 4 GB RAM for Mediant VE low-capacity; AWS EC2 for Mediant VE low-capacity; VMware for Mediant VE high-capacity; KVM 8 vCPU 16 GB RAM SR-IOV Intel NICs for Mediant VE high-capacity. ▪ Miscellaneous: Allowed access to CLI re user levels; configuring media latching.
41866	<ul style="list-style-type: none"> ▪ Updated sections: Changing Index Position of Table Rows; Searching for Configuration Parameters; Configuring TLS Certificate Contexts (IPSec removed); Enabling the HTTP Proxy Application (license); Direct Media; Configuring SBC IP-to-IP Routing (IP Group load balancing); MAC Address Placeholder in Configuration File Name; VolPerfect; Channel Capacity. ▪ New sections: Configuring IP Group Sets. ▪ Updated parameters: SIPInterface_SBCDirectMedia; IPProfile_SBCDirectMediaTag; IpProfile_DisconnectOnBrokenConnection; IP2IPRouting_DestType; IPOutboundManipulation_PrivacyRestrictionMode; BrokenConnectionEventTimeout. ▪ New parameters: IP2IPRouting_IPGroupSetName; EnableNonCallCdr; PGroupSet; IPGroupSetMember; NoRTPDetectionTimeout; DisconnectOnBrokenConnection; BrokenConnectionEventTimeout.

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our Web site at <http://www.audiocodes.com/downloads>.

1 Introduction

This User's Manual describes how to configure and manage your AudioCodes product (hereafter, referred to as *device*). This document is intended for the professional person responsible for installing, configuring and managing the device.

1.1 Product Overview

AudioCodes Mediant Software Session Border Controllers (SBC) are pure-software products, enabling connectivity and security between Enterprises' and Service Providers' VoIP networks. The Mediant Software product line includes the following product variants:

- **Mediant Server Edition SBC:** x86 server-based platform, which must be installed on a server that complies to the specified hardware requirements (see "Technical Specifications" on page 857 or refer to the *Mediant Server Edition SBC Installation Manual*)
- **Mediant Virtual Edition SBC:** Installed and hosted in a virtual machine environment that complies to specified requirements (see "Technical Specifications" on page 857 or refer to the *Mediant Virtual Edition SBC Installation Manual*)

These devices provide perimeter defense for protecting companies from malicious VoIP attacks; voice and signaling mediation and normalization for allowing the connection of any IP-PBX to any Service Provider; and service assurance for service quality and manageability. The device offers call "survivability", ensuring service continuity to enterprises served by a centralized SIP-based IP-Centrex server or branch offices of distributed enterprises. Survivability functionality enables internal office communication between SIP clients in the case of disconnection from the centralized SIP IP-Centrex server or IP-PBX.

The device offers multiple local and remote management platforms, including HTTP/S-based Web server, command-line interface (CLI), and SNMP.





Note: For maximum call capacity figures, see "Channel Capacity" on page 845.

1.2 Typographical Conventions

This document uses the following typographical conventions to convey information:

Table 1-1: Typographical Conventions

Convention	Description	Example
Boldface font	Used for the following Web interface elements: <ul style="list-style-type: none"> ▪ Buttons ▪ Selectable parameter values ▪ Navigational path 	Click the Add button.
Text enclosed by double apostrophe "..."	Parameter value that you need to type.	In the 'IP Address' field, enter "10.10.1.1".
Courier font	CLI commands.	At the prompt, type the following:

Convention	Description	Example
		# configure system
Text enclosed by square brackets [...]	Ini file parameters and values.	Configure the [GWDebugLevel] parameter to [1].
Text enclosed by single apostrophe '...'	Web interface parameters.	From the 'Debug Level' drop-down list, select Basic .
	Notes highlight important or useful information.	-
	Warnings alert you to potentially serious problems if a specific action is not taken.	-

1.3 Getting Familiar with Configuration Concepts and Terminology

Before using your device, it is recommended that you familiarize yourself with the basic configuration concepts and terminology. An understanding of the basic concepts and terminology will help you configure and manage your device more effectively and easily.

1.3.1 SBC Application

The objective of your configuration is to enable the device to forward calls between telephony endpoints in the SIP-based Voice-over-IP (VoIP) network. The endpoints (SIP entities) can be servers such as SIP proxy servers and IP PBXs, or end users such as IP phones. In the SIP world, the endpoints are referred to as SIP user agents (UA). The UA that initiates the call is referred to as the user agent client (UAC); the UA that accepts the call is referred to as the user-agent server (UAS).

The following table describes the main configuration concepts and terminology.

Table 1-2: Configuration Concepts and Terminology

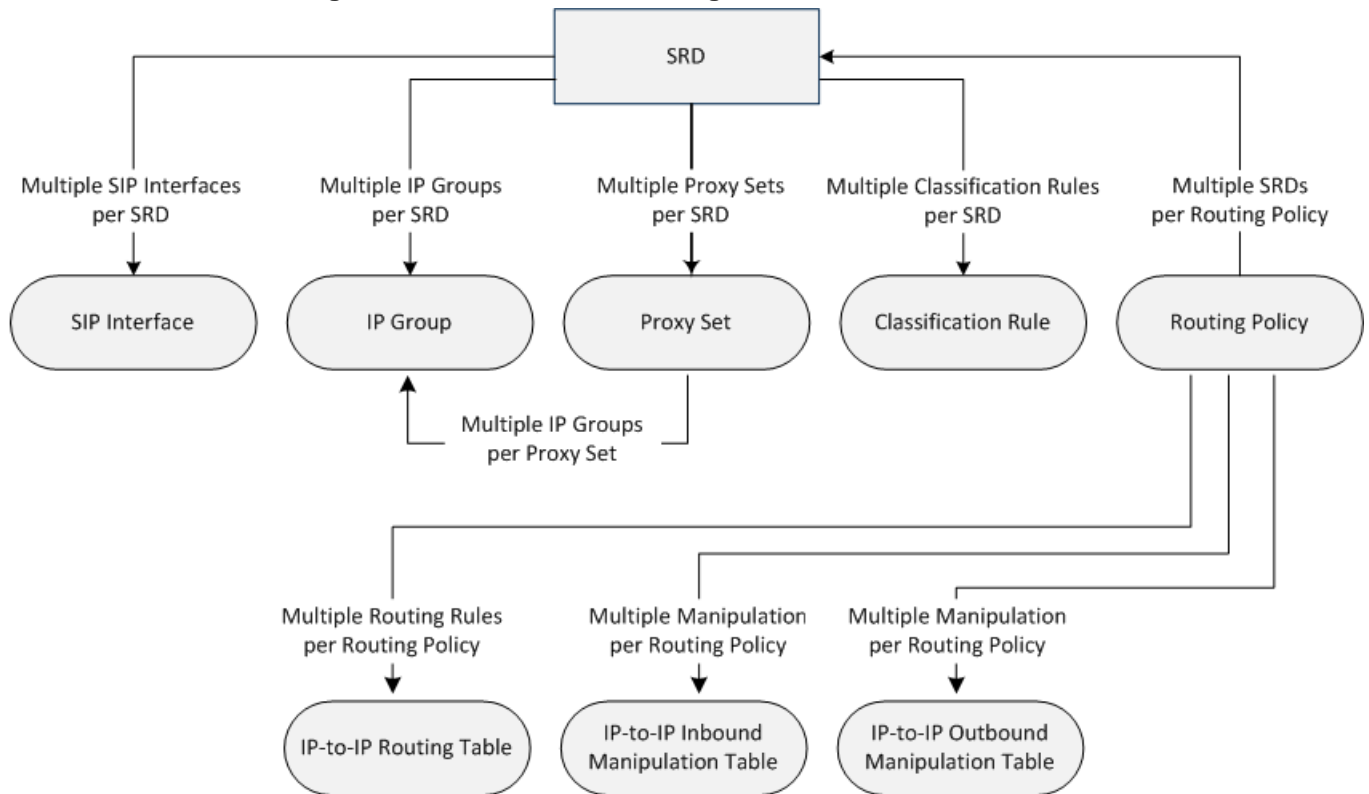
Configuration Terms	Description
IP Group	The IP Group is a logical representation of the SIP entity (UA) with which the device receives and sends calls. The SIP entity can be a server (e.g., IP PBX or SIP Trunk) or it can be a group of users (e.g., LAN IP phones). For servers, the IP Group is typically used to define the address of the entity (by its associated Proxy Set). IP Groups are used in IP-to-IP routing rules to denote the source and destination of the call.
Proxy Set	The Proxy Set defines the actual address (IP address or FQDN) of SIP entities that are servers (e.g., IP PBX). As the IP Group represents the SIP entity, to associate an address with the SIP entity, the Proxy Set is assigned to the IP Group. You can assign the same Proxy Set to multiple IP Groups (belonging to the same SRD).
SIP Interface	The SIP Interface represents a Layer-3 network. It defines a local listening port for SIP signaling traffic on a local, logical IP network interface. The term <i>local</i> implies that it's a logical port and network interface on the device. The SIP Interface is used to receive and send SIP messages with a specific SIP entity (IP Group). Therefore, you can create a SIP Interface for each SIP entity in the VoIP network with which

Configuration Terms	Description
	<p>your device needs to communicate. For example, if your VoIP network consists of three SIP entities -- a SIP Trunk, a LAN IP PBX, and remote WAN users -- a SIP Interface can be created for each of these Layer-3 networks.</p> <p>The SIP Interface is associated with the SIP entity, by assigning it to an SRD that is in turn, assigned to the IP Group of the SIP entity.</p>
Media Realm	<p>The Media Realm defines a local UDP port range for RTP (media) traffic on any one of the device's logical IP network interfaces. The Media Realm is used to receive and send media traffic with a specific SIP entity (IP Group).</p> <p>The Media Realm can be associated with the SIP entity, by assigning the Media Realm to the IP Group of the SIP entity, or by assigning it to the SIP Interface associated with the SIP entity.</p>
SRD	<p>The SRD is a logical representation of your entire SIP-based VoIP network (Layer 5) containing groups of SIP users and servers. The SRD is in effect, the foundation of your configuration to which all other previously mentioned configuration entities are associated. For example, if your VoIP network consists of three SIP entities -- a SIP Trunk, a LAN IP PBX, and remote WAN users -- the three SIP Interfaces defining these Layer-3 networks would all assigned to the same SRD.</p> <p>Typically, only a single SRD is required and this is the recommended configuration topology. As the device provides a default SRD, in a single SRD topology, the device automatically assigns the SRD to newly created configuration entities. Thus, in such scenarios, there is no need to get involved with SRD configuration.</p> <p>Multiple SRDs are required only for multi-tenant deployments, where it "splits" the device into multiple logical devices. For multiple SRDs, the SRD can be configured with a Sharing Policy. The Sharing Policy simply means whether the SRD's resources (SIP Interfaces, IP Groups, and Proxy Sets) can be used by other SRDs. For example, if all tenants route calls with the same SIP Trunking service provider, the SRD of the SIP Trunk would be configured as a <i>Shared</i> Sharing Policy. SRDs whose resources are not shared, would be configured with an <i>Isolated</i> Sharing Policy.</p>
IP Profile	<p>The IP Profile is an optional configuration entity that defines a wide range of call settings for a specific SIP entity (IP Group). The IP Profile includes signaling and media related settings, for example, jitter buffer, silence suppression, voice coders, fax signaling method, SIP header support (local termination if not supported), and media security method. The IP Profile is in effect, the interoperability "machine" of the device, enabling communication between SIP endpoints that "speak" different call "languages".</p> <p>The IP Profile is associated with the SIP entity, by assigning the IP Profile to the IP Group of the SIP entity.</p>
Classification	<p>Classification is the process that identifies the incoming call (SIP dialog request) as belonging to a specific SIP entity (IP Group).</p> <p>There are three chronological classification stages, where each stage is done only if the previous stage fails. The device first attempts to classify the SIP dialog by checking if it belongs to a user that is already registered in the device's registration database. If this stage fails, the device checks if the source IP address is defined for a Proxy Set and if yes, it classifies it</p>

Configuration Terms	Description
	<p>to the IP Group associated with the Proxy Set. If this fails, the device classifies the SIP dialog using the Classification table, which defines various characteristics of the incoming dialog that if matched, classifies the call to a specific IP Group. The main characteristics of the incoming call is the SIP Interface that is associated with the SRD for which the Classification rule is configured.</p>
IP-to-IP Routing	<p>IP-to-IP routing rules define the routes for routing calls between SIP entities. As the SIP entities are represented by IP Groups, the routing rules typically employ IP Groups to denote the source and destination of the call. For example, to route calls from the IP PBX to the SIP Trunk, the routing rule can be configured with the IP PBX as the source IP Group and the SIP Trunk as the destination IP Group.</p> <p>Instead of IP Groups, various other source and destination methods can be used. For example, the source can be a source host name while the destination can be an IP address or based on an LDAP query.</p>
Inbound and Outbound Manipulation	<p>Inbound and Outbound Manipulation lets you manipulate the user part of the SIP URI in the SIP message for a specific entity (IP Group). Inbound manipulation is done on messages received from the SIP entity; outbound manipulation is done on messages sent to the SIP entity.</p> <p>Inbound manipulation lets you manipulate the user part of the SIP URI for source (e.g., in the SIP From header) and destination (e.g., in the Request-URI line) in the incoming SIP dialog request. Outbound manipulation lets you manipulate the user part of the Request-URI for source (e.g., in the SIP From header) or destination (e.g., in the SIP To header) or calling name, in outbound SIP dialog requests.</p> <p>The Inbound and Outbound manipulation are associated with the SIP entity, by configuring the rules with incoming characteristics such as source IP Group and destination host name. The manipulation rules are also assigned a Routing Policy, which in turn, is assigned to IP-to-IP routing rules. As most deployments require only one Routing Policy, the default Routing Policy is automatically assigned to the manipulation rules and to the routing rules.</p>
Routing Policy	<p>Routing Policy logically groups routing and manipulation (inbound and outbound) rules to a specific SRD. It also enables Least Cost Routing (LCR) for routing rules and associates an LDAP server for LDAP-based routing. However, as multiple Routing Policies are required only for multi-tenant deployments, for most deployments only a single Routing Policy is required. When only a single Routing Policy is required, handling of this configuration entity is not required as a default Routing Policy is provided, which is automatically associated with all relevant configuration entities.</p>
Call Admission Control	<p>Call Admission Control (CAC) lets you configure the maximum number of permitted concurrent calls (SIP dialogs) per IP Group, SIP Interface, SRD, or user.</p>
Accounts	<p>Accounts are used to register or authenticate a "served" SIP entity (e.g., IP PBX) with a "serving" SIP entity (e.g., a registrar or proxy server). The device does this on behalf of the "served" IP Group. Authentication (SIP 401) is typically relevant for INVITE messages forwarded by the device to a "serving" IP Group. Registration is for REGISTER messages, which are initiated by the device on behalf of the "serving" SIP entity.</p>

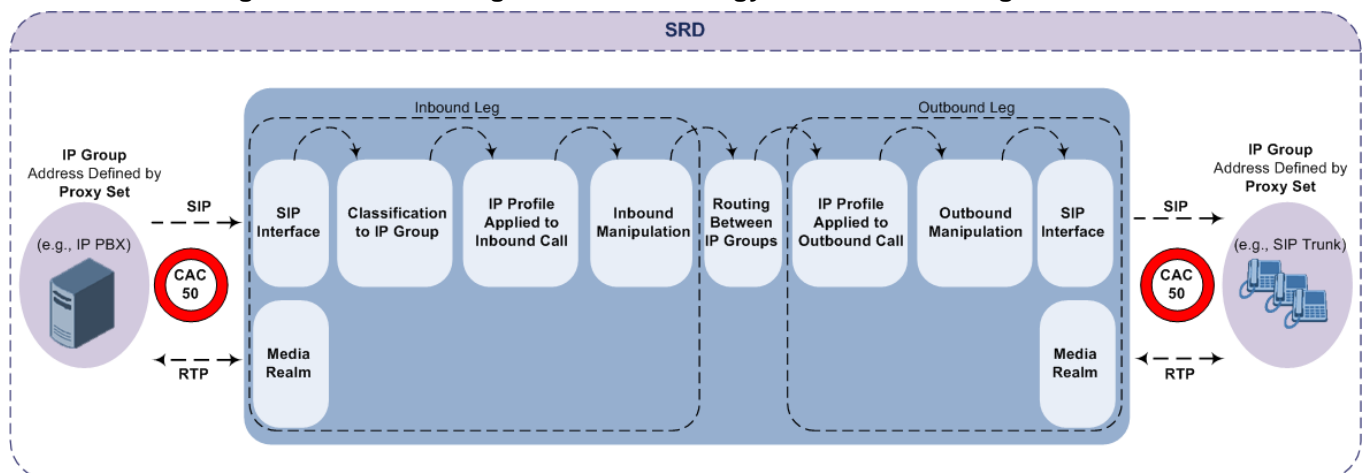
The associations between the configuration entities are summarized in the following figure:

Figure 1-1: Association of Configuration Entities



The main configuration entities and their involvement in the call processing is summarized in following figure. The figure is used only as an example to provide basic understanding of the configuration terminology. Depending on configuration and network topology, the call process may include additional stages or a different order of stages.

Figure 1-2: SBC Configuration Terminology for Call Processing



1. The device determines the SIP Interface on which the incoming SIP dialog is received and thus, determines its associated SRD.
2. The device classifies the dialog to an IP Group (origin of dialog), using a specific Classification rule that is associated with the dialog's SRD and that matches the incoming characteristics of the incoming dialog defined for the rule.

3. IP Profile and inbound manipulation can be applied to incoming dialog.
4. The device routes the dialog to an IP Group (destination), using the IP-to-IP Routing table. The destination SRD (and thus, SIP Interface and Media Realm) is the one assigned to the IP Group. Outbound manipulation can be applied to the outgoing dialog.

Part I

Getting Started with Initial Connectivity

2 Introduction

This part describes how to initially access the device's management interface and change its default IP address to correspond with your networking scheme.

This page is intentionally left blank.

3 Default OAMP IP Address

The device is shipped with a factory default IP address for operations, administration, maintenance, and provisioning (OAMP), through its VoIP LAN interface. You can use this address to initially access the device from any of its management tools (embedded Web server, EMS, or Telnet/SSH). You can also access the device through the console CLI, by connecting the device's serial (RS-232) port to a PC.

The table below lists the device's default IP address.

Table 3-1: Default VoIP LAN IP Address for OAMP

IP Address	Value
Application Type	OAMP + Media + Control
IP Address	192.168.0.1
Prefix Length	24 (255.255.255.0)
Ethernet Device	vlan 1
Interface Name	O+A+M+P

This page is intentionally left blank.

4 Installing the Software

For installing the device, refer to the following documents:

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

This page is intentionally left blank.

5 Changing Default IP Address to Suit your Network Addressing Scheme

After initial installation, the device is assigned with 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.

The procedure below describes how to change the default IP address through the CLI. The procedure uses the regular CLI commands. Alternatively, you can use the CLI Wizard utility to set up your device with the initial OAMP settings. The utility provides a fast-and-easy method for initial configuration of the device through CLI. For more information, refer to the *CLI Wizard User's Guide*.



Note: The Server Edition orders available NICs in alphabetical order of corresponding MAC addresses. If, however, the device identifies an on-board NIC, it selects it first even if external NICs' MAC addresses precede it alphabetically.

➤ To change the IP address through CLI:

1. Establish a CLI session with the device using any of the following connection methods:

- Server Edition: Use a VGA monitor and keyboard to connect to the CLI management interface.
- Virtual Edition: Connect to the Virtual Machine's (VM) console (e.g., in vSphere, click the Console tab).

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, and then press Enter:

```
Password: Admin
```

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

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

8. At the prompt, type the following command to complete the network interface configuration:

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

9. If the device is connected to an IP network that uses a VLAN ID, type the following commands to configure it (otherwise, skip this step):

```
(config-network)# network-dev 0
(network-dev-0)# vlan-id 10
(network-dev-0)# exit
```

10. At the prompt, type the following command to complete configuration:

```
(config-network)# exit
```

11. At the prompt, make sure that Port #1 is connected (i.e., link is UP) by typing the following command:

```
show network physical-port
```

The port is mapped to network-if-0, by default. For more information on mapping physical ports to the logical configuration ports, see "Configuring Ethernet Port Groups" on page 126.

12. 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 43.

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 130
- To configure the used physical Ethernet ports (speed, and mode), see "Configuring Physical Ethernet Ports" on page 124.

6 Licensing the Device

By default, the device is shipped with a pre-installed License Key that enables up to three call sessions only. After you have successfully installed the software (as described in the *Installation Manual*), follow the instructions in the *Installation Manual* for licensing your product and installing the License Key for the ordered features.

This page is intentionally left blank.

Part II

Management Tools

7 Introduction

This part describes the various management tools that you can use to configure the device:

- Embedded HTTP/S-based Web server - see "Web-based Management" on page 43
- Command Line Interface (CLI) - see "CLI-Based Management" on page 71
- Simple Network Management Protocol (SNMP) - see "SNMP-Based Management" on page 83
- Configuration *ini* file - see "INI File-Based Management" on page 91



Note:

- Some configuration settings can only be done using a specific management tool.
- For a list and description of all the configuration parameters, see "Configuration Parameters Reference" on page 733.

This page is intentionally left blank.

8 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.



Note:

- 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 License Key (see "License Key" on page 597).

8.1 Getting Acquainted with the Web Interface

This section provides a description of the Web interface.

8.1.1 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 11.0.13 or later)
 - Mozilla Firefox® (Versions 5.02 or later)
 - Google Chrome (Version 50 or later)
- 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.

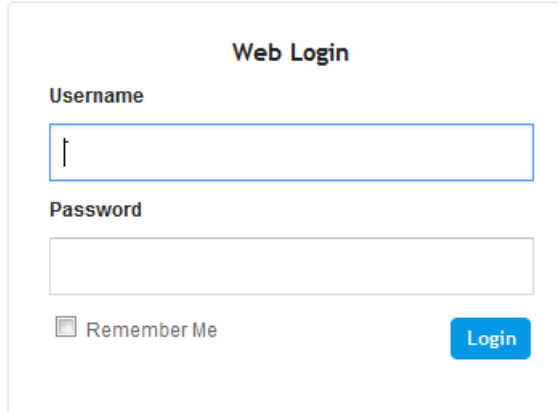
8.1.2 Accessing the Web Interface

The following procedure describes how to access the Web interface.

➤ **To access the Web interface:**

1. Open a standard Web browser.
2. In the Web browser, specify the OAMP IP address of the device (e.g., `http://10.1.10.10`); the Web interface's Login window appears, as shown below:

Figure 8-1: Web Login Screen



3. In the 'Username' and 'Password' fields, enter the username and password, respectively. The credentials are case-sensitive.
4. If you want the Web browser to remember your username and password, select the 'Remember Me' check box and then agree to the browser's prompt (depending on your browser). On your next login attempt, the 'Username' field is automatically populated with your username. Simply press the Tab or Enter key to auto-fill the 'Password' field, and then click **Login**.
5. Click **Login**.

Note:



- The default login username and password is "Admin" (case-sensitive). To change the login credentials, see "Configuring Management User Accounts" on page 60.
- By default, Web access is only through the IP address of the OAMP interface. However, you can allow access from all of the device's IP network interfaces, by setting the EnableWebAccessFromAllInterfaces parameter to 1.
- By default, autocompletion of the login username is enabled whereby the 'Username' field offers previously entered usernames. To disable autocompletion, use the WebLoginBlockAutoComplete ini file parameter.
- Depending on your Web browser's settings, a security warning box may be displayed. The reason for this is that the device's certificate is not trusted by your PC. The browser may allow you to install the certificate, thus skipping the warning box the next time you connect to the device. If you are using Windows Internet Explorer, click **View Certificate**, and then **Install Certificate**. The browser also warns you if the host name used in the URL is not identical to the one listed in the certificate. To resolve this, add the IP address and host name (ACL_nnnnnn, where nnnnnn is the serial number of the device) to your hosts file, located at /etc/hosts on UNIX or C:\Windows\System32\Drivers\ETC\hosts on Windows; then use the host name in the URL (e.g., https://ACL_280152). Below is an example of a host file:

```
127.0.0.1 localhost
10.31.4.47 ACL_280152
```

8.1.3 Areas of the GUI

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

Figure 8-2: Main Areas of the Web Interface GUI

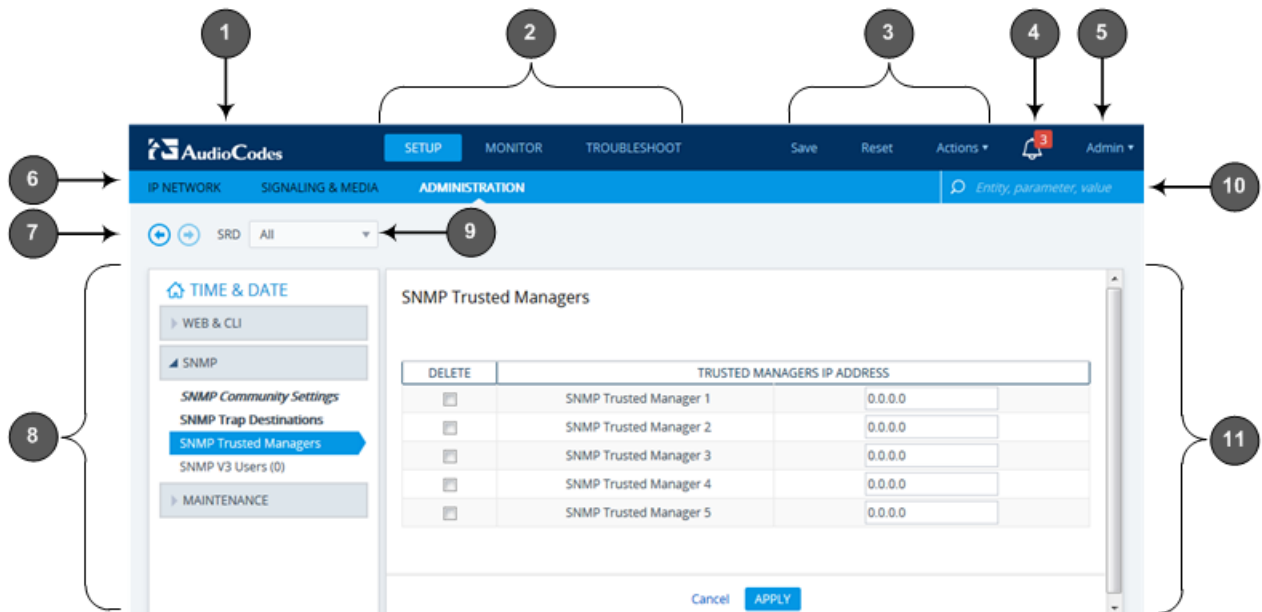




Table 8-1: Description of the Web GUI Areas

Item #	Description
1	Company logo.
2	Menu bar containing the menus.
3	<p>Toolbar providing frequently required command buttons.</p> <ul style="list-style-type: none"> ▪ Save: Saves configuration changes to the device's flash memory (without resetting the device). If you make a configuration change, the button is surrounded by a red-colored border as a reminder to save your settings to flash memory, by clicking the button. ▪ Reset: Opens the Maintenance Actions page, which is used for performing various maintenance procedures such as resetting the device (see "Basic Maintenance" on page 579). If you make a configuration change that takes effect only after a device reset, the button is surrounded by a red-colored border as a reminder to save your settings to flash memory with a device reset; otherwise, your changes revert to previous settings if the device subsequently resets or powers off. ▪ Actions: <ul style="list-style-type: none"> ✓ Configuration File: Opens the Configuration File page, which is used for saving the <i>ini</i> file to a folder on your PC, or for loading an ini file to the device (see "Backing Up and Loading Configuration File" on page 613). ✓ Auxiliary Files: Opens the Auxiliary Files page, which is used for loading Auxiliary files to the device (see "Loading Auxiliary Files through Web Interface" on page 586). ✓ License Key: Opens the License Key page, which is used for installing a new License Key file (see "Installing License Key through Web Interface" on page 600). ✓ Software Upgrade: Starts the Software Upgrade Wizard for upgrading the device's software (see "Software Upgrade Wizard" on page 604). ✓ Switchover: Opens the High Availability Maintenance page, which is used for switching between Active and Redundant devices (see High Availability Maintenance on page 582).
4	Alarm bell icon, which displays the number of active alarms generated by the device. The color of the number of alarms display indicates the highest severity of an active alarm. If you click the icon, the Active Alarms table is displayed. For more information on the table, see Viewing Active Alarms.
5	Button displaying the username of the currently logged in user. If you click the button, information of the logged-in user is displayed (see "Viewing Logged-In User Information" on page 65) and the Log Out button is provided to log out the Web session (see "Logging Off the Web Interface" on page 60).
6	<p>Tab bar containing tabs pertaining to the selected menu:</p> <ul style="list-style-type: none"> ▪ Setup menu: <ul style="list-style-type: none"> ✓ IP Network ✓ Signaling & Media ✓ Administration ▪ Monitor menu: Monitor ▪ Troubleshoot menu: Troubleshoot
7	<p>Back and Forward buttons that enable quick-and-easy navigation through previously opened pages. This is especially useful when you find that you need to return to a previously accessed page, and then need to go back to the page you just left.</p> <ul style="list-style-type: none"> ▪  Back button: Goes back to the previously accessed page. ▪  Forward button: Opens the page that you initially left using the back button. The button is available only if you have used the Back button.

Item #	Description
8	Navigation pane, which displays the Navigation tree containing the commands (items) for opening the configuration pages (see "Navigation Tree" on page 47).
9	SRD filter. When your configuration includes multiple SRDs, you can filter tables in the Web interface by a specific SRD. For more information, see "Filtering Tables in Web Interface by SRD" on page 317.
10	Search box for searching parameter names and values (see "Searching for Configuration Parameters" on page 57).
11	Work pane where configuration pages are displayed.

8.1.4 Accessing Configuration Pages from Navigation Tree

Accessing configuration pages is a three-fold process that consists of selecting a menu on the menu bar, a tab on the tab bar, and then a page item in the Navigation pane. The Navigation pane provides the Navigation tree, which is a tree-like structure of folders and page items that open configuration pages in the Work pane. The hierarchical structure and organization of the items in the Navigation tree allow you to easily drill-down and locate the required item.

The Navigation tree consists of the following areas:


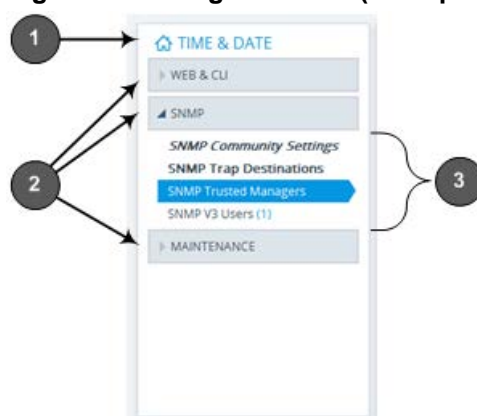
- **Home** : (Callout #1) First ("home") page displayed when a menu-tab combination is initially selected. For example, the home page of the **Setup** menu - **Administration** tab combination is the Time & Date page.
- **Folders**: (Callout #2) Folders group items of similar functionality. To open and close a folder, simply click the folder name.
- **Items**: (Callout #3) Items open configuration pages. In some cases, an item may be listed under a sub-item. An item can open a page containing stand-alone parameters or a table. If it opens a page with stand-alone parameters, the item is displayed in italics. If it opens a page with a table, the item is displayed in regular font, or bold font to indicate an item that is commonly required.

Figure 8-3: Navigation Tree (Example)



The items of the Navigation tree depend on the menu-tab combination, selected from the menu bar and tab bar, respectively. The menus and their respective tabs are listed below:

- **Setup menu:**
 - **IP Network** tab
 - **Signaling & Media** tab

- **Administration tab**

- **Monitor menu:** Monitor tab
- **Troubleshoot menu:** Troubleshoot tab

When you open the Navigation tree, folders containing commonly required items are opened by default, allowing quick access to their pages.

Items that open pages containing tables provide the following indications in the Navigation tree:

- Number of configured rows. For example, the item below indicates that two rows have been configured:

Ethernet Groups (2)

If you have filtered the Web interface display by SRD, the number reflects only the rows that are associated with the filtered SRD.

- Invalid row configuration. If you have configured a row with at least one invalid value, a red-colored icon is displayed next to the item, as shown in the following example:

Ethernet Groups (2) ●

If you hover your cursor over the icon, it displays the number of invalid rows (*lines*).

- Association with an invalid row: If you have associated a parameter of a row with a row of a different table that has an invalid configuration, the item appears with an arrow and a red-colored icon, as shown in the following example:

Ethernet Devices (2) →●

If you hover your cursor over the icon, it displays the number of rows in the table that are associated with invalid rows.

- Folder containing an item with an invalid row: If a folder contains an item with an invalid row (or associated with an invalid row), the closed folder displays a red-colored icon, as shown in the following example:



▶ CORE ENTITIES ●

If you hover your cursor over the icon, it displays the names of the items that are configured with invalid values. If you have filtered the Web interface display by SRD, only items with invalid rows that are associated with the filtered SRD are displayed.

➤ **To open a configuration page:**

1. On the menu bar, click the required menu.
2. On the tab bar, click the required tab; the Navigation tree displays the items pertaining to the selected menu-tab combination.
3. In the Navigation pane, open the folder in which the required item is located. The folders are opened and closed by clicking the title of the folder. When opened, the folder's arrow is displayed as ▲; when closed, the arrow is displayed as ▶.
4. In the folder, click the required item; the page is displayed in the Work pane.

You can also easily navigate through previously accessed pages, using the **Back** and **Forward** buttons located above the Navigation pane:

-  **Back** button: Click to go back to the previously accessed page or keep on clicking until you reach any other previously accessed page.
-  **Forward** button: Click to open the page that you just left as a result of clicking the **Back** button.

These buttons are especially useful when you find that you need to return to a previously accessed page, and then need to go back to the page you just left.



Note: Depending on the access level (e.g., Monitor level) of your Web user account, certain pages may not be accessible or may be read-only (see "Configuring Management User Accounts" on page 60). For read-only privileges:

- Read-only pages with stand-alone parameters: "Read Only Mode" is displayed at the bottom of the page.
- Read-only pages with tables: Configuration buttons (e.g., **New** and **Edit**) are missing.

8.1.5 Configuring Stand-alone Parameters

Parameters that are not contained in a table are referred to as *stand-alone* parameters.

- If you change the value of a parameter (before clicking **Apply**), the parameter's field is highlighted, as shown in the example below:

- If you change the value of a parameter from its default value and then click **Apply**, a dot appears next to the parameter's field, as shown in the example below:

•

- If you change the value of a parameter that is displayed with a lightning-bolt ⚡ icon (as shown in the example below), you must save your settings to flash memory with a device reset for your changes to take effect. When you change such a parameter and then click **Apply**, the **Reset** button on the toolbar is encircled by a red border. If you click the button, the Maintenance Actions page opens, which provides commands for doing this (see "Basic Maintenance" on page 579).

⚡

- Typically required parameters are displayed in bold font.
- If you enter an invalid value for a parameter and then click **Apply**, a message box appears notifying you of the invalid value. Click **OK** to close the message. The parameter reverts to its previous value and the field is surrounded by a colored border, as shown in the figure below:

- To get help on a parameter, simply hover your mouse over the parameter's field and a pop-up help appears, displaying a brief description of the parameter.

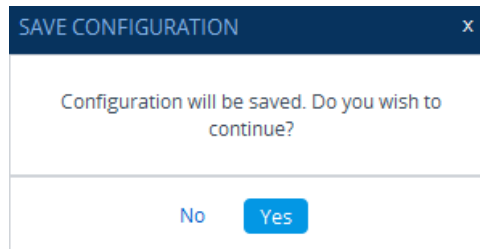
The following procedure describes how to configure stand-alone parameters.

➤ To configure a stand-alone parameter:

1. Modify the parameter's value as desired.
2. Click **Apply**; the changes are saved to the device's volatile memory (RAM).
3. Save the changes to the device's non-volatile memory (flash):
 - If a device reset is not required:

- a. On the toolbar, click **Save**; a confirmation message box appears:

Figure 8-4: Save Configuration Confirmation Box



- b. Click **Yes** to confirm; the changes are save to flash memory.
- If a device reset is required:
 - a. On the toolbar, click **Reset**; the Maintenance Actions page opens.
 - b. Click **Reset**; the device saves the changes to flash memory and then resets.



Warning: When you click **Apply**, your changes are saved only to the device's volatile memory and thus, revert to their previous settings if the device later undergoes a hardware reset, a software reset (without saving to flash) or powers down. Therefore, make sure that you save your configuration to the device's flash memory.

8.1.6 Configuring Table Parameters







A typical configuration table is shown below and subsequently described:

Figure 8-5: Description of Tables

The screenshot shows the 'Proxy Sets' configuration page. Callout 1 points to the title 'Proxy Sets (2)'. Callout 2 points to the toolbar with 'New', 'Edit', and a trash icon. Callout 3 points to the table with columns: INDEX, NAME, SRD, GATEWAY IPv4 SIP INTERFACE, PROXY KEEP-ALIVE TIME [SEC], REDUNDANCY MODE, and PROXY HOT SWAP. Callout 4 points to the configuration details for '#0[ProxySet_0]'. Callout 5 points to the 'Proxy Address 0 items >>' link. Callout 6 points to the table's pagination 'Page 1 of 1'. Callout 7 points to the 'Specify Columns' search box. Callout 8 points to the 'Edit' button for the selected row.

Table 8-2: General Description of Configuration Tables

Item #	Button
--------	--------

Item #	Button	
1	-	Page title (i.e., name of table). The page title also displays the number of configured rows as well as the number of invalid rows. For more information on invalid rows, see "Invalid Value Indications" on page 53.
2		Adds a new row to the table (see "Adding Table Rows" on page 51).
		Modifies the selected row (see "Modifying Table Rows" on page 52).
		Adds a new row with similar settings as the selected row (i.e., clones the row). For more information, see "Cloning SRDs" on page 320. Note: The button appears only in the SRDs table.
		Deletes the selected row (see "Deleting Table Rows" on page 53).
		Changes the index position of a selected row (see "Changing Index Position of Table Rows" on page 56).
	Action	Drop-down menu providing commands (e.g., Register and Un-Register). Note: The button appears only in certain tables (e.g., Accounts table).
3	-	Added table rows displaying only some of the table parameters (columns).
4	-	Detailed view of a selected row, displaying all parameters.
5	-	Link to open the "child" table of the "parent" table. A link appears only if the table has a "child" table. The "child" table is opened for the selected row.
6	-	Navigation bar for scrolling through the table's pages (see "Viewing Table Rows" on page 55).
7	-	Search tool for searching parameters and values (see "Searching Table Entries" on page 57).
8		Modifies the selected row (see "Modifying Table Rows" on page 52).

8.1.6.1 Adding Table Rows


The following procedure describes how to add table rows. Before adding rows, the following GUI conventions are used:

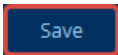
- Commonly required parameters are displayed in **bold** font.
- If you change the value of a parameter (before clicking **Apply**), the parameter's field is highlighted, as shown in the example below:

6010

- For indications of invalid values, see "Invalid Value Indications" on page 53.

➤ **To add a row:**

1. Click the **New**  button, located on the table's toolbar; a dialog box appears.
2. Configure the parameters of the row as desired. For information on configuring parameters that are assigned a value which is a row referenced from another table, see "Assigning a Row from Another Table" on page 52.

3. Click **Apply** to add the row to the table or click **Cancel** to ignore your configuration.
4. If the **Save**  button is surrounded by a red border, you must save your settings to flash memory, otherwise they are discarded if the device resets (without a save to flash) or powers off.

8.1.6.1.1 Assigning a Row from Another Table

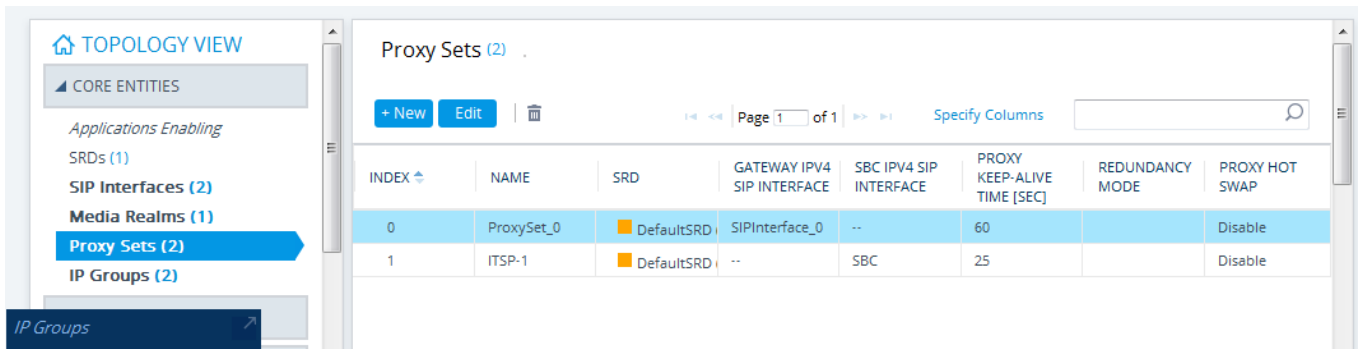
A table may contain parameters assigned a value which is a row referenced from another table. For example, the 'Proxy Set' parameter in the IP Groups table is used to assign a Proxy Set (configured in the Proxy Sets table) to an IP Group. For such parameters, a **View** button (as shown in the example below) appears next to their fields, which opens the row-referenced table (e.g., Proxy Sets table).


Figure 8-6: Clicking View Button (Example)




The **View** button is useful in that it not only allows you to check the configured rows before deciding which one to assign the parameter, but also allows you to configure a new row and then assign it to the parameter. When you click the button, the dialog box in which the parameter appears (e.g., for the IP Group) is minimized in the bottom-left corner of the Web interface and the row-referenced table (e.g., Proxy Sets table) opens, as shown in the example below:

Figure 8-7: Dialog Box Minimized and Referenced Table Opened




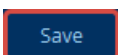
To return to your configuration, click the arrow  icon on the minimized dialog box to restore it to its previous size.

8.1.6.2 Modifying Table Rows

The following procedure describes how to modify (edit) the configuration of an existing table row. Remember that a gray-colored dot  icon displayed next to a parameter's value (as shown in the example below), indicates that it was changed from its default value:



To edit a table row:


1. Select the row that you want to edit.
2. Click the **Edit**  button, located on the table's toolbar; a dialog appears displaying the current configuration settings of the row.
3. Make your changes as desired, and then click **Apply**; the dialog box closes and your new settings are applied.
4. If the **Save**  button is surrounded by a red border, you must save your

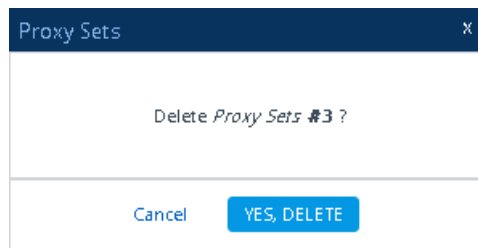
settings to flash memory, otherwise they are discarded if the device resets (without a save to flash) or powers off.

8.1.6.3 Deleting Table Rows

The following procedure describes how to delete a row from a table.


➤ **To delete a table row:**

1. Select the row that you want to delete.
2. Click the delete  icon, located on the table's toolbar; a confirmation message box appears requesting you to confirm deletion, as shown in the example below:



3. Click **Yes, Delete**; the row is removed from the table and the total number of configured rows that is displayed next to the page title and page item in the Navigation tree is updated to reflect the deletion.




Note: If the deleted row (e.g., a Proxy Set) was referenced in another table (e.g., IP Group), the reference is removed and replaced with an empty field. In addition, if the reference in the other table is for a mandatory parameter, the invalid  icon is displayed where relevant. For example, if you delete a SIP Interface that you have assigned to a Proxy Set, the invalid icon appears alongside the **Proxy Sets** item in the Navigation tree as well as on the Proxy Sets page.

8.1.6.4 Invalid Value Indications

The Web interface provides the following indications of invalid values when configuring table rows:

- **Parameters configured with invalid values:** An invalid value is a value that is not permissible for the parameter. This can include incorrect syntax (string, numeral, or character) or an out-of-range value. If you enter an invalid value and then click **Apply**, the field is surrounded by a colored border as shown in the example below.

Figure 8-8: Invalid Value

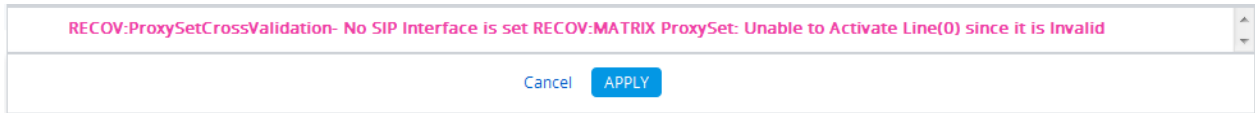


60000000

If you hover your mouse over the field, a pop-up message appears providing the valid values. If you enter a valid value, the colored border is removed from the field. If you leave the parameter at the invalid value and click **Apply**, the parameter reverts to its previous value.

- **Mandatory parameters that reference rows of other configuration tables:**

- **Adding a row:** If you do not configure the parameter and you click **Apply**, an error message is displayed at the bottom of the dialog box, as shown in the example below:

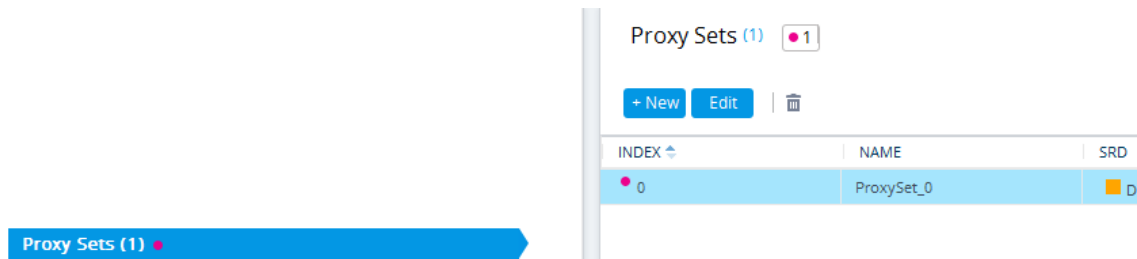


If you click **Cancel**, the dialog box closes and the row is not added to the table. To add the row, you must configure the parameter.

- **Editing a row:** If you modify the parameter so that it's no longer referencing a row of another table (i.e., blank value), when you close the dialog box, the **Invalid Line** ● icon appears in the following locations:
 - ◆ 'Index' column of the row.
 - ◆ Page title of the table. The total number of invalid rows in the table is also displayed with the icon.
 - ◆ Item in the Navigation tree that opens the table.

For example, if a mandatory parameter is not configured for Proxy Set at Index 0, **Invalid Line** ● icons are displayed for the Proxy Sets table, as shown below:

Figure 8-9: Invalid Line (Row) Icons

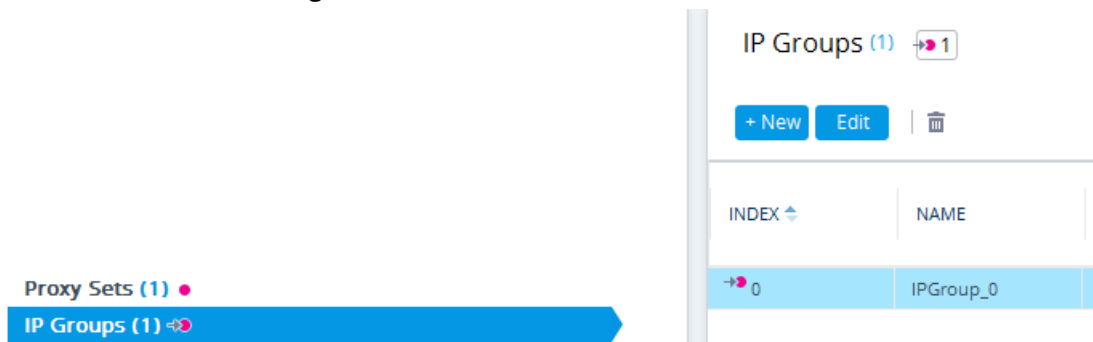


- **Parameters that reference rows of other configuration tables that are configured with invalid values:** If a row has a parameter that references a row of another table that has a parameter with an invalid value, the **Invalid Reference Line** →● icon is displayed in the following locations:


- 'Index' column of the row.
- Page title of the table. The total number of invalid rows in the table is also displayed with the icon.
- Item in the Navigation tree that opens the table.

For example, if an IP Group row (in the IP Groups table) has a parameter that references a Proxy Set row (in the Proxy Sets table) that is configured with an invalid value, the **Invalid Reference Line** →● icons are displayed for the IP Groups table, as shown below:

Figure 8-10: Invalid Reference Line Icons





Note: If you assign a non-mandatory parameter with a referenced row and then later delete the referenced row (in the table in which the row is configured), the parameter's value automatically changes to an empty field (i.e., no row assigned). Therefore, make sure that you are aware of this and if necessary, assign a different referenced row to the parameter. Only if the parameter is mandatory is the **Invalid Line**  icon displayed for the table in which the parameter is configured. For example, if you delete a SIP Interface that you have assigned to a Proxy Set, the invalid icon appears alongside the **Proxy Sets** item in the Navigation tree as well as on the Proxy Sets page.

8.1.6.5 Viewing Table Rows

Tables display a certain number of rows per page. If you have configured more than this number, you can use the table's navigation bar to scroll through the table pages, as shown below and described in the subsequent table:

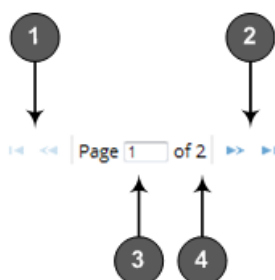


Table 8-3: Table Navigation Bar Description

Item #	Description
1	Navigation buttons to view previous table rows: <ul style="list-style-type: none"> ◀◀ Displays the previous table page ◀ Displays the first table page (i.e., page with at least the first index row)
2	Navigation buttons to view the next table rows: <ul style="list-style-type: none"> ▶▶ Displays the next table page ▶ Displays the last table page (i.e., page with last index row)
3	Currently displayed table page. To open a specific table page, enter the page number and then press the Enter key.
4	Total number of table pages.

8.1.6.6 Sorting Tables by Column

You can sort table rows by any column and in ascending order (e.g., 1, 2 and 3 / a, b, and c) or descending order (e.g., 3, 2, and 1 / c, b, and a). By default, most tables are sorted by the Index column and in ascending order.

➤ **To sort table rows by column:**

1. Click the name of the column by which you want to sort the table rows; the up-down ↕ arrows appear alongside the column name and the up button is displayed in a darker shade of color, indicating that the column is sorted in ascending order:

Figure 8-11: Table Sorted by Index in Ascending Order

INDEX ↕
0
1
2
3
4

2. To sort the column in descending order, click the column name again; only the down arrow is displayed in a darker shade of color, indicating that the column is sorted in descending order:

Figure 8-12: Table Sorted by Index in Descending Order

INDEX ↓
4
3
2
1
0

8.1.6.7 Changing Index Position of Table Rows

You can change the position (index) of rows in tables. This is done by using the up-down ↑ ↓ arrows located on the table's toolbar.



Note:

- Changing row position can only be done when the table is sorted by the 'Index' column and in ascending order; otherwise, the buttons are grayed out. For sorting table columns, see 'Sorting Tables by Column' on page 55.
- Changing row position is supported only by certain tables (e.g., IP-to-IP Routing table).

➤ **To change the position of a row:**

1. Click the 'Index' column header so that the rows are sorted in ascending order (e.g., 0, 1, 2, and so on).
2. Select the row that you want to move.
3. Do one of the following:
 - To move one index up (e.g., from Index 3 to 2): Click the up ↑ arrow; the row moves one index up in the table (e.g., to 2) and the row that originally occupied the index is moved one index down (e.g., to 3). In other words, the rows have swapped positions.

- To move one index down (e.g., from Index 3 to Index 4): Click the down ↓ arrow; the row moves one index down in the table (e.g., to 4) and the row that originally occupied the index is moved one index up (e.g., to 3). In other words, the rows have swapped positions.
4. Continue clicking the required arrow until the row has moved to the desired location in the table.

8.1.6.8 Searching Table Entries

You can search for any parameter value (alphanumeric) in configuration tables, using the Search tool. The Search tool, located above each table, is shown below and described in the subsequent table:

Figure 8-13: Table Search Tool



Table 8-4: Table Search Tool Description

Item #	Description
1	'Specify Columns' drop-down list for selecting the table column (parameter) in which to do the search. By default, the search is done in all columns.
2	Search box to enter your search key (parameter value).
3	Magnifying-glass icon which when clicked performs the search.

➤ To search for a table value:

1. If you want to perform the search on all table columns, skip this step; otherwise, from the 'Specify Columns' drop-down list, select the table column in which you want to perform the search; the name of the drop-down list changes to the name of the selected column.
2. In the Search box, enter the value for which you want to search.
3. Click the magnifying-glass icon to run the search. If the device finds the value, the table displays only the rows in which the value was found. You can then select any row and modify it by clicking the **Edit** button. If the search is unsuccessful, no rows are displayed.
4. To quit the Search tool and continue configuring rows, click the **×** icon located in the Search box.

8.1.7 Searching for Configuration Parameters

You can search in the Web interface for parameter names (standalone or table parameters) and values. The search key can include the full parameter name (Web or ini file name) or a substring of it. If you search for a substring, all parameters containing the substring in their names are listed in the search result. For example, to search for the parameter 'Telnet Server TCP Port', you can use any of the following search keys:

- "Telnet Server TCP Port" (Web name)
- "TelnetServerPort" (ini file name)

- "Telnet"
- "Port"

When the device completes the search, it displays a list of found results based on the search key. Each possible result, when clicked, opens the page on which the parameter or value is located. You need to click the most appropriate result.

➤ **To search for a parameter:**


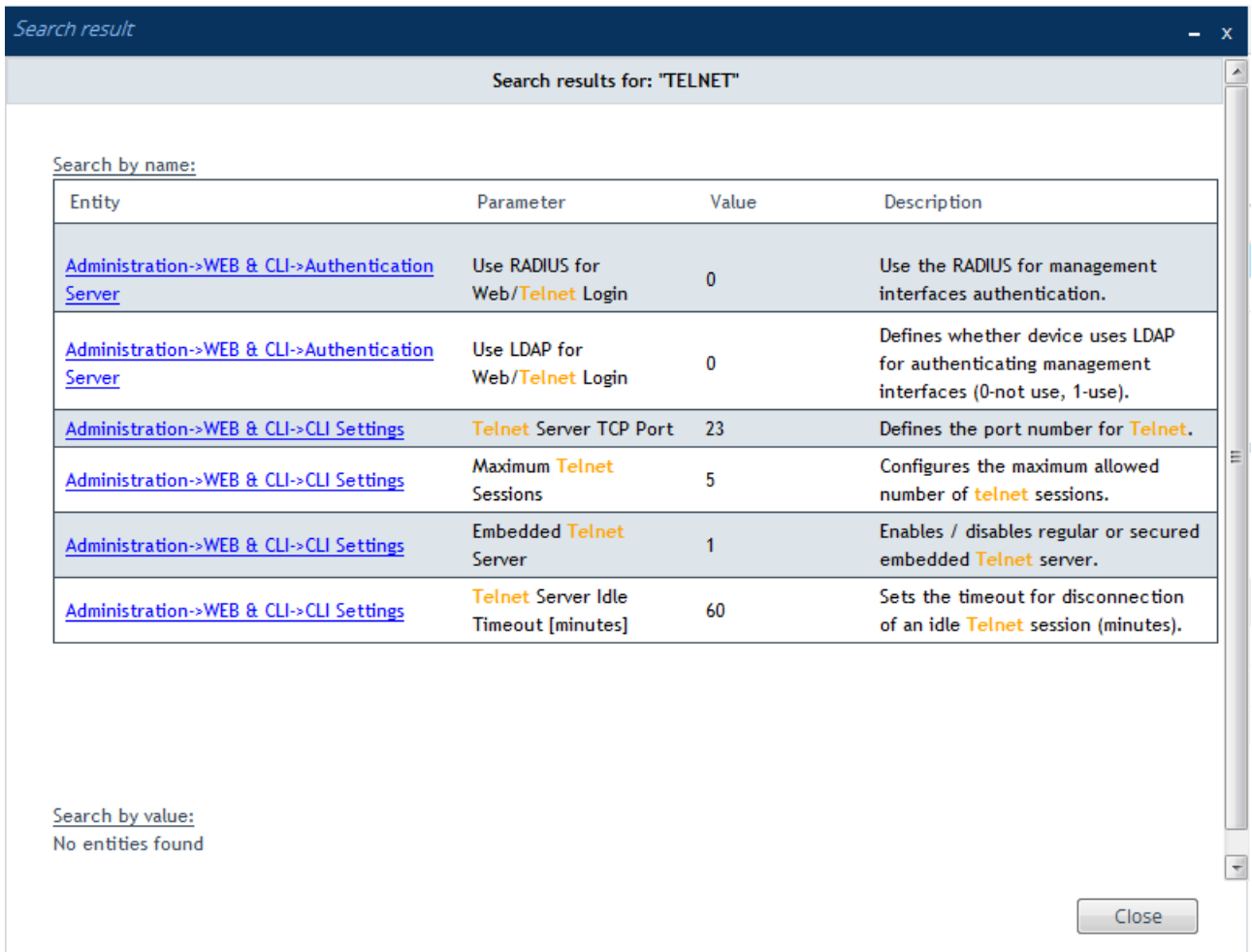
1. In the search box, enter the search key (parameter name or value).
2. Click the search  icon; the Search Result window appears, listing found parameters based on your search key. Each searched result displays the following:
 - Navigation path (link) to the page on which the parameter appears
 - Parameter's name
 - Parameter's value
 - Brief description of parameter

Figure 8-14: Search Result Window



The screenshot shows a window titled "Search result" with a search bar containing "TELNET". Below the search bar, there is a table of search results. The table has four columns: Entity, Parameter, Value, and Description. The results are as follows:

Entity	Parameter	Value	Description
Administration->WEB & CLI->Authentication Server	Use RADIUS for Web/Telnet Login	0	Use the RADIUS for management interfaces authentication.
Administration->WEB & CLI->Authentication Server	Use LDAP for Web/Telnet Login	0	Defines whether device uses LDAP for authenticating management interfaces (0-not use, 1-use).
Administration->WEB & CLI->CLI Settings	Telnet Server TCP Port	23	Defines the port number for Telnet.
Administration->WEB & CLI->CLI Settings	Maximum Telnet Sessions	5	Configures the maximum allowed number of telnet sessions.
Administration->WEB & CLI->CLI Settings	Embedded Telnet Server	1	Enables / disables regular or secured embedded Telnet server.
Administration->WEB & CLI->CLI Settings	Telnet Server Idle Timeout [minutes]	60	Sets the timeout for disconnection of an idle Telnet session (minutes).

Below the table, there is a section for "Search by value:" which shows "No entities found". A "Close" button is located at the bottom right of the window.

3. Click the link of the navigation path corresponding to the required found parameter to open the page on which the parameter appears.

8.1.8 Creating a Login Welcome Message

You can create a personalized welcome message that is displayed on the Web Login page, as shown in the example below:

Figure 8-15: User-Defined Web Welcome Message after Login

The figure shows a yellow box with the following text:

```
Note
*****
** This is a Welcome message! **
*****
```

Below this is the 'Web Login' form with the following elements:

- Username: [Text Input Field]
- Password: [Text Input Field]
- Remember Me
- Login [Button]

➤ **To create a login welcome message:**

1. Save the device's ini Configuration file to a folder on your PC (see "Backing Up and Loading Configuration File" on page 613).
2. Open the file, and then configure the welcome message using the WelcomeMessage table ini file parameter, as shown in the example below:

```
[WelcomeMessage ]
FORMAT WelcomeMessage_Index = WelcomeMessage_Text ;
WelcomeMessage 1 = "*****";
WelcomeMessage 2 = "** This is a Welcome message! **";
WelcomeMessage 3 = "*****";
[ \WelcomeMessage ]
```

3. Save the file, and then load it to the device.

To remove the welcome message, load the ini file without the parameter.

8.1.9 Getting Help

The Web interface provides you with context-sensitive pop-up help of standalone parameters. When you hover your mouse over a parameter's field, a pop-up appears with a short description of the parameter, as shown in the following example:

Figure 8-16: Viewing Context-Sensitive Help for a Parameter

SIP Transport Type U Enable SIP secured URI usage

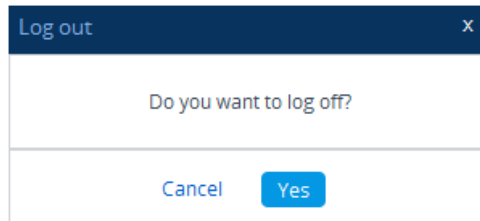
8.1.10 Logging Off the Web Interface

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

➤ **To log off the Web interface:**

1. On the menu bar, from the 'Admin' drop-down list, click **Log Out**; the following confirmation message box appears:

Figure 8-17: Log Out Confirmation Box



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

8.2 Configuring Management User Accounts

The Local Users table lets you configure up to 10 management user accounts for the device's Web interface and CLI. You configure each user account with login credentials (username and password) and with a management user level which defines the level of read and write privileges. The table below describes the different types of user levels:

Table 8-5: Description of Management User Levels

User Level	Numeric Representation in RADIUS	Privileges
Security Administrator	200	Read/write privileges for all Web pages. This user level can create all other user levels and is the only one that can create the first Master user. Note: At least one Security Administrator user must exist.
Master	220	Read/write privileges for all Web pages. This user level can create all user levels, including additional Master users and Security Administrators. It can delete all users except the last Security Administrator. Note: Only Master users can delete Master users. If only one Master user exists, it can be deleted only by itself.
Administrator	100	Read/write privileges for all Web pages, except security-related pages and the Local Users table where this user has read-only privileges.
Monitor	50	Read-only privileges and access to security-related pages is blocked.



Note: Only Security Administrator and Master users can configure users in the Local Users table. Administrator users have read-only privileges and Monitor users are denied access to the table. However, Administrator and Monitor users can change their login credentials in the Web Settings page (see "Configuring Web Session and Access Settings" on page 66).

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

Table 8-6: Default User Accounts

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



Note:

- For security, it's recommended that you change the default username and password of the default users.
- To restore the device to the default users (and with their default usernames and passwords), configure the *ini* file `ResetWebPassword` parameter to 1. If you have configured any other accounts, they are deleted.
- If you delete a user who is currently in an active Web session, the user is immediately logged off the device.
- Up to five users can be concurrently logged in to the Web interface; they can all be the same user.
- You can set the entire Web interface to read-only (regardless of Web user access levels), using the *ini* file parameter `DisableWebConfig` (see "Web and Telnet Parameters" on page 733).
- You can define additional Web user accounts using a RADIUS server (see "RADIUS Authentication" on page 222).

The following procedure describes how to configure user accounts through the Web interface. You can also configure it through CLI (`configure system > create-users-table`).

➤ **To configure management user accounts:**

1. Open the Local Users table (**Setup** menu > **Administration** tab > **Web & CLI** folder > **Local Users**).

Figure 8-18: Local Users Table

INDEX ↕	USERNAME	PASSWORD	STATUS	PASSWORD AGE	SESSION LIMIT	SESSION TIMEOUT	BLOCK DURATION	USER LEVEL
0	Admin	*	Valid	0	2	15	60	Security Administrator
1	User	*	Valid	0	2	15	60	Monitor

- Click **New**; the following dialog box is displayed:

Figure 8-19: Local Users Table - Dialog Box

The dialog box is titled "Local Users" and contains two tabs: "GENERAL" and "SECURITY".

GENERAL Tab:

- Index:
- Username:
- Password:
- User Level: (dropdown menu)
- Status: (dropdown menu)

SECURITY Tab:

- Password Age:
- Session Limit:
- Session Timeout:
- Block Duration:

- Configure a user account according to the parameters described in the table below.
- Click **Apply**, and then save your settings to flash memory.

Table 8-7: Local Users Table Parameter Descriptions

Parameter	Description
General	
Index	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
Username user	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.
Password password	Defines the Web user's password. The valid value is a string of 8 to 40 ASCII characters. To ensure strong passwords, adhere to the following password complexity requirements: <ul style="list-style-type: none"> Contain at least eight characters. Contain at least two letters that are upper case (e.g., A). Contain at least two letters that are lower case (e.g., a). Contain at least two numbers (e.g., 4). Contain at least two symbols (non-alphanumeric characters) (e.g., \$, #, %). No spaces. Contain at least four new characters that were not used in the previous password. Note: To enforce the password complexity requirements mentioned above, configure the EnforcePasswordComplexity to 1.
User Level privilege	Defines the user's access level. <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. Administrator = Read/write privileges for all pages except security-related pages including the Local Users table where this user has read-only privileges. Security Administrator = Full read/write privileges for all pages.

Parameter	Description
	<ul style="list-style-type: none"> ▪ Master = Read/write privileges for all pages. This user also functions as a security administrator. <p>Note:</p> <ul style="list-style-type: none"> ▪ At least one Security Administrator must exist. You cannot delete the last remaining Security Administrator. ▪ 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 (except the last Security Administrator). ▪ Only Security Administrator and Master users can add, edit, and delete Administrator and Monitor users.
Status status	<p>Defines the status of the 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 Login = The 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 Session and Access Settings" on page 66). 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 Security Administrator or Master. ▪ Inactivity = The 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 Session and Access Settings" on page 66). 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>Note:</p> <ul style="list-style-type: none"> ▪ The Inactivity status is applicable only to Administrator and Monitor users; Security 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.
Security	
Password Age password-age	<p>Defines the duration (in days) of the validity of the password. When the 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>
Session Limit session-limit	<p>Defines the maximum number of concurrent Web interface sessions allowed for the specific user. For example, if configured to 2, the same user account can be logged into the device's Web interface (i.e., same username-password combination) from two different management stations (i.e., IP addresses) at any one time. Once the user logs in, the session is active until the user logs off (by clicking the Log off icon on</p>

Parameter	Description
	the toolbar) or until the session expires if the user is inactive for a user-defined duration (see the 'Session Timeout' parameter below). The valid value is 0 to 5. The default is 2. Note: Up to five users can be concurrently logged in to the Web interface.
Session Timeout session-timeout	Defines the duration (in minutes) of inactivity of a logged-in user in the Web interface, after which the user is automatically logged off the Web session. In other words, the session expires when the user has not performed any operations (activities) in the Web interface for the configured timeout duration. The valid value is 0 to 100000. A value of 0 means no timeout. The default value is according to the settings of the WebSessionTimeout global parameter (see "Configuring Web Session and Access Settings" on page 66).
Block Duration block-duration	Defines the duration (in seconds) for which the user is blocked when the user exceeds a user-defined number of failed login attempts. 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 Session and Access Settings" on page 66). Note: <ul style="list-style-type: none"> ▪ To enable this feature, see the 'Deny Access On Fail Count' parameter in "Configuring Web Session and Access Settings" on page 66. ▪ The 'Deny Authentication Timer' parameter relates to failed Web logins from specific IP addresses.

8.3 Displaying Login Information upon Login

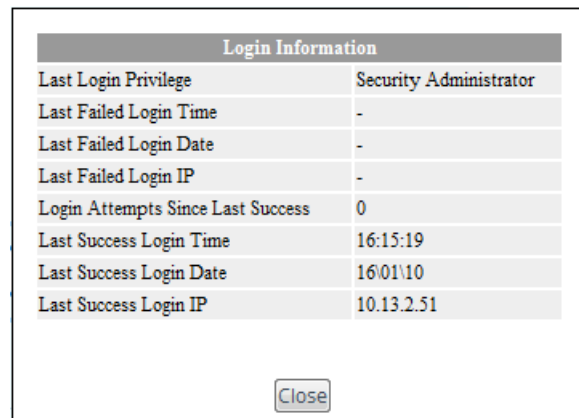
You can enable the device to display login information immediately upon Web login.

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

1. Open the Web Settings page (**Setup** menu > **Administration** tab > **Web & CLI** folder > **Web Settings**).
2. Under the **Security** group, from the 'Display Last Login Information' drop-down list, select **Enable**.
3. Click **Apply**.

Once enabled, each time you login to the device, the Login Information window is displayed, as shown in the example below:

Figure 8-20: Login Information Window



Login Information	
Last Login Privilege	Security Administrator
Last Failed Login Time	-
Last Failed Login Date	-
Last Failed Login IP	-
Login Attempts Since Last Success	0
Last Success Login Time	16:15:19
Last Success Login Date	16/01/10
Last Success Login IP	10.13.2.51

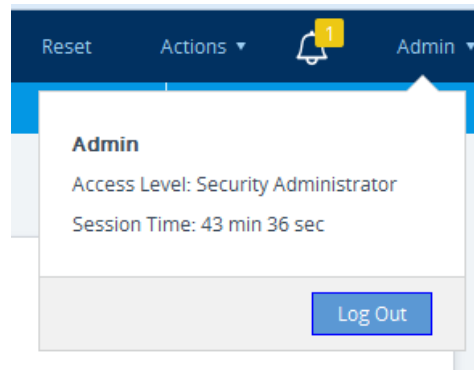
Close

To close the window, click **Close**.

8.4 Viewing Logged-In User Information

The username of the currently logged in user is displayed in the top-right corner of the Web interface. If you click the username (e.g., "Admin"), a pop-up callout appears:

Figure 8-21: Logged-in User Information



The following information is displayed:

- 'Access Level': User level of the currently logged in user (e.g., Security Administrator).
- 'Session Time': Duration of the current Web session (starting from login).

The **Log Out** button is also provided for logging out of the Web session (see "Logging Off the Web Interface" on page 60).

8.5 Configuring Web Session and Access Settings

The following procedure describes how to configure security features related to Web user sessions and access.



Note: You can only perform the configuration described in this section if you are a management user with Security Administrator level or Master level. For more information, see "Configuring Management User Accounts" on page 60.

➤ **To configure Web user sessions and access security:**

1. Open the Web Settings page (**Setup** menu > **Administration** tab > **Web & CLI** folder > **Web Settings**).
2. Under the **Session** group, configure the following parameters:

Figure 8-22: Configuring Web User Sessions

SESSION	
Password Change Interval (minutes)	<input type="text" value="1440"/>
User Inactivity Timeout (days)	<input type="text" value="90"/>
Session Timeout (minutes)	<input type="text" value="60"/>

- 'Password Change Interval': Duration (in minutes) of the validity of the Web login passwords. When the duration expires, the user must change the password in order to log in again.
 - 'User Inactivity Timeout': If the user has not logged into the Web interface within this duration, the status of the user becomes inactive and the user can no longer access the Web interface. The user can only log in to the Web interface if its status is changed (to **New** or **Valid**) by a Security Administrator or Master user (see "Configuring Management User Accounts" on page 60).
 - 'Session Timeout': Duration (in minutes) of inactivity (i.e., no actions are performed in the Web interface) of a logged-in user, after which the Web session expires and the user is automatically logged off the Web interface and needs to log in again to continue the session. You can also configure the functionality per user in the Local Users table (see "Configuring Management User Accounts" on page 60), which overrides this global setting.
3. Under the **Security** group, configure the following parameters:

Figure 8-23: Configuring Web User Security

SECURITY	
Deny Authentication Timer	<input type="text" value="60"/>
Deny Access On Fail Count (0 = No Deny)	<input type="text" value="3"/> ▼
Display Last Login Information	<input type="text" value="Disable"/> ▼

- 'Deny Authentication Timer': Interval (in seconds) that the user needs to wait before logging in from the same IP address after reaching the maximum number of failed login attempts (see next step).

- 'Deny Access On Fail Count': Number of failed login attempts (e.g., incorrect username or password) after which the device blocks access to the user for a user-defined duration (previous step).

4. Click **Apply**.

For a detailed description of the above parameters, see "Web Parameters" on page 734.

8.6 Changing Login Password for Administrator and Monitor Users

If you are logged in as a user with Administrator level or Monitor level, you can change your login password by performing the following procedure.



Note:

- Users with Security Administrator level or Master level can change passwords for themselves and for other users in the Local Users table (see "Configuring Management User Accounts" on page 60).
- You can only change the password if the duration configured in the 'Password Change Interval' has elapsed (see "Configuring Web Session and Access Settings" on page 66).

➤ **To change the login password:**

1. Open the Web Settings page (**Setup** menu > **Administration** tab > **Web & CLI** folder > **Web Settings**).

Figure 8-24: Changing Login Password for Administrator and Monitor User Levels

FILL IN THE FOLLOWING 3 FIELDS TO CHANGE THE PASSWORD	
Current Password	<input type="text"/>
New Password	<input type="text"/>
Confirm New Password	<input type="text"/> <input type="button" value="Change"/>

2. In the 'Current Password' field, type in your current login password.
3. In the 'New Password' field, type in your new password.
4. In the 'Confirm New Password' field, type in your new password again.
5. Click **Change**; you are logged off the Web session and prompted to login in again with your new login password.

8.7 Configuring Secured (HTTPS) Web

By default, the device allows remote management (client) through HTTP and HTTPS. However, you can enforce secure Web access communication by configuring the device to accept only HTTPS.

➤ **To configure secure (HTTPS) Web access:**

1. Open the Web Settings page (**Setup** menu > **Administration** tab > **Web & CLI** folder > **Web Settings**).
2. Under the **General** group, configure the following:

SECURITY	
Deny Authentication Timer	<input type="text" value="60"/>
Deny Access On Fail Count (0 = No Deny)	<input type="text" value="3"/>
Display Last Login Information	<input type="text" value="Disable"/>

3. From the 'Secured Web Connection (HTTPS)' drop-down list, select **HTTPS Only**.
4. To enable two-way authentication whereby both management client and server are authenticated using X.509 certificates, from the 'Require Client Certificates for HTTPS connection' drop-down list, select **Enable**.
5. In the 'HTTPS Cipher String' field, enter the cipher string for HTTPS (in OpenSSL cipher list format).
6. Click **Apply**, and then reset the device with a save-to-flash for your settings to take effect.

For more information on secure Web-based management including TLS certificates, see "TLS for Remote Device Management" on page 112.

8.8 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.

8.9 Configuring Web and Telnet Access List

The Access List table lets you restrict access to the device's management interfaces (Web, Telnet and SSH) by specifying IP addresses (up to ten) of management clients that are permitted to access the device. Access to the device's management interfaces from undefined IP addresses is denied. If you don't specify any IP addresses, this security feature is inactive and the device can be accessed from any IP address.

The following procedure describes how to configure the Access List through the Web interface. You can also configure it through ini file (WebAccessList_x).



Note:

- Configure the IP address of the computer from which you are currently logged into the device as the first authorized IP address in the Access List. If you configure any other IP address, access from your computer will be immediately denied.
- If you configure network firewall rules in the Firewall table (see "Configuring Firewall Rules" on page 157), you must configure a firewall rule that permits traffic from IP addresses configured in the Access List table.

➤ **To add IP addresses to the Access List:**

1. Open the Access List table (**Setup** menu > **Administration** tab > **Web & CLI** folder > **Access List**).

Figure 8-25: Access List - Adding IP Address

Access List

Add an authorized IP address

2. In the 'Add an authorized IP address' field, configure an IP address, and then click **Add New Entry**; the IP address is added to the table.

Figure 8-26: Web & Telnet Access List Table

DELETE ROW	AUTHORIZED IP ADDRESS
1 <input type="checkbox"/>	10.13.2.51

If you have configured IP addresses in the Access List and you no longer want to restrict access to the management interface based on the Access List, delete all the IP addresses in the table, as described in the following procedure.



Note: When deleting all the IP addresses, make sure that you delete the IP address of the computer from which you are currently logged into the device, **last**; otherwise, access from your computer will be immediately denied.

- **To delete an IP address from the Access List:**
 1. Select the Delete Row check box corresponding to the IP address that you want to delete.
 2. Click **Delete Selected Addresses**.

9 CLI-Based Management

This chapter provides an overview of the CLI-based management and provides configuration relating to CLI management.



Note:

- By default, CLI is disabled (for security purposes).
- The CLI can only be accessed by management users with the following user levels:
 - ✓ Administrator
 - ✓ Security Administrator
 - ✓ Master
- For a description of the CLI commands, refer to the CLI Reference Guide.

9.1 Getting Familiar with CLI

This section describes the basic structure of the device's CLI, which you may need to know before configuring the device through CLI.

9.1.1 Understanding Configuration Modes

Before you begin your CLI session, you should familiarize yourself with the CLI command modes. Each command mode provides different levels of access to commands, as described below:

- **Basic command mode:** Initial mode that is accessed upon a successful CLI login authentication. Any user level can access the mode and thus, the commands supported by this command tier are limited, as is interaction with the device itself. The mode allows you to view various information (using the show commands) and activate various debugging capabilities.

```
Welcome to ...
Username: Admin
Password:
>
```

The Basic mode prompt is ">".

- **Enable command mode:** The mode is the high-level tier in the command hierarchy, one step up from the Basic mode. A password ("Admin", by default) is required to access the mode **after** you have accessed the Basic mode. The mode allows you to configure all the device's settings. The Enable mode is accessed by typing the following commands:

```
> enable
Password: <Enable mode password>
#
```

The Enable mode prompt is "#".



Note: The default password for accessing the Enable mode is "Admin" (case-sensitive). To change the password, use the CLIPrivPass ini file parameter.

The Enable mode groups the configuration commands under the following command sets:

- configure network:** Contains IP network-related commands (e.g., interface and dhcp-server):


```
# configure network
(config-network)#
```
- configure voip:** Contains voice-over-IP related commands (e.g., ip-group, sbc, gateway, and media):


```
# configure voip
(config-voip)#
```
- configure system:** Contains system-related commands (e.g., clock, snmp settings, and web):


```
# configure system
(config-system)#
```
- configure troubleshoot:** Contains logging-related commands (e.g., syslog, logging and test-call):


```
# configure troubleshoot
(config-troubleshoot)#
```

9.1.2 Using CLI Shortcuts

The CLI provides several editing shortcut keys to help you configure your device more easily, as listed in the table below.

Table 9-1: CLI Editing Shortcut keys

Shortcut Key	Description
Up arrow key	Retypes the previously entered command. Continuing to press the Up arrow key cycles through all commands entered, starting with the most recent command.
<Tab> key	Pressing the <Tab> key after entering a partial (but unique) command automatically completes the command, displays it on the command prompt line, and waits for further input. Pressing the <Tab> key after entering a partial and not unique command displays all completing options.

Shortcut Key	Description
? (question mark)	<ul style="list-style-type: none"> Displays a list of all subcommands in the current mode, for example: <pre>(config-network)# ? access-list Network access list dhcp-server DHCP server configuration dns DNS configuration ...</pre> Displays a list of available commands beginning with certain letter(s), for example: <pre>(config-network)# d? dhcp-server DHCP server configuration dns DNS configuration</pre> Displays syntax help for a specific command by entering the command, a space, and then a question mark (?). This includes the range of valid values and a brief description of the next parameter expected for that particular command. For example: <pre>(config-network)# dns srv2ip ? [0-9] index</pre> <p>If a command can be invoked (i.e., all its arguments have been entered), the question mark at its end displays "<cr>" to indicate that a carriage return (Enter) can now be entered to run the command, for example:</p> <pre>(config)# logging host 10.1.1.1 ? <cr></pre>
<Ctrl + A>	Moves the cursor to the beginning of the command line.
<Ctrl + E>	Moves the cursor to the end of the command line.
<Ctrl + U>	Deletes all the characters on the command line.
auto finish	You need only enter enough letters to identify a command as unique. For example, entering "int G 0/0" at the configuration prompt provides you access to the configuration parameters for the specified Gigabit-Ethernet interface. Entering "interface GigabitEthernet 0/0" would work as well, but is not necessary.
Space Bar at the --More--prompt	Displays the next screen of output. You can configure the size of the displayed output, as described in "Configuring Displayed Output Lines in CLI Terminal Window" on page 80.

9.1.3 Common CLI Commands

The following table contains descriptions of common CLI commands.

Table 9-2: Common CLI Commands

Command	Description
do	Provides a way to execute commands in other command sets without taking the time to exit the current command set. The following example shows the do command, used to view the GigabitEthernet interface configuration while in the

Command	Description
	virtual-LAN interface command set: <pre>(config)# interface vlan 1 (conf-if-VLAN 1)# do show interfaces GigabitEthernet 0/0</pre>
no	Undoes an issued command or disables a feature. Enter no before the command: <pre># no debug log</pre>
activate	Activates a command. When you enter a configuration command in the CLI, the command is not applied until you enter the activate and exit commands. Note: Offline configuration changes require a reset of the device. A reset can be performed at the end of the configuration changes. A required reset is indicated by an asterisk (*) before the command prompt.
exit	Leaves the current command-set and returns one level up. If issued on the top level, the session ends. For online parameters, if the configuration was changed and no activate command was entered, the exit command applies the activate command automatically. If issued on the top level, the session will end: <pre>(config)# exit # exit (session closed)</pre>
display	Displays the configuration of current configuration set.
help	Displays a short help how-to string.
history	Displays a list of previously run commands.
list	Displays the available command list of the current command-set.
 <filter>	Applied to a command output. The filter should be typed after the command with a pipe mark (). Supported filters: <ul style="list-style-type: none"> ▪ include <word> – filter (print) lines which contain <word> ▪ exclude <word> – filter lines which does not contain <word> ▪ grep <options> - filter lines according to <i>grep</i> common Unix utility options ▪ egrep <options> - filter lines according to <i>egrep</i> common Unix utility options ▪ begin <word> – filter (print) lines which begins with <word> ▪ between <word1> <word2> – filter (print) lines which are placed between <word1> and <word2> ▪ count – show the output's line count Example: <pre># show system version grep Number ;Serial Number: 2239835;Slot Number: 1</pre>

9.1.4 Configuring Tables through CLI

Throughout the CLI, many configuration elements are in table format where each table row is represented by an index number. When you add a new row to a table, the device automatically assigns it the next consecutive, available index number. However, you can specify a different index number.

Table rows are added using the **new** command after the table command:

```
# <the table's CLI command name> new
```

When you add a new table row, the device accesses the row's configuration mode. For example, if three rows are configured in the Accounts table (account-0, account-1, and account-2) and you then add a new row, account-3 is automatically created and its configuration mode is accessed:

```
(config-voip)# sip-definition account new
(account-3)#
```

You can also add a new table row to any specific index number, even if a row has already been configured for that index number. The row that was previously assigned that index number is incremented to the next consecutive index number, as well as all the index rows listed below it in the table. To add a new table row to a specific index number, use the **insert** command:

```
# <table name> <index> insert
```

For example, if three rows are configured in the Accounts table (account-0, account-1, and account-2) and you then add a new row with index 1, the previous account-1 becomes account-2 and the previous account-2 becomes account-3, and so on. The following command is run for this example:

```
(config-voip)# sip-definition account 1 insert
```



Note: The insert table row feature is applicable only to tables that do not have "child" tables (sub-tables).

You can also change the position (index) of a configured row by moving it one row up or one row down in the table, using the following command:

```
# <table> <index to move> move-up|move-down
```

For example, to move the row at Index 1 down to Index 2 in the IP-to-IP Routing table:

```
<config-voip># sbc routing ip2ip-routing 1 move-down
```

In this example, the previous row at Index 2 is moved up to Index 1.



Note: Changing of row position is applicable only to certain tables.

9.1.5 Understanding CLI Error Messages

The CLI provides feedback on commands by displaying informative messages:

- Failure reason of a run command. The failure message is identical to the notification failure message sent by Syslog. For example, an invalid Syslog server IP address is displayed in the CLI as follows:


```
(logging)# syslog-ip 1111.1.1.1
Parameter 'SyslogServerIP' does NOT accept the IP-Address:
1111.1.1.1, illegal IPAddress.
Configuration failed
Command Failed!
```
- "Invalid command" message: The command may not be valid in the current command mode, or you may not have entered sufficient characters for the command to be recognized. Use "?" to determine your error.
- "Incomplete command" message: You may not have entered all of the pertinent information required to make the command valid. Use "?" to determine your error.

9.2 Enabling CLI

By default, access to the device's CLI through Telnet and SSH is disabled. This section describes how to enable these protocols.



9.2.1 Enabling Telnet for CLI

The following procedure describes how to enable Telnet. You can enable a secured Telnet that uses Secure Socket Layer (SSL) where information is not transmitted in clear text. 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. To configure such a message, see "Creating a Login Welcome Message" on page 59.

➤ To enable Telnet:

1. Open the CLI Settings page (**Setup** menu > **Administration** tab > **Web & CLI** folder > **CLI Settings**).

TELNET	
Embedded Telnet Server	Enable Unsecured 
Telnet Server TCP Port	23
Telnet Server Idle Timeout [minutes]	5 
Maximum Telnet Sessions	5

2. Configure the following parameters:
 - 'Embedded Telnet Server': Select **Enable Unsecured** or **Enable Secured** (i.e., SSL) to enable Telnet.
 - 'Telnet Server TCP Port': Enter the port number of the embedded Telnet server.
 - 'Telnet Server Idle Timeout': Enter the duration of inactivity in the Telnet session after which the session automatically ends.
3. Click **Apply**, and then reset the device with a save-to-flash for your settings to take effect.

For a detailed description of the Telnet parameters, see "Telnet Parameters" on page 737.

9.2.2 Enabling SSH with RSA Public Key for CLI

Unless configured for TLS, Telnet is not secure as it requires passwords to be transmitted in clear text. To overcome this, you can use Secure SHell (SSH) 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 device's 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 software):**

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 9-1: Selecting Public RSA Key in PuTTY



2. Open the CLI Settings page (**Setup** menu > **Administration** tab > **Web & CLI** folder > **CLI Settings**), and then do the following:
 - a. From the 'Enable SSH Server' drop-down list, select **Enable**.
 - b. Paste the public key that you copied in Step 1.d into the 'Admin Key' field, as shown below:

SECURE SHELL (SSH)	
Enable SSH Server	Enable
Server Port	22
Admin Key	AAAAB3NzaC1yc2EAAAEE
Public Key	Enable
Max Payload Size	32768
Max Binary Packet Size	35000
Enable Last Login Message	Enable
Max Login Attempts	3
Maximum SSH Sessions	5

- c. For additional security, you can configure the 'Public Key' field to **Enable**. This ensures that SSH access is only possible by using the RSA key and not by username and password.
 - d. Configure the other SSH parameters as required. For a description of these parameters, see "SSH Parameters" on page 773.
 - e. Click **Apply**.
 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 CLI Settings page, and then paste the value copied in Step 2 into the 'Admin Key' field.
 4. Click **Apply**.
 5. Connect to the device with SSH, using the following command (where xx.xx.xx.xx is the device's IP address):


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

 RSA-key negotiation occurs automatically and no password is required.

9.3 Configuring Maximum Telnet/SSH Sessions

You can configure the maximum number of concurrent Telnet and SSH sessions (up to five) permitted on the device.



Note: Before changing the setting, make sure that not more than the number of sessions that you want to configure are currently active; otherwise, the new setting will not take effect.

- **To configure the maximum number of concurrent Telnet and SSH sessions:**
1. Open the CLI Settings page (**Setup** menu > **Administration** tab > **Web & CLI** folder > **CLI Settings**).
 2. For Telnet: Under the **Telnet** group, in the 'Maximum Telnet Sessions' field, enter the maximum number of concurrent sessions.
 3. For SSH: Under the **SSH** group, in the 'Maximum SSH Sessions' field, enter the maximum number of concurrent sessions.
 4. Click **Apply**.

9.4 Establishing a CLI Session

You can access the device's CLI using any of the following methods:

- **RS-232:** The device can be accessed through its RS-232 serial port, by connecting a VT100 terminal to it or using a terminal emulation program (e.g., HyperTerminal) with a PC. For connecting to the CLI through RS-232, see CLI.
- **Secure SHell (SSH):** The device can be accessed through its Ethernet interface by the SSH protocol using SSH client software. A popular and freeware SSH client software is Putty, which can be downloaded from <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>
- **Telnet:** The device can be accessed through its Ethernet interface by the Telnet protocol using Telnet client software.

The following procedure describes how to access the CLI through Telnet/SSH.



Note: The CLI login credentials are the same as all the device's other management interfaces (such as Web interface). The default username and password is "Admin" and "Admin" (case-sensitive), respectively. To configure login credentials and management user accounts, see "Configuring Management User Accounts" on page 60.

- **To establish a CLI session with the device:**
1. Connect the device to the network.
 2. Establish a Telnet or SSH session using the device's OAMP IP address.
 3. Log in to the session using the username and password assigned to the Admin user of the Web interface:
 - a. At the Username prompt, type the username, and then press Enter:
Username: Admin
 - b. At the Password prompt, type the password, and then press Enter:
Password: Admin
 - c. At the prompt, type the following, and then press Enter:
> enable
 - d. At the prompt, type the password again, and then press Enter:
Password: Admin

9.5 Viewing Current CLI Sessions

You can view users that are currently logged in to the device's CLI. This applies to users logged in to the CLI through RS-232 (console), Telnet, or SSH. For each logged-in user, the following is displayed: the type of interface (console, Telnet, or SSH), username, remote IP address from where the user logged in, and the duration (days and time) of the session. Each user is displayed with a unique index (session ID).

➤ **To view currently logged-in CLI users:**

1. Establish a CLI session with the device.
2. Run the following command:

```
# show users
[0] console      Admin      local      0d00h03m15s
[1] telnet       John       10.4.2.1   0d01h03m47s
[2]* ssh         Alex       192.168.121.234 12d00h02m34s
```

The current session from which this show command was run is displayed with an asterisk (*).



Note: The device can display management sessions of up to 24 hours. After this time, the duration counter is reset.

9.6 Terminating a User's CLI Session

You can terminate users that are currently logged in to the device's CLI. This applies to users logged in to the CLI through RS-232 (console), Telnet, or SSH.

➤ **To terminate the CLI session of a specific CLI user:**

1. Establish a CLI session with the device.
2. Run the following command:

```
# clear user <session ID>
```

Where *<session ID>* is a unique identification of each currently logged in user. You can view the session ID by running the **show users** command (see "Viewing Current CLI Sessions" on page 80).



Note: The session from which the command is run cannot be terminated.

9.7 Configuring Displayed Output Lines in CLI Terminal Window

You can configure the maximum number of lines (height) displayed in the terminal window for the output of CLI commands (Telnet and SSH). The number of displayed lines can be from 0 to 65,535, or determined by re-sizing the terminal window by mouse-dragging the window's border.

➤ **To specify the number of displayed output lines:**

1. Establish a CLI session with the device.

2. Access the System menu:

```
# configure system
```

3. At the prompt, type the following command:

```
(config-system)# cli-terminal
```

4. At the prompt, type the following command:

```
<cli-terminal># window-height [0-65535]
```

If window-height is set to 0, the entire command output is displayed. In other words, even if the output extends beyond the visible terminal window length, the --MORE-- prompt is not displayed.

➤ **To configure the number of displayed output lines by dragging terminal window:**

1. Establish a CLI session with the device.

2. Access the System menu:

```
# configure system
```

3. At the prompt, type the following command:

```
(config-system)# cli-terminal
```

4. At the prompt, type the following command:

```
<cli-terminal># window-height automatic
```

When this mode is configured, each time you change the height of the terminal window using your mouse (i.e., dragging one of the window's borders or corners), the number of displayed output command lines is changed accordingly.

This page is intentionally left blank.

10 SNMP-Based Management

The device provides an embedded SNMP agent that lets you manage it using AudioCodes Element Management System (EMS) or a third-party SNMP manager. The SNMP agent supports standard and proprietary Management Information Base (MIBs). All supported MIB files are supplied to customers as part of the release. The SNMP agent can send unsolicited SNMP trap events to the SNMP manager.

**Note:**

- By default, SNMP-based management is enabled.
- For more information on the device's SNMP support such as SNMP trap alarms and events, refer to the *SNMP Reference Guide*.
- For more information on AudioCodes EMS, refer to the *EMS User's Manual*.

10.1 Enabling SNMP

By default, SNMP is enabled. You can enable SNMP as described in the following procedure.

➤ **To enable SNMP:**

1. Open the SNMP Community Settings page (**Setup** menu > **Administration** tab > **SNMP** folder > **SNMP Community Settings**).

Figure 10-1: Enabling SNMP



2. Under the **Misc. Settings** group, from the 'Disable SNMP' drop-down list (DisableSNMP parameter), select **Yes**.
3. Click **Apply**.

10.2 Configuring SNMP Community Strings

SNMP community strings determine the access privileges (read-only and read-write) of SNMP clients with the device's SNMP agent. You can configure up to five read-only SNMP community strings and up to five read-write SNMP community strings. The device's SNMP agent accepts SNMP Get (read-only) and Set (read-write) requests only if the correct community string is used in the request.

You can also configure a unique password-like community string used for sending SNMP traps. The device sends the traps with the community string.



Note:

- SNMP community strings are applicable only to SNMPv1 and SNMPv2c; SNMPv3 uses username-password authentication along with an encryption key (see "Configuring SNMP V3 Users" on page 88).
- You can enhance security by configuring Trusted Managers (see "Configuring SNMP Trusted Managers" on page 87). A Trusted Manager is an IP address from which the SNMP agent accepts Get and Set requests.

For detailed descriptions of the SNMP parameters, see "SNMP Parameters" on page 738.

➤ **To configure SNMP community strings:**

1. Open the SNMP Community Settings page (**Setup** menu > **Administration** tab > **SNMP** folder > **SNMP Community Settings**).
2. Configure SNMP community strings for access privileges:

READ ONLY COMMUNITY STRINGS	
Read Only 1	<input type="text"/>
Read Only 2	<input type="text"/>
Read Only 3	<input type="text"/>
Read Only 4	<input type="text"/>
Read Only 5	<input type="text"/>

READ/WRITE COMMUNITY STRINGS	
Read/Write 1	<input type="text"/>
Read/Write 2	<input type="text"/>
Read/Write 3	<input type="text"/>
Read/Write 4	<input type="text"/>
Read/Write 5	<input type="text"/>

- Under the **Read Only Community Strings** group, configure read-only community strings (see the table below).
 - Under the **Read/Write Community Strings** group, configure read-write community strings (see the table below).
3. Configure a community string for SNMP traps: Under the **Misc. Settings** group, in the 'Trap Community String' field, configure a community string (see the table below).

Figure 10-2: Configuring SNMP Trap Community String

Trap Community String	<input type="text" value="trapuser"/>
-----------------------	---------------------------------------

4. Click **Apply**, and then reset the device with a save-to-flash for your settings to take effect.

To delete a community string, delete the configured string, click **Apply**., and then reset the device with a save-to-flash for your settings to take effect.

Table 10-1: SNMP Community String Parameter Descriptions

Parameter	Description
Read-Only Community Strings configure system > snmp settings > ro-community-string [SNMPReadOnlyCommunityString_x]	Defines read-only SNMP community strings. Up to five read-only community strings can be configured. The valid value is a string of up to 19 characters that can include only the following: <ul style="list-style-type: none"> ▪ Upper- and lower-case letters (a to z, and A to Z) ▪ Numbers (0 to 9) ▪ Hyphen (-) ▪ Underline (_) For example, "Public-comm_string1". The default is "public".
Read-Write Community Strings configure system > snmp settings > rw-community-string [SNMPReadWriteCommunityString_x]	Defines read-write SNMP community strings. Up to five read-write community strings can be configured. The valid value is a string of up to 19 characters that can include only the following: <ul style="list-style-type: none"> ▪ Upper- and lower-case letters (a to z, and A to Z) ▪ Numbers (0 to 9) ▪ Hyphen (-) ▪ Underline (_) For example, "Private-comm_string1". The default is "private".
Trap Community String configure system > snmp trap > community-string [SNMPTrapCommunityString]	Defines the community string for SNMP traps. The valid value is a string of up to 19 characters that can include only the following: <ul style="list-style-type: none"> ▪ Upper- and lower-case letters (a to z, and A to Z) ▪ Numbers (0 to 9) ▪ Hyphen (-) ▪ Underline (_) For example, "Trap-comm_string1". The default is "trapuser".

10.3 Configuring SNMP Trap Destinations with IP Addresses

The SNMP Trap Destinations table lets you to configure up to five SNMP trap managers to receive traps sent by the device. The SNMP manager is defined by IP address and port. 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.

The following procedure describes how to configure SNMP trap destinations through the Web interface. You can also configure it through ini file (SNMPManager) or CLI (configure system > snmp trap-destination).

➤ **To configure SNMP trap destinations:**

1. Open the SNMP Trap Destinations table (**Setup** menu > **Administration** tab > **SNMP** folder > **SNMP Trap Destinations**).

Figure 10-3: SNMP Trap Destinations Table

	NAME	IP ADDRESS	TRAP PORT	TRAP USER	TRAP ENABLE
<input type="checkbox"/>	SNMP Manager 1	0.0.0.0	162	v2cParams	Enable
<input type="checkbox"/>	SNMP Manager 2	0.0.0.0	162	v2cParams	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	162	v2cParams	Enable

2. Configure the SNMP trap manager according to the table below.
3. Select the check boxes corresponding to the configured SNMP managers that you want to enable.
4. Click **Apply**.



Note:

- Rows whose corresponding check boxes are cleared revert to default settings when you click **Apply**.
- To enable the sending of the trap event, `acPerformanceMonitoringThresholdCrossing`, which is sent every time a threshold (high or low) of a performance monitored SNMP object is crossed, configure the ini file parameter `PM_EnableThresholdAlarms` to 1.
- Instead of configuring SNMP trap managers with an IP address in dotted-decimal notation, you can configure a single SNMP trap manager with an FQDN (see "Configuring an SNMP Trap Destination with FQDN" on page 87).

Table 10-2: SNMP Trap Destinations Table Parameters Description

Parameter	Description
(check box) [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
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.
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 88

Parameter	Description
Trap Enable [SNMPManagerTrapSendingEnable_x]	Activates the sending of traps to the SNMP Manager. <ul style="list-style-type: none"> ▪ [0] Disable ▪ [1] Enable (Default)

10.4 Configuring an SNMP Trap Destination with FQDN

Instead of configuring SNMP trap destinations (managers) with IP addresses in dotted-decimal notation in the SNMP Trap Destinations table (see "Configuring SNMP Trap Destination with IP Addresses" on page 85), you can configure a single SNMP trap manager with an FQDN (e.g., mngr.corp.mycompany.com). The device sends the traps to the DNS-resolved IP address. The resolved IP address replaces the IP address of the last row (SNMP Manager 5) in the SNMP Trap Destinations table (and the last trap manager entry in the snmpTargetAddrTable in the snmpTargetMIB).



Note: If you configure an FQDN for an SNMP trap manager:

- The device ignores your configuration in the SNMP Trap Destinations table.
- Only one SNMP trap manager can be configured.

➤ To configure an SNMP trap destination with an FQDN:

1. Open the SNMP Community Settings page (**Setup** menu > **Administration** tab > **SNMP** folder > **SNMP Community Settings**).
2. Under the **Misc. Settings** group, in the 'Trap Manager Host Name' field (SNMPTrapManagerHostName parameter), enter the FQDN.
3. Click **Apply**.

10.5 Configuring SNMP Trusted Managers

The SNMP Trusted Managers table lets you configure up to five SNMP Trusted Managers. 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 (see "Configuring SNMP Community Strings" on page 83). You can enhance security by configuring Trusted Managers, which is an IP address from which the device's SNMP agent accepts and processes SNMP requests. If no SNMP Trusted Manager is configured, any SNMP manager can access the device (as long as the community string is correct).

The following procedure describes how to configure SNMP Trusted Managers through the Web interface. You can also configure it through ini file (SNMPTrustedMgr_x) or CLI (configure system > snmp settings > trusted-managers).

➤ **To configure SNMP Trusted Managers:**

1. Open the SNMP Trusted Managers table (**Setup** menu > **Administration** tab > **SNMP** folder > **SNMP Trusted Managers**).

Figure 10-4: SNMP Trusted Managers Table

DELETE	TRUSTED MANAGERS IP ADDRESS		
<input type="checkbox"/>	SNMP Trusted Manager 1		0.0.0.0
<input type="checkbox"/>	SNMP Trusted Manager 2		0.0.0.0
<input type="checkbox"/>	SNMP Trusted Manager 3		0.0.0.0
<input type="checkbox"/>	SNMP Trusted Manager 4		0.0.0.0
<input type="checkbox"/>	SNMP Trusted Manager 5		0.0.0.0

2. Configure an IP address (in dotted-decimal notation) for one or more SNMP Trusted Managers.
3. Select the check boxes corresponding to the configured SNMP Trusted Managers that you want to enable.
4. Click **Apply**, and then reset the device with a save-to-flash for your settings to take effect.

10.6 Enabling SNMP Traps for Web Activity

You can enable the device to send SNMP traps to notify of management users' activities in the Web interface. A trap is sent each time an activity is done by a user. To configure the types of Web activities that you want reported, see "Configuring Reporting of Management User Activities" on page 705.

➤ **To enable traps to SNMP manager for Web activity:**

1. Open the SNMP Community Settings page (**Setup** menu > **Administration** tab > **SNMP** folder > **SNMP Community Settings**).
2. Under the **Misc. Settings** group, from the 'Activity Trap' drop-down list (EnableActivityTrap), select **Enable**.

Figure 10-5: Enabling Trap for Web User Activities



3. Click **Apply**.

10.7 Configuring SNMP V3 Users

The SNMPv3 Users table lets you configure up to 10 SNMP v3 users for authentication and privacy.

The following procedure describes how to configure SNMP v3 users through the Web interface. You can also configure it through ini file (SNMPUsers) or CLI (configure system > snmp v3-users).



Note: If you delete a user that is associated with a trap destination (see "Configuring SNMP Trap Destinations with IP Addresses" on page 85), the trap destination becomes disabled and the trap user reverts to default (i.e., SNMPv2).

- **To configure an SNMP v3 user:**
- 1. Open the SNMPv3 Users table (**Setup** menu > **Administration** tab > **SNMP** folder > **SNMP V3 Users**).
- 2. Click **New**; the following dialog box appears:

Figure 10-6: SNMPv3 Users Table - Dialog Box

- 3. Configure the SNMP V3 parameters according to the table below.
- 4. Click **Apply**, and then reset the device with a save-to-flash for your settings to take effect.

Table 10-3: SNMPv3 Users Table Parameters Description

Parameter	Description
Index [SNMPUsers_Index]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
User Name username [SNMPUsers_Username]	Name of the SNMP v3 user. The name must be unique.
Authentication Protocol auth-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 priv-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	Authentication key. Keys can be entered in the form of a text password

Parameter	Description
auth-key [SNMPUsers_AuthKey]	or long hex string. Keys are always persisted as long hex strings and keys are localized.
Privacy Key priv-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 group [SNMPUsers_Group]	The group with which the SNMP v3 user is associated. <ul style="list-style-type: none"> ▪ [0] Read-Only ▪ [1] Read-Write (default) ▪ [2] Trap Note: All groups can be used to send traps.

11 INI File-Based Management

You can configure the device through an ini file, which is a text-based file with an *.ini file extension name, created using any standard text-based editor such as Notepad. Once you have created an ini file with all your configuration settings, you need to install (load) it to the device to apply the configuration. For a list of the *ini* file parameters, see "Configuration Parameters Reference" on page 733.

11.1 INI File Format

There are two types of *ini* file parameters:

- Individual parameters - see "Configuring Individual ini File Parameters" on page 91
- Table parameters - see "Configuring Table ini File Parameters" on page 91

11.1.1 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 ";".

```
[optional 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 93.

11.1.2 Configuring Table ini File Parameters

Table ini file parameters allow you to configure tables, which include multiple parameters (*columns*) and row entries (*indices*). The table ini file parameter is composed of the following elements:

- **Table title:** 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).

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_CoderSpecific;
CodersGroup0 0 = g711Alaw64k, 20, 0, 255, 0, 0;
CodersGroup0 1 = eg711Ulaw, 10, 0, 71, 0, 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.

11.1.3 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.

11.2 Configuring an ini File

There are different methods that you can use for configuring an ini file before you load it to the device.

- Modifying the device's current ini file: This method is recommended if you mainly need to change the settings of parameters that you have previously configured.
 1. Save the device's current configuration as an *ini* file on your computer, using the Web interface (see "Saving Configuration" on page 582).
 2. Open the file using a text file editor, and then modify the *ini* file as required.
 3. Save and close the file.
 4. Load the file to the device.
- Creating a new ini file that includes only updated configuration:
 1. Open a text file editor such as Notepad.
 2. Add only the required parameters and their settings.
 3. Save the file with the ini file extension name (e.g., myconfiguration.ini).
 4. Load the file to the device.

For loading ini files to the device, see "Loading an ini File to the Device" on page 94.



Note:

- If you save an ini file from the device and a table row is configured with invalid values, the ini file displays the row prefixed with an exclamation mark (!), for example:

```
!CpMediaRealm 1 = "ITSP", "Voice", "", 60210, 2, 6030, 0, "",  
" ";
```

- To restore the device to default settings through the *ini* file, see "Restoring Factory Defaults" on page 633.

11.3 Loading an ini File to the Device

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

- CLI:
 - Voice Configuration: # copy voice-configuration from <URL>
- Web interface:
 - Auxiliary Files page (see "Loading Auxiliary Files" on page 585): The device updates its configuration according to the loaded ini file while preserving the remaining current configuration.
 - Configuration File page (see "Backing Up and Loading Configuration File" on page 613): The device updates its configuration according to the loaded ini file and applies default values to parameters that were not included in the loaded ini file.

When you load an ini file to the device, its configuration settings are saved to the device's non-volatile memory.



Note: Before you load an *ini* file to the device, make sure that the file extension name is **.ini*.

11.4 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 the *DConvert Utility User's Guide*.



Note: If you save an ini file from the device to a folder on your PC, an *ini* file that was loaded to the device encoded is saved as a regular *ini* file (i.e., unencoded).

11.5 Configuring Password Display in ini File

Passwords can be displayed in the ini file in one of the following formats, configured by the INIPasswordsDisplayType ini file parameter:

- Obscured: The password characters are concealed and displayed as encoded. The password is displayed using the syntax, `1<obscured password>`, for example, `1S3p+fno=`.
- Hidden: the password is replaced with an asterisk (*).

When you save an ini file from the device to a PC, the passwords are displayed according to the enabled format. When you load an ini file to the device, obscured passwords are parsed and applied to the device; hidden passwords are ignored.

By default, the enabled format is obscured passwords, thus enabling their full recovery in case of configuration restore or copy to another device.

When obscured password mode is enabled, you can enter a password in the ini file using any of the following formats:

- `1<obscured password>`: Password in obscured format as generated by the device; useful for restoring device configuration and copying configuration from one device to another.
- `0<plain text>`: Password can be entered in plain text; useful for configuring a new password. When the ini file is loaded to the device and then later saved from the device to a PC, the password is displayed obscured (i.e., `1<obscured password>`).

11.6 INI Viewer and Editor Utility

AudioCodes INI Viewer & Editor utility provides a user-friendly graphical user interface (GUI) that lets you easily view and modify the device's ini file. This utility is available from AudioCodes Web site at www.AudioCodes.com/downloads, and can be installed on any Windows-based PC.

For more information, refer to the *INI Viewer & Editor User's Guide*.

Part III

General System Settings

12 Configuring SSL/TLS Certificates

The TLS Contexts table lets you 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, default TLS setup. Configure certificates only if required.
- Since X.509 certificates have an expiration date and time, you must configure the device to use Network Time Protocol (NTP) to obtain the current date and time from an NTP server. Without the correct date and time, client certificates cannot work. To configure NTP, see "Configuring Automatic Date and Time using SNTP" on page 115.
- Only **Base64 (PEM)** encoded X.509 certificates can be loaded to the device.

12.1 Configuring TLS Certificate Contexts

The TLS Contexts table lets you configure up to 100 TLS certificates, referred to as *TLS Contexts*. The Transport Layer Security (TLS), also known as Secure Socket Layer (SSL) can be used to secure the device's SIP signaling connections or SIP over TLS (SIPS), Web (HTTPS) sessions, Telnet sessions and SSH sessions. The TLS/SSL protocol provides confidentiality, integrity, and authenticity between two communicating applications over TCP/IP.

The device is shipped with a default TLS Context (configured in row index 0 and called "default"), which includes a self-generated random private key and a self-signed server certificate. The subject name of the default certificate is "ACL_nnnnnnn", where *nnnnnn* denotes the serial number of the device.



Note:

- The default TLS Context cannot be deleted.
- The default TLS Context can be used for SIPS or any other supported application such as Web (HTTPS), Telnet, and SSH.
- If you configure new TLS Contexts, you can use them only for SIPS.
- If a TLS Context for an existing TLS connection is changed during the call by the user agent, the device ends the connection.

You can configure each TLS Context with the following:

- TLS version (SSL 3.0, TLS 1.0, TLS 1.1 and TLS 1.2)
- Encryption ciphers for server and client - DES, RC4 compatible, Advanced Encryption Standard (AES)
- TLS certificate expiry check, whereby the device periodically checks the validation date of the installed TLS server certificates and sends an SNMP trap event if a certificate is nearing expiry. To configure TLS certificate expiry check, see "Configuring TLS Server Certificate Expiry Check" on page 114.
- Online Certificate Status Protocol (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 OCSP. When OCSP is enabled, the device queries the OCSP server for revocation information whenever a

peer certificate is received (TLS client mode, or TLS server mode with mutual authentication).



Note:

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

- Private key - externally created and then uploaded to device.
- Different levels of security strength (key size) per TLS certificate.
- X.509 certificates - self-signed certificates or signed as a result of a certificate signing request (CSR).
- Trusted root certificate authority (CA) store (for validating certificates).

To use a TLS Context for SIPS, assign it to a Proxy Set and/or SIP Interface associated with the IP Group for which you want to employ TLS certificates. When the device establishes a TLS connection (handshake) with a SIP user agent (UA), the TLS Context is determined as follows:

■ **Incoming calls:**

1. Proxy Set: If the incoming call is successfully classified to an IP Group based on Proxy Set (i.e., IP address of calling party) and the Proxy Set is configured for TLS ('Transport Type' parameter is set to **TLS**), the TLS Context assigned to the Proxy Set is used. To configure Proxy Sets, see "Configuring Proxy Sets" on page 341.
2. SIP Interface: If the Proxy Set is either not configured for TLS (i.e., the 'Transport Type' parameter is set to **UDP**) or not assigned a TLS Context, and/or classification to a Proxy Set fails, the device uses the TLS Context assigned to the SIP Interface used for the call. To configure SIP Interfaces, see "Configuring SIP Interfaces" on page 321.
3. Default TLS Context (ID 0): If the SIP Interface is not assigned a TLS Context or no SIP Interface is used for the call, the device uses the default TLS Context.

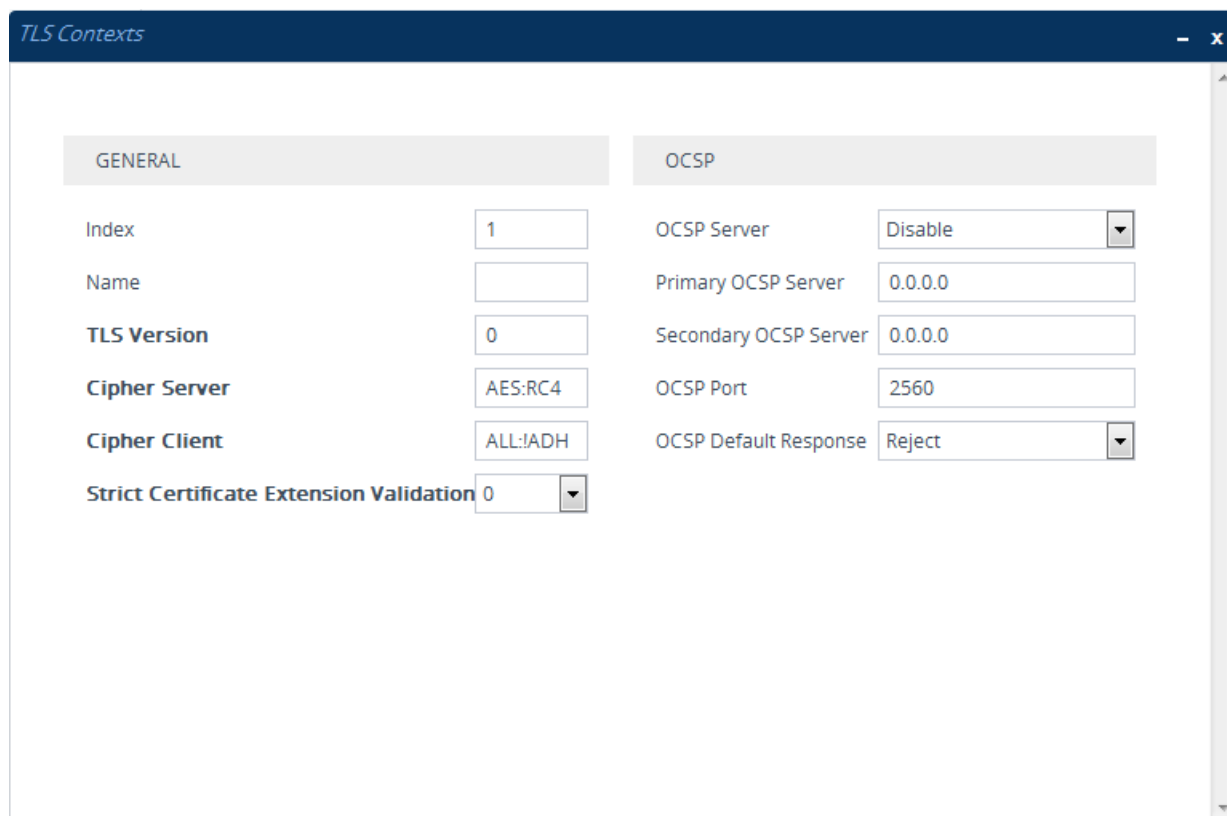
■ **Outgoing calls:**

1. Proxy Set: If the outgoing call is sent to an IP Group associated with a Proxy Set that is assigned a TLS Context and the Proxy Set is configured for TLS (i.e., 'Transport Type' parameter is set to **TLS**), the TLS Context is used. If the 'Transport Type' parameter is set to **UDP**, the device uses UDP to communicate with the proxy and no TLS Context is used.
2. SIP Interface: If the Proxy Set is not assigned a TLS Context, the device uses the TLS Context assigned to the SIP Interface used for the call.
3. Default TLS Context (ID 0): If the SIP Interface is not assigned a TLS Context or no SIP Interface is used for the call, the device uses the default TLS Context.

The following procedure describes how to configure a TLS Context through the Web interface. You can also configure it through ini file (TLSContexts) or CLI (configure system > tls <ID>).

➤ **To configure a TLS Context:**

1. Open the TLS Contexts table (**Setup** menu > **IP Network** tab > **Security** folder > **TLS Contexts**).
2. Click **New** to add a new TLS Context or **Edit** to modify the default TLS Context at Index 0; the following dialog box appears (for adding a TLS Context):



3. Configure the TLS Context according to the parameters described in the table below.
4. Click **Apply**, and then reset the device with a save-to-flash for your settings to take effect.

Table 12-1: TLS Contexts Parameter Descriptions

Parameter	Description
General	
Index tls <ID> [TLSContexts_Index]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
Name name [TLSContexts_Name]	Defines an arbitrary name to easily identify the row. The valid value is a string of up to 31 characters.
TLS Version tls-version [TLSContexts_TLSVersion]	Defines the supported SSL/TLS protocol version. Clients attempting to communicate with the device using a different TLS version are rejected. <ul style="list-style-type: none"> ▪ [0] Any - Including SSLv3 = (Default) SSL 3.0 and all TLS versions are supported. ▪ [1] TLSv1.0 = Only TLS 1.0. ▪ [2] TLSv1.1 = Only TLS 1.1. ▪ [3] TLSv1.0 and TLSv1.1 = Only TLS 1.0 and TLS 1.1. ▪ [4] TLSv1.2 = Only TLS 1.2. ▪ [5] TLSv1.0 and TLSv1.2 = Only TLS 1.0 and TLS 1.2. ▪ [6] TLSv1.1 and TLSv1.2 = Only TLS 1.1 and TLS 1.2.

Parameter	Description
	<ul style="list-style-type: none"> [7] TLSv1.0 TLSv1.1 and TLSv1.2 = Only TLS 1.0, TLS 1.1 and TLS 1.2 (excludes SSL 3.0).
Cipher Server ciphers-server [TLSContexts_ServerCipherString]	Defines the supported cipher suite for the TLS server (in OpenSSL cipher list format). For valid values, refer to URL http://www.openssl.org/docs/apps/ciphers.html . The default is AES:RC4. For example, configure the parameter to "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. Note: <ul style="list-style-type: none"> If the installed License Key includes the Strong Encryption feature, the default of the parameter is changed to RC4:EXP, enabling RC-128-bit encryption. The value "ALL" can be used only if the installed License Key includes the Strong Encryption feature.
Cipher Client ciphers-client [TLSContexts_ClientCipherString]	Defines the supported cipher suite for TLS clients. The valid value is up to 255 strings (e.g., "EXP"). The default is ALL:!ADH. For possible values and additional details, refer to http://www.openssl.org/docs/apps/ciphers.html .
Strict Certificate Extension Validation require-strict-cert [TLSContexts_RequireStrictCert]	Enables the validation of the extensions (keyUsage and extendedKeyUsage) of peer certificates. The 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. <ul style="list-style-type: none"> [0] Disable (default) [1] Enable
OCSP	
OCSP Server ocp-server [TLSContexts_OcspEnable]	Enables or disables certificate checking using OCSP. <ul style="list-style-type: none"> [0] Disable (default) [1] Enable
Primary OCSP Server ocp-server-primary [TLSContexts_OcspServerPrimary]	Defines the IP address (in dotted-decimal notation) of the primary OCSP server. The default is 0.0.0.0.
Secondary OCSP Server ocp-server-secondary [TLSContexts_OcspServerSecondary]	Defines the IP address (in dotted-decimal notation) of the secondary OCSP server (optional). The default is 0.0.0.0.
OCSP Port ocp-port [TLSContexts_OcspServerPort]	Defines the OCSP server's TCP port number. The default port is 2560.
OCSP Default Response ocp-default-response [TLSContexts_OcspDefaultResponse]	Determines whether the device allows or rejects peer certificates if it cannot connect to the OCSP server. <ul style="list-style-type: none"> [0] Reject (default)

Parameter	Description
esponse]	<ul style="list-style-type: none"> ▪ [1] Allow

12.2 Assigning CSR-based Certificates to TLS Contexts

The following procedure describes how to request a digitally signed certificate from a Certification Authority (CA) for a TLS Context. This process is referred to as a certificate signing request (CSR) and is required if your organization employs a Public Key Infrastructure (PKI) system. The CSR contains information identifying the device such as a distinguished name in the case of an X.509 certificate.

➤ **To assign a CSR-based certificate to a TLS Context:**

1. Your network administrator should allocate a unique DNS name for the device (e.g., dns_name.corp.customer.com). The DNS name is used to access the device and therefore, must be listed in the server certificate.
2. Open the TLS Contexts table (see "Configuring TLS Certificate Contexts" on page 99).
3. In the table, select the required TLS Context, and then click the **Change Certificate** link located below the table; the Context Certificates page appears.
4. Under the **Certificate Signing Request** group, do the following:
 - a. In the 'Subject Name [CN]' field, enter the DNS name.



Note: For the Subject Name, you can use the IP address of the device instead of a qualified DNS name. However, it is not recommended since the IP address is subject to change and may not uniquely identify the device.

- a. From the 'Signature Algorithm' drop-down list, select the hash function algorithm (SHA-1, SHA-256, or SHA-512) with which to sign the certificate.
- 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 12-1: Certificate Signing Request Group

CERTIFICATE SIGNING REQUEST

Subject Name [CN]	
Organizational Unit [OU] <i>(optional)</i>	Headquarters
Company name [O] <i>(optional)</i>	Corporate
Locality or city name [L] <i>(optional)</i>	Poughkeepsie
State [ST] <i>(optional)</i>	New York
Country code [C] <i>(optional)</i>	US
Signature Algorithm	SHA-1 ▼

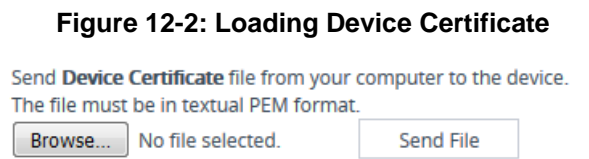
After creating the CSR, copy the text below (including the BEGIN/END lines) and send it to your Certification Authority for signing.

```
-----BEGIN CERTIFICATE REQUEST-----
MIIBOjCCAQsCAQAwYjEVMBMGA1UECwwMSGVhZHF1YXJ0ZXJzMRIwEAYDVQQKDA1D
b3Jwb3JhdGUxFTATBgNVBACMDFBvdWdoe2V1cHNpZTERMA8GA1UECAwITmV3IFlv
cm91dCZAJBgNVBAYTA1VIMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQDA2+oJ
FV6WPLu+sibZ4cn2EAB448Ty2GHR0fCN2pRRqOdWduOIrkqLUejsSrWYBkJUYH3B
3etIvXAssHTmNH+yn4Xyid/s022nBYfUI6rAM65FvL7hi821Ks2Fn401Lz0kdhaG
IV1gPVjJnLIuce70RCG5eEdtLetj1Vc86TDZ0wIDAQABoAAwDQYJKoZIhvcNAQEF
BQADgYEAS8Fb70g4bTlWmPXg5ANa9q9MzasJr3pGriOxQHhnmhv/1AWit9/u/UwN
V9occI+N/cd/jWdEwjWdMwJxu0yCTRg0IdryXAKinorGGhh8Zqtfdr+XWRLrb07J
7TXgr652s52P7v2eMy+vDFm8ON6C17ls78OCYmnuAccCrT8Wj8=
-----END CERTIFICATE REQUEST-----
```

5. Copy the text and send it to your security provider (CA) to sign this request.
6. When the CA sends you a server certificate, save the certificate to a file (e.g., cert.txt). Make sure 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/MQswCQYDVQQGEw
JGUxFTBMBEGA1UEChMKQ2VydG1wb3N0ZTEbMBkGA1UEAxMSQ2VydG1wb3N0ZSBT
ZXJ2ZXVyb3R4b3R5b3R5b3R5b3R5b3R5b3R5b3R5b3R5b3R5b3R5b3R5b3R5b3R5
UEBhMCRlIxEzARBgNVBAoTc2VydG1wb3N0ZTEbMBkGA1UEAxMSQ2VydG1wb3N0ZSBT
ZXJ2ZXVyb3R4b3R5b3R5b3R5b3R5b3R5b3R5b3R5b3R5b3R5b3R5b3R5b3R5b3R5
dGUgU2VydMv1cjCCASEwDQYJKoZIhvcNAQEBBQADggEoADCCAQkCggEAPqd4Mz
iR4spWldGRx8bQrhZkonWnNm`+Yhb7+4Q67ecf1janH7GcN/SXsfx7jJpreWUL
f7v7Cvpr4R7qIJcmdHIntmf7JPM5n6cDBv17uSW63er7NkVnMFHwK1QaGFLMyb
FkzaeGrvFm4k3lRefiXDmuOe+FhJgHYezYHf44LvPRPwhSrzi9+AQ3o8pWDguJ
uZDIUP1F1jMa+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.

9. Verify that the private key is correct:
 - a. Open the TLS Contexts table.
 - b. Select the required TLS Context index row.
 - c. Click the **Certificate Information** link located below the table.
 - d. Make sure that the 'Private key' field displays "OK"; otherwise, consult with your security administrator.

Figure 12-3: Verifying Private Key
Certificate Information

GENERAL	
Certificate subject:	/CN=ACL_5469038
Certificate issuer:	/CN=ACL_5469038
Time to expiration:	7299 days
Key size:	1024 bits
Private key:	OK



Note:

- The certificate replacement process can be repeated whenever necessary (e.g., the new certificate expires).
- You can also load the device certificate through the device's Automatic Provisioning mechanism, using the HTTPSCertFileName *ini* file parameter.

12.3 Viewing Certificate Information

You can view information of TLS certificates installed on the device for each TLS Context, as described in the following procedure.

➤ **To view certificate information:**

1. Open the TLS Contexts table (see "Configuring TLS Certificate Contexts" on page 99).

2. Select a TLS Context row, and then click the **Certificate Information** link located below the table; the Certificate Information page appears:

Figure 12-4: Viewing Certificate Information

PRIVATE KEY	
Key size:	1024 bits
Status:	OK

CERTIFICATE	
Certificate:	
Data:	
Version:	1 (0x0)
Serial Number:	0 (0x0)
Signature Algorithm:	sha1WithRSAEncryption
Issuer:	CN=ACL_5469038
Validity	
Not Before:	Aug 4 07:41:38 2015 GMT
Not After :	Jul 30 08:41:38 2035 GMT
Subject:	CN=ACL_5469038
Subject Public Key Info:	
Public Key Algorithm:	rsaEncryption
Public-Key:	(1024 bit)
Modulus:	
00:c0:67:ea:09:15:5e:96:3c:bb:be:b2:26:d9:e1:	
c9:f6:10:00:78:e3:c4:f2:d8:61:d1:d1:f0:8d:da:	
94:51:a8:e7:56:76:e3:88:ae:4a:8b:51:e8:ec:4a:	
b5:98:06:42:54:60:7d:c1:dd:eb:48:bd:70:2c:b0:	
74:e6:34:7f:b2:9f:85:f2:21:df:ec:3b:6d:a7:05:	
87:d4:23:aa:c0:33:ae:45:bc:be:e1:8b:c6:75:2a:	
cd:85:9f:8d:25:2f:33:a4:76:16:86:21:5d:60:3d:	
58:c9:9c:b2:2e:71:ee:f4:44:21:b9:78:47:6d:2d:	
eb:63:d5:57:3c:e9:30:d9:3b	
Exponent:	65537 (0x10001)
Signature Algorithm: sha1WithRSAEncryption	
9a:14:fb:54:70:90:57:f4:41:3f:db:9a:88:85:a6:d0:e4:b8:	
f9:8c:f8:55:17:19:f3:d3:b0:4c:09:d6:99:4c:02:93:f1:46:	
a0:c2:16:1e:7d:c6:0b:df:7d:4b:a6:5b:b5:89:b0:ad:4c:79:	
f6:4f:c0:55:ee:4f:7a:94:90:f4:0f:f6:8a:6b:2f:64:dd:8a:	
a7:ec:ce:7e:c5:bd:d3:56:82:d5:22:6e:a9:7f:1e:7f:fb:4d:	
86:f3:4e:07:de:b0:77:22:6c:9e:2c:5d:1a:d1:20:47:3e:72:	
f2:78:0a:20:3d:6f:c3:3c:5d:8a:22:e2:10:4d:1d:b3:30:5d:	
ea:c2	

12.4 Assigning Externally Created Private Keys to TLS Contexts

The following procedure describes how to assign an externally created private key to a TLS Context.

- **To assign an externally created private key to a TLS Context:**
 1. Obtain a private key in either textual PEM (PKCS #7) or PFX (PKCS #12) format (typically provided by your security administrator). The file may be encrypted with a short pass-phrase.
 2. Open the TLS Contexts table (see "Configuring TLS Certificate Contexts" on page 99).

3. In the table, select the required TLS Context index row, and then click the **Change Certificate** link located below the table; the Context Certificates page appears.
4. Scroll down to the **Upload Certificate Files From Your Computer** group:

Figure 12-5: Upload Certificate Files from your Computer Group

UPLOAD CERTIFICATE FILES FROM YOUR COMPUTER

Private key pass-phrase *(optional)*

Send **Private Key** file from your computer to the device.
The file must be in either PEM or PFX (PKCS#12) format.

No file selected.

Note: Replacing the private key is not recommended but if it's done, it should be over a physically-secure network link.

Send **Device Certificate** file from your computer to the device.
The file must be in textual PEM format.

No file selected.

5. Fill in the 'Private key pass-phrase' field, if required.
6. Click the **Browse** button corresponding to the 'Send Private Key file ...' text, navigate to the private key file (Step 1), and then click **Send File**.
7. If the security administrator has provided you with a device certificate file, load it using the **Browse** button corresponding to the 'Send Device Certificate file ...' text.
8. After the files successfully load to the device, save the configuration with a device reset.
9. Verify that the private key is correct:
 - a. Open the TLS Contexts table.
 - b. Select the required TLS Context index row.
 - c. Click the **Certificate Information** link located below the table.
 - d. Make sure that the 'Private key' field displays "OK"; otherwise, consult with your security administrator.

Figure 12-6: Verifying Private Key
Certificate Information

GENERAL

Certificate subject: /CN=ACL_5469038
 Certificate issuer: /CN=ACL_5469038
 Time to expiration: 7299 days
 Key size: 1024 bits
 Private key: OK

12.5 Generating Private Keys for TLS Contexts

You can let the device generate the private key for a TLS Context. The private key can be generated for CSR or self-signed certificates.

➤ **To generate a new private key for a TLS Context:**

1. Open the TLS Contexts table (see "Configuring TLS Certificate Contexts" on page

- 99).
2. In the table, select the required TLS Context index row, and then click the **Change Certificates** link located below the table; the Context Certificates page appears.
3. Scroll down to the **Generate New Private Key and Self-signed Certificate** group:

Figure 12-7: Generate new private key and self-signed certificate Group

GENERATE NEW PRIVATE KEY AND SELF-SIGNED CERTIFICATE

Private Key Size

Press the "Generate Private Key" button to create new private key.
 Press the "Generate Self-Signed Certificate" button to create self-signed certificate.
 Note that the certificate will use the subject name configured in "Certificate Signing Request" box.
Important: generation of private key is a lengthy operation during which the device service may be affected.

4. From the 'Private Key Size' drop-down list, select the desired private key size (in bits) for RSA public-key encryption for newly self-signed generated keys:
 - 512
 - 768
 - 1024 (default)
 - 2048
 - 4096
5. Click **Generate Private-Key**; a message appears requesting you to confirm key generation.
6. Click **OK** to confirm key generation; the device generates a new private key, indicated by a message in the **Certificate Signing Request** group.

Figure 12-8: Indication of Newly Generated Private Key

CERTIFICATE SIGNING REQUEST

Subject Name [CN]

Organizational Unit [OU] *(optional)*

Company name [O] *(optional)*

Locality or city name [L] *(optional)*

State [ST] *(optional)*

Country code [C] *(optional)*

Signature Algorithm

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

→ A new 512-bits Private-Key was generated for Context-ID=2
 Please save the configuration.

7. Continue with the certificate configuration by either creating a CSR or generating a new self-signed certificate.
8. Save the configuration with a device reset for the new certificate to take effect.

12.6 Creating Self-Signed Certificates for TLS Contexts

The following procedure describes how to assign a certificate that is digitally signed by the device itself to a TLS Context. In other words, the device acts as a CA.

➤ **To assign a self-signed certificate to a TLS Context:**

1. Before you begin, make sure of the following:
 - You have a unique DNS name for the device (e.g., dns_name.corp.customer.com). The name is used to access the device and therefore, must be listed in the server certificate.
 - No traffic is running on the device. The certificate generation process is disruptive to traffic and should be done during maintenance time.
2. Open the TLS Contexts table (see "Configuring TLS Certificate Contexts" on page 99).
3. In the table, select the required TLS Context index row, and then click the **Change Certificate** link located below the table; the Context Certificates page appears.
4. Under the **Certificate Signing Request** group, in the 'Subject Name [CN]' field, enter the fully-qualified DNS name (FQDN) as the certificate subject.
5. Scroll down the page to the **Generate New Private Key and Self-signed Certificate** group:

Figure 12-9: Generate new private key and self-signed certificate Group

GENERATE NEW PRIVATE KEY AND SELF-SIGNED CERTIFICATE

Private Key Size

512

Press the "Generate Private Key" button to create new private key.

Press the "Generate Self-Signed Certificate" button to create self-signed certificate.

Note that the certificate will use the subject name configured in "Certificate Signing Request" box.

Important: generation of private key is a lengthy operation during which the device service may be affected.

Generate Private-Key

Generate Self-Signed Certificate

6. Click **Generate Self-Signed Certificate**; a message appears requesting you to confirm generation.

- Click **OK** to confirm generation; the device generates a new self-signed certificate displaying the new subject name, indicated by a message in the **Certificate Signing Request** group:

Figure 12-10: Generated Self-Signed Certificate

CERTIFICATE SIGNING REQUEST

Subject Name [CN]	<input type="text" value="audio.com"/>
Organizational Unit [OU] <i>(optional)</i>	<input type="text" value="Headquarters"/>
Company name [O] <i>(optional)</i>	<input type="text" value="Corporate"/>
Locality or city name [L] <i>(optional)</i>	<input type="text" value="Poughkeepsie"/>
State [ST] <i>(optional)</i>	<input type="text" value="New York"/>
Country code [C] <i>(optional)</i>	<input type="text" value="US"/>
Signature Algorithm	<input type="text" value="SHA-1"/>

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

A new self-signed certificate was generated for Context-ID=3, with subject name: audio.com. Please save the configuration and restart the device.

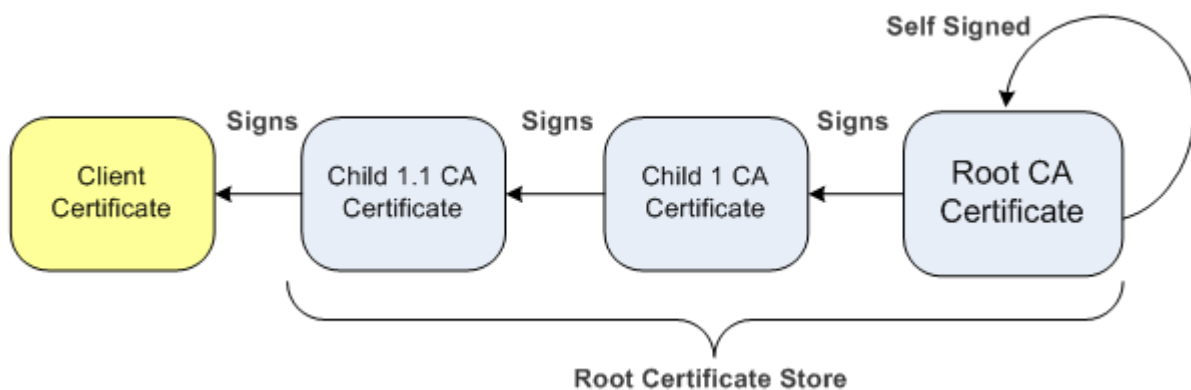
- Save the configuration with a device reset for the new certificate to take effect.

12.7 Importing Certificates and Certificate Chain into Trusted Certificate Store

The device provides its own Trusted Root Certificate Store. This lets you manage certificate trust. You can add up to 20 certificates to the store per TLS Context (but this may be less depending on certificate file size).

The trusted store can also be used for certificate chains. 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 12-11: Certificate Chain Hierarchy



For the device to trust a whole chain of certificates per TLS Context, you need to add them to the device's Trusted Certificates Store, as described below.

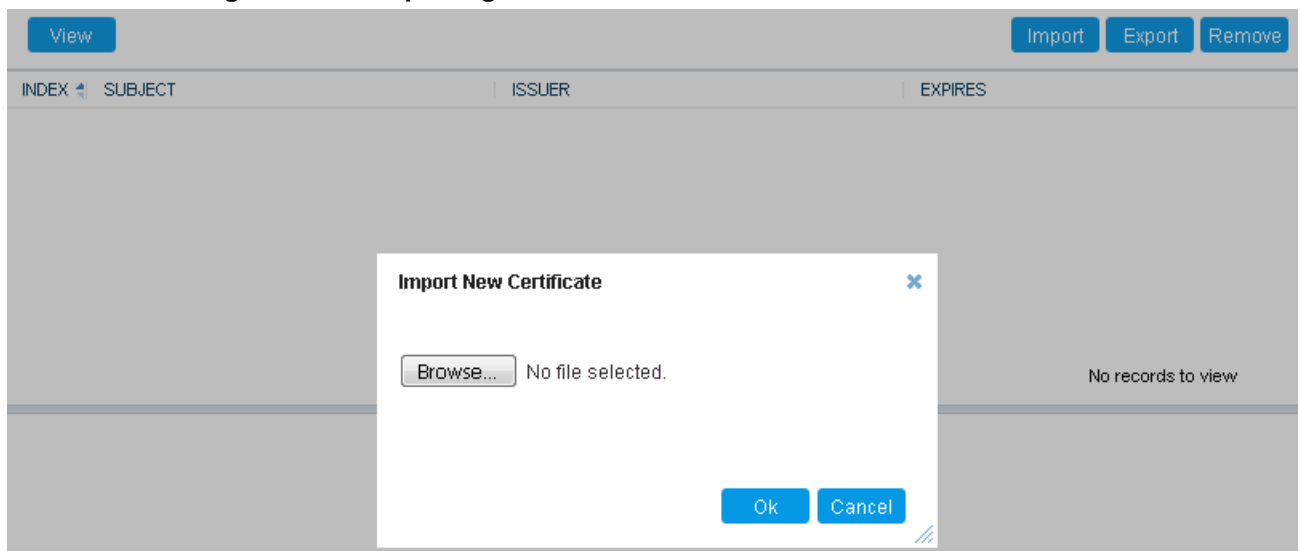


Note: Only Base64 (PEM) encoded X.509 certificates can be loaded to the device.

➤ **To import certificates into device's Trusted Root Certificate Store:**

1. Open the TLS Contexts table (see "Configuring TLS Certificate Contexts" on page 99).
2. In the table, select the required TLS Context index row, and then click the **Trusted Root Certificates** link located below the table; the Trusted Certificates table appears.
3. Click the **Import** button, and then browse to and select the certificate file.

Figure 12-12: Importing Certificate into Trusted Certificates Store



4. Click **OK**; the certificate is loaded to the device and listed in the Trusted Certificates store.

You can also do the following with certificates that are in the Trusted Certificates store:

- Delete certificates: Select the required certificate, click **Remove**, and then in the Remove Certificate dialog box, click **Remove**.
- Save certificates to a folder on your PC: Select the required certificate, click **Export**, and then in the Export Certificate dialog box, browse to the folder on your PC where you want to save the file and click **Export**.

12.8 Configuring Mutual TLS Authentication

This section describes how to configure mutual (two-way) TLS authentication.

12.8.1 TLS for SIP Clients

When Secure SIP (SIPS) is implemented using TLS, it is sometimes required to use two-way (mutual) authentication between the device and a SIP user agent (client). When the device acts as the TLS server in a specific connection, the device demands the

authentication of the SIP client's certificate. Both the device and the client use certificates from a CA to authenticate each other, sending their X.509 certificates to one another during the TLS handshake. Once the sender is verified, the receiver sends its' certificate to the sender for verification. SIP signaling starts when authentication of both sides completes successfully.

TLS mutual authentication can be configured for calls by enabling mutual authentication on the SIP Interface associated with the calls. The TLS Context associated with the SIP Interface or Proxy Set belonging to these calls are used.



Note: SIP mutual authentication can also be configured globally for all calls, using the 'TLS Mutual Authentication' (SIPSRequireClientCertificate) parameter (see "Configuring TLS for SIP" on page 162).

➤ **To configure mutual TLS authentication for SIP messaging:**

1. Enable two-way authentication on the specific SIP Interface:
 - a. In the SIP Interfaces table (see "Configuring SIP Interfaces" on page 321), configure the 'TLS Mutual Authentication' parameter to **Enable** for the specific SIP Interface.
 - b. Reset the device with a save-to-flash for your settings to take effect.
2. Configure a TLS Context with the following certificates:
 - Import the certificate of the CA that signed the certificate of the SIP client into the Trusted Certificates table (certificate root store) so that the device can authenticate the client (see "Importing Certificates and Certificate Chain into Trusted Certificate Store" on page 110).
 - Make sure that the TLS certificate is signed by a CA that the SIP client trusts so that the client can authenticate the device.

12.8.2 TLS for Remote Device Management

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 management PC and loading the root CA's certificate to the device's Trusted Certificates table (certificate root store). The Trusted Root Certificate file may contain more than one CA certificate combined, using a text editor.

➤ **To enable mutual TLS authentication for HTTPS:**

1. On the Web Settings page (see "Configuring Secured (HTTPS) Web" on page 68), configure the 'Secured Web Connection (HTTPS)' parameter to **HTTPS Only**. The setting ensures that you have a method for accessing the device in case the client certificate doesn't work. Restore the previous setting after testing the configuration.
2. In the TLS Contexts table (see "Configuring TLS Certificate Contexts" on page 99), select the required TLS Context row, and then click the **Trusted Root Certificates** link located below the table; the Trusted Certificates table appears.
3. Click the **Import** button, and then select the certificate file.
4. Wait until the import operation finishes successfully.
5. On the Web Settings page, configure the 'Require Client Certificates for HTTPS connection' parameter to **Enable**.
6. Reset the device with a save-to-flash for your settings to take effect.

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.



Note:

- 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 with your security administrator.
- The root certificate can also be loaded through the device's Automatic Provisioning mechanism, using the HTTPSRootFileName *ini* file parameter.
- You can enable the device to check whether a peer's certificate has been revoked by an OCSP server per TLS Context (see "Configuring TLS Certificate Contexts" on page 99).

12.9 Configuring TLS Server Certificate Expiry Check

You can configure the TLS Server Certificate Expiry Check feature per TLS Context, whereby the device periodically checks the validation date of installed TLS server certificates. You can also configure the device to send a notification SNMP trap event (acCertificateExpiryNotification) at a user-defined number of days before the installed TLS server certificate is to expire. The trap indicates the TLS Context to which the certificate belongs.

➤ **To configure TLS certificate expiry checks and notification:**

1. Open the TLS Contexts table (see "Configuring TLS Certificate Contexts" on page 99).
2. Select the required TLS Context index row, and then click the **Change Certificate** link located below the table; the Context Certificates page appears.
3. Scroll down the page to the **TLS Expiry Settings** group:

Figure 12-13: TLS Expiry Settings Group

TLS EXPIRY SETTINGS

TLS Expiry Check Start (days)	<input style="width: 90%;" type="text" value="60"/>
TLS Expiry Check Period (days)	<input style="width: 90%;" type="text" value="7"/>

4. In the 'TLS Expiry Check Start' field, enter the number of days before the installed TLS server certificate is to expire when the device sends an SNMP trap event to notify of this.
5. In the 'TLS Expiry Check Period' field, enter the periodical interval (in days) for checking the TLS server certificate expiry date. By default, the device checks the certificate every 7 days.
6. Click the **Submit TLS Expiry Settings** button.

13 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.

13.1 Configuring Automatic Date and Time using SNTP

The device's 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 device, as an 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. The NTP client follows a simple process in managing system time: 1) the NTP client requests an NTP update, 2) receives an NTP response and then 3) updates the local system clock based on an NTP server within the network. The client requests a time update from the user-defined NTP server (IP address or FQDN) at a user-defined update interval. Typically, the update interval is every 24 hours based on when the system was restarted.

You can also configure the device to authenticate and validate NTP messages received from the NTP server. Authentication is done using an authentication key with the MD5 cryptographic hash algorithm. When this feature is enabled, the device ignores NTP messages received without authentication.

The following procedure describes how to configure SNTP through the Web interface. For detailed descriptions of the configuration parameters, see "NTP and Daylight Saving Time Parameters" on page 755.

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

1. Open the Time & Date page (**Setup** menu > **Administration** tab > **Time & Date**), and then scroll down to the NTP Server group:

Figure 13-1: Configuring NTP Server

NTP SERVER	
Primary NTP Server Address (IP or FQDN)	• 0.0.0.0
Secondary NTP Server Address (IP or FQDN)	
NTP Update Interval	Hours: 24 Minutes: 0
NTP Authentication Key Identifier	0
NTP Authentication Secret Key	

2. Configure the NTP server address:
 - In the 'Primary NTP Server Address' (NTPServerIP) field, configure the primary NTP server's address (IP or FQDN).
 - (Optional) In the 'Secondary NTP Server Address' (NTPSecondaryServerIP) field, configure the backup NTP server.
3. In the 'NTP Updated Interval' (NTPUpdateInterval) field, configure the period after which the date and time of the device is updated.
4. Configure NTP message authentication:
 - In the 'NTP Authentication Key Identifier' field, configure the NTP authentication key identifier.
 - In the 'NTP Authentication Secret Key' field, configure the secret authentication key shared between the device and the NTP server.

- Verify that the device has received the correct date and time from the NTP server. The date and time is displayed in the 'UTC Time' read-only field under the Time Zone group.



Note: If the device does not receive a response from the NTP server, it polls the NTP server for 10 minutes. If there is still no response after this duration, the device declares the NTP server as unavailable and raises an SNMP alarm (acNTPServerStatusAlarm). The failed response could be due to incorrect configuration.

13.2 Configuring Date and Time Manually

You can manually configure the date and time of the device instead of using an NTP server (as described in "Configuring Automatic Date and Time using SNTP" on page 115).

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

- Open the Time & Date page (**Setup** menu > **Administration** tab > **Time & Date**), and then scroll down to the Local Time group:

Figure 13-2: Configuring Manual Date and Time

LOCAL TIME

Local Time

Year	Month	Day	Hours	Minutes	Seconds
2010	1	24	15	27	45

- Configure the current date and time of the geographical location in which the device is installed:
 - Date:
 - ◆ 'Year' in *yyyy* format (e.g., "2015")
 - ◆ 'Month' in *mm* format (e.g., "3" for March)
 - ◆ 'Day' in *dd* format (e.g., "27")
 - Time:
 - ◆ 'Hours' in 24-hour format (e.g., "4" for 4 am)
 - ◆ 'Minutes' in *mm* format (e.g., "57")
 - ◆ 'Seconds' in *ss* format (e.g., "45")
- Click **Apply**; the date and time is displayed in the 'UTC Time' read-only field.



Note:

- If the device is configured to obtain date and time from an NTP server, the fields under the Local Time group are read-only, displaying the date and time received from the NTP server.
- After performing a hardware reset, the date and time are returned to default values and thus, you should subsequently update the date and time.

13.3 Configuring the Time Zone

You can configure the time zone in which the device is deployed. This is referred to as the Coordinated Universal Time (UTC) time offset and defines how many hours the device is

from Greenwich Mean Time (GMT). For example, Germany Berlin is one hour ahead of GMT (UTC/GMT is +1 hour) and therefore, you would configure the offset to "1". USA New York is five hours behind GMT (UTC/GMT offset is -5 hours) and therefore, you would configure the offset as a minus value "-5".

➤ **To configure the time zone:**

1. Open the Time & Date page (**Setup** menu > **Administration** tab > **Time & Date**), and then scroll down to the Time Zone group:

Figure 13-3: Configuring UTC Offset

TIME ZONE	
UTC Time	24 Jan, 2010 15:27:45
UTC Offset	Hours: <input type="text" value="0"/> Minutes: <input type="text" value="0"/>

2. In the 'UTC Offset' fields (NTPServerUTCOffset), configure the time offset in relation to the UTC. For example, if your region is GMT +1 (an hour ahead), enter "1" in the 'Hours' field.
3. Click **Apply**; the updated time is displayed in the 'UTC Time' read-only field and the fields under the Local Time group.

13.4 Configuring Daylight Saving Time

You can apply daylight saving time (DST) to the date and time of the device. DST defines a date range in the year (summer) where the time is brought forward so that people can experience more daylight. DST applies an offset of up to 60 minutes (default) to the local time. For example, Germany Berlin has DST from 30 March to 26 October, where the time is brought forward by an hour (e.g., 02:00 to 03:00 on 30 March). Therefore, you would configure the DST offset to 60 minutes (one hour).

➤ **To configure DST through the Web interface:**

1. Open the Time & Date page (**Setup** menu > **Administration** tab > **Time & Date**), and then scroll down to the Time Zone group:

Figure 13-4: Configuring Daylight Savings

Day Light Saving Time	<input type="text" value="Disable"/>
DST Mode	<input type="text" value="Day of year"/>
Start Time	Jan <input type="text" value="01"/> <input type="text" value="0"/> : <input type="text" value="0"/>
End Time	Jan <input type="text" value="01"/> <input type="text" value="0"/> : <input type="text" value="0"/>
Offset [min]	<input type="text" value="60"/>
Day of Month Start	Jan <input type="text" value="Sunday"/> <input type="text" value="First"/> <input type="text" value="0"/> : <input type="text" value="0"/>
Day of Month End	Jan <input type="text" value="Sunday"/> <input type="text" value="First"/> <input type="text" value="0"/> : <input type="text" value="0"/>

2. From the 'Day Light Saving Time' (DayLightSavingTimeEnable) drop-down list, select **Enable**.
3. From the 'DST Mode' drop-down list, select the range type for configuring the start and end dates for DST:

- **Day of year:** The range is configured by exact date (day number of month), for example, from March 30 to October 30. If 'DST Mode' is set to **Day of year**, in the 'Start Time' (DayLightSavingTimeStart) and 'End Time' (DayLightSavingTimeEnd) drop-down lists, configure the period for which DST is relevant.
 - **Day of month:** The range is configured by month and day type, for example, from the last Sunday of March to the last Sunday of October. If 'DST Mode' is set to **Day of month**, in the 'Day of Month Start' and 'Day of Month End' drop-down lists, configure the period for which DST is relevant.
4. In the 'Offset' (DayLightSavingTimeOffset) field, configure the DST offset in minutes.
 5. If the current date falls within the DST period, verify that it has been successful applied to the device's current date and time. You can view the device's date and time in the 'UTC Time' read-only field.

Part IV

General VoIP Configuration


14 Network

This section describes network-related configuration.

14.1 Building and Viewing your Network Topology

The Network view lets you easily build and view your voice network topology entities, including IP network interfaces, Ethernet Devices (VLANs), Ethernet Groups, and physical Ethernet ports. The Topology view graphically displays these entities and the associations between them, giving you a better understanding of your network topology and configuration. You can use the Network view as an alternative to configuring the entities in their respective Web pages or you can use it in combination.

➤ **To access the Network view:**

- Click the Network View home  icon (**Setup** menu > **IP Network** tab > **Network View**).

The areas of the Network view is shown in the example below and described in the subsequent table.



Note: The below figure is used only as an example; your device may show different Ethernet Groups and Ethernet ports.

Figure 14-1: Network View (Example)

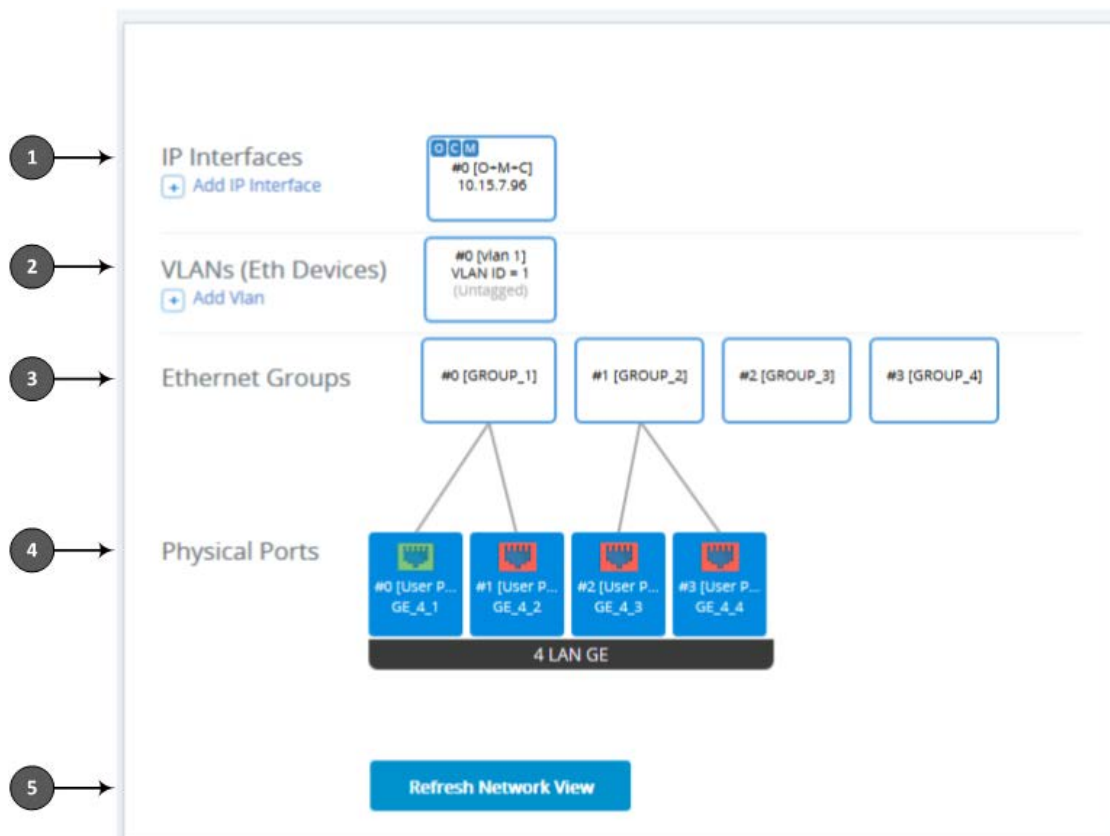

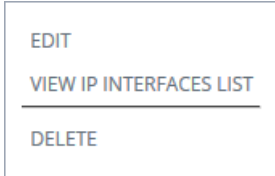


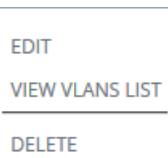






Table 14-1: Description of Network View

Item #	Description
<p>1</p>	<p>Configures and displays IP Interfaces.</p> <p>The IP Interface appears as an icon, displaying the application type ("OCM" for OAMP, "C" for Control, and "M" for Media), row index number, name, and IP address, as shown in the example below:</p>  <p>If you click the icon, a drop-down menu appears listing the following commands:</p>  <ul style="list-style-type: none"> ▪ Edit: Opens a dialog box in the IP Interfaces table to modify the IP Interface. ▪ View IP Interfaces List: Opens the IP Interfaces table, allowing you to configure IP Interfaces. ▪ Delete: Opens the IP Interfaces table where you are prompted to confirm deletion of the IP Interface. <p>To add an IP Interface:</p> <ol style="list-style-type: none"> 1 Click  Add IP Interface; the IP Interfaces table opens with a new dialog box for adding an IP Interface to the next available index row. 2 Configure the IP Interface as desired, and then click Apply; the IP Interfaces table closes and you are returned to the Network View, displaying the newly added IP Interface. <p>For more information on configuring IP Interfaces, see "Configuring IP Network Interfaces" on page 130.</p>
<p>2</p>	<p>Configures and displays Ethernet Devices.</p> <p>The Ethernet Device appears as an icon, displaying the row index number, name, VLAN ID and whether its tagged or untagged, as shown in the example below:</p>  <p>If you click the icon, a drop-down menu appears listing the following commands:</p>  <ul style="list-style-type: none"> ▪ Edit: Opens a dialog box in the Ethernet Devices table to modify the Ethernet Device. ▪ View VLANs List: Opens the Ethernet Devices table, allowing you to configure all Ethernet Devices. ▪ Delete: Opens the Ethernet Devices table where you are prompted to confirm deletion of the Ethernet Device. <p>To add an Ethernet Device:</p> <ol style="list-style-type: none"> 1 Click  Add VLAN; the Ethernet Devices table opens with a new dialog box for adding an Ethernet Device to the next available index row. 2 Configure the Ethernet Devices as desired, and then click Apply; the Ethernet Devices

Item #	Description
	<p>table closes and you are returned to the Network View, displaying the newly added Ethernet Device.</p> <p>For more information on configuring Ethernet Devices, see "Configuring Underlying Ethernet Devices" on page 128.</p>
3	<p>Configures and displays Ethernet Groups.</p> <p>The Ethernet Groups appear as icons, displaying the row index number and name, as shown in the example below:</p> <div data-bbox="790 544 935 640" style="text-align: center;"> </div> <p>Ethernet ports associated with Ethernet Groups are indicated by lines connecting between them, as shown in the example below:</p> <div data-bbox="600 719 1123 1048" style="text-align: center;"> </div> <p>To edit an Ethernet Group:</p> <ol style="list-style-type: none"> 1 Click the Ethernet Group icon, and then from the drop-down menu, choose Edit; the Ethernet Groups table opens with a dialog box for editing the Ethernet Group. 2 Configure the Ethernet Group as desired, and then click Apply; the Ethernet Groups table closes and you are returned to the Network View. <p>For more information on configuring IP Interfaces, see "Configuring Ethernet Port Groups" on page 126.</p> <p>To open the Ethernet Groups table, click any Ethernet Group icon, and then from the drop-down menu, choose View Ethernet Group List. You can then view and edit all the Ethernet Groups in the table.</p>

Item #	Description
4	<p>Configures and displays the device's Ethernet ports.</p> <p>To configure an Ethernet port:</p> <ol style="list-style-type: none"> 1 Click the required port icon, and then from the drop-down menu, choose Edit; the Physical Ports table opens with a dialog box for editing the Ethernet port. 2 Configure the Ethernet Port as desired, and then click Apply; the Physical Ports table closes and you are returned to the Network View. <p>For more information on configuring Ethernet ports, see "Configuring Underlying Ethernet Devices" on page 128.</p> <p>The Ethernet ports appear as icons, displaying the row index number, description, and port string number, as shown in the example below:</p> <div data-bbox="810 618 916 734" style="text-align: center;">  </div> <p>The connectivity status of the port is indicated by the color of the icon:</p> <ul style="list-style-type: none"> ▪  Green: Network connectivity exists through port (port connected to network). ▪  Red: No network connectivity through port (e.g., cable disconnected). <p>To refresh the status indication, click the Refresh Network View button (described below in Item #5).</p> <p>To open the Physical Ports table, click any port icon, and then from the drop-down menu, choose View Physical Port List. You can then view and edit all the ports in the table.</p>
5	<p>If you keep the Network view page open for a long time, you may want to click the Refresh Network View button to refresh the connectivity status display of the Ethernet ports.</p>

14.2 Configuring Physical Ethernet Ports

The Physical Ports table lets you configure the device's Ethernet ports. This includes configuring port speed and duplex mode (half or full), and a brief description of the port. The table also displays the status of the port as well as the port group (*Ethernet Group*) to which the port belongs. For more information on Ethernet Groups, see "Configuring Ethernet Port Groups" on page 126.

The names of the ports displayed in the device's management tools (e.g., Web interface) are different to the labels of the physical ports on the chassis. The figure below shows the mapping between the two:

You can also view the mapping of the ports, using the following CLI command:

```
# show network physical-port
```



Note: Each Ethernet port must have a unique VLAN ID in scenarios where the ports are connected to the same switch.

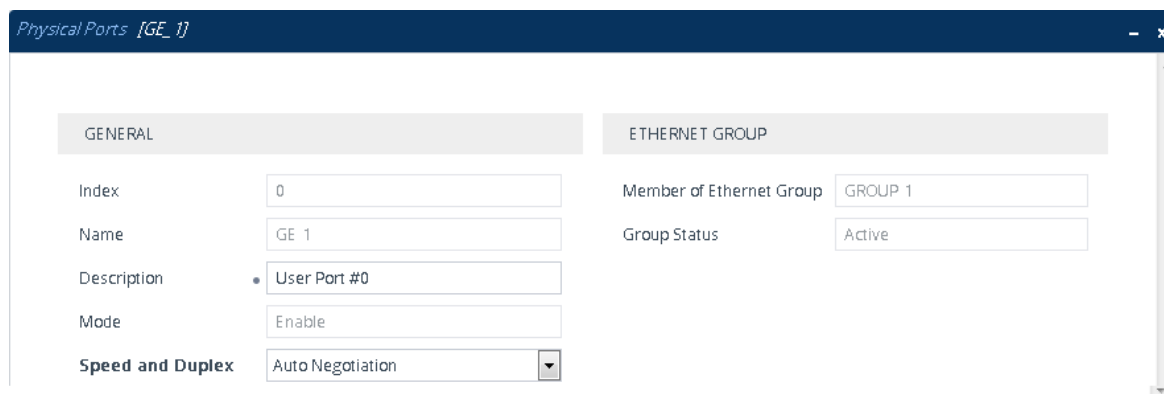
The following procedure describes how to configure Ethernet ports through the Web interface. You can also configure it through ini file (PhysicalPortsTable) or CLI (configure network > physical-port).

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

1. Open the Physical Ports table (**Setup** menu > **IP Network** tab > **Core Entities** folder >

Physical Ports).

2. Select a port that you want to configure, and then click **Edit**; the following dialog box appears:



3. Configure the port according to the parameters described in the table below.
4. Click **Apply**, and then save your settings to flash memory.

Table 14-2: Physical Ports Table Parameter Descriptions

Parameter	Description
General	
Index	(Read-only) Displays the index number for the table row.
Name port [PhysicalPortsTable_Port]	(Read-only) Displays the Ethernet port number. See the figure in the beginning of this section for the mapping between the GUI port number and the physical port on the chassis.
Description port-description [PhysicalPortsTable_PortDescription]	Defines a description of the port. By default, the value is "User Port #<row index>". Note: Each row must be configured with a unique name.
Mode mode [PhysicalPortsTable_Mode]	(Read-only) Displays the mode of the port. <ul style="list-style-type: none"> ▪ [0] Disable ▪ [1] Enable (default)
Speed and Duplex 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
Ethernet Group	
Member of Ethernet Group group-member [PhysicalPortsTable_GroupMember]	(Read-only) Displays the Ethernet Group to which the port belongs. To assign the port to a different Ethernet Group, see "Configuring Ethernet Port Groups" on page 126.
Group Status	(Read-only) Displays the status of the port:

Parameter	Description
group-status [PhysicalPortsTable_GroupStatus]	<ul style="list-style-type: none"> "Active": Active port. When the Ethernet Group includes two ports and their transmit/receive mode is configured to 2RX 1TX or 2RX 2TX, both ports show "Active".

14.3 Configuring Ethernet Port Groups

The Ethernet Groups table lets you configure Ethernet Groups. An Ethernet Group represents a physical Ethernet port(s) on the device. You can assign an Ethernet Group with one, two, or no ports (*members*). When two ports are assigned to an Ethernet Group, 1+1 Ethernet port redundancy can be implemented in your network. This provides port redundancy within the Ethernet Group, whereby if a port is disconnected the device switches over to the other port in the Ethernet Group. If you configure an Ethernet Group with only one port, the Ethernet Group operates as a single port (no redundancy).

The Ethernet Groups table also lets you configure the transmit (Tx) and receive (Rx) settings of the Ethernet ports per Ethernet Group. The Tx/Rx setting is applicable only to Ethernet Groups that contain two ports. This setting determines whether either both ports or only one of the ports can receive and/or transmit traffic.

The maximum number of Ethernet Groups that you can configure is the same as the number of Ethernet ports provided by the device. Thus, the device supports up to 12 Ethernet Groups where each contains one port, or 6 Ethernet Groups where each contain two ports. By default, each Ethernet Group is assigned one port.

You can assign Ethernet ports to IP network interfaces. This is done by first configuring an Ethernet Device with the required Ethernet Group containing the port or ports (see "Configuring Underlying Ethernet Devices" on page 128). Then by assigning the Ethernet Device to the IP network interface in the IP Interfaces table (see "Configuring IP Network Interfaces" on page 130). 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 (VoIP calls).

The following procedure describes how to configure Ethernet Groups through the Web interface. You can also configure it through ini file (EtherGroupTable) or CLI (configure network > ether-group).

Note:

- If you want to assign a port to a different Ethernet Group, you must first remove the port from its current Ethernet Group. To remove the port, configure the 'Member' field so that no port is selected or select a different port.
- When implementing 1+1 Ethernet port redundancy, each port in the Ethernet Group (port pair) must be connected to a different switch (but in the same subnet).
- For Mediant Virtual Edition (VE), Ethernet port redundancy is not relevant as the virtual NIC ("port") is logical and always available. Therefore, it is sufficient to configure the Ethernet Group with only one port member. To employ Ethernet port redundancy, you need to configure the virtual switch of the hypervisor for Ethernet port redundancy (or bonding) with the physical NICs. Refer to your hypervisor's support material on how to do this.



➤ To configure Ethernet Groups:

1. Open the Ethernet Groups table (**Setup** menu > **IP Network** tab > **Core Entities**

folder > **Ethernet Groups**).

2. Select the Ethernet Group that you want to configure, and then click **Edit**; the following dialog box appears:

The screenshot shows a configuration window for an Ethernet Group. The window title is "Ethernet Groups [GROUP_1]". Under the "GENERAL" tab, the following fields are visible:

- Index:** 0
- Name:** GROUP 1
- Mode:** Single (selected from a dropdown menu)
- Member 1:** #0 [GE_1] (with a "View" link)
- Member 2:** -- (with a "View" link)

3. Configure the Ethernet Group according to the parameters described in the table below.
4. Click **Apply**, and then save your settings to flash memory.

Table 14-3: Ethernet Groups Table Parameter Descriptions

Parameter	Description
Index	(Read-only) Displays the index number for the table row.
Name group [EtherGroupTable_Group]	(Read-only) Displays the Ethernet Group number.
Mode mode [EtherGroupTable_Mode]	<p>Defines the mode of operation of the ports in the Ethernet Group. This applies only to Ethernet Groups containing two ports.</p> <ul style="list-style-type: none"> ▪ [3] 2RX/1TX = Both ports in the Ethernet 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 and receive. ▪ [4] 2RX/2TX = Both ports in the Ethernet Group can receive and transmit packets. This option is applicable only to the Maintenance interface for High Availability (HA) deployments. For more information, see Network Topology Types and Rx/Tx Ethernet Port Group Settings on page 561. ▪ [5] Single = (Default) Select this option if the Ethernet Group contains only one port. ▪ [6] None = Select this option to remove all ports from the Ethernet Group. <p>Note:</p> <ul style="list-style-type: none"> ▪ It is recommended to use the 2RX/1TX option. 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. ▪ For Ethernet Group settings for the Maintenance interface when implementing High Availability, see Initial HA Configuration on page 561.
Member 1	Assigns the first port to the Ethernet Group. To assign no port, set this

Parameter	Description
member1 [EtherGroupTable_Member1]	field to None . Note: Before you can re-assign a port to a different Ethernet Group, you must first remove the port from its current Ethernet Group. To remove the port, either set this field to None or to a different port.
Member 2 member2 [EtherGroupTable_Member2]	Assigns the second port to the Ethernet Group. To assign no port, set this field to None . Note: Before you can re-assign a port to a different Ethernet Group, you must first remove the port from its current Ethernet Group. To remove the port, either set this field to None or to a different port.

14.4 Configuring Underlying Ethernet Devices

The Ethernet Devices table lets you configure up to 1,024 *Ethernet Devices*. An Ethernet Device represents a Layer-2 bridging device and is assigned a VLAN ID and an Ethernet Group (Ethernet port group). Multiple Ethernet Devices can be associated with the same Ethernet Group. The Ethernet Device (VLAN) can be configured with a VLAN tagging policy, which determines whether the Ethernet Device accepts tagged or untagged packets received on the Ethernet port associated with the Ethernet Device.

Once configured, assign the Ethernet Device to an IP network interface in the IP Interfaces table ('Underlying Device' field) and/or with a static route in the Static Routes table ('Device Name' field). You can assign the same Ethernet Device to multiple IP network interfaces and thereby, implement multi-homing (multiple addresses on the same interface/VLAN).

By default, the device provides a pre-configured Ethernet Device at Index 0 with the following settings:

- Name: "vlan 1"
- VLAN ID: 1
- Ethernet Group: GROUP 1
- Tagging Policy: Untagged

The pre-configured Ethernet Device is associated with the default IP network interface (ie., OAMP) in the IP Interfaces table. The Untagged policy of the pre-configured Ethernet Device enables you to connect to the device using the default OAMP interface.

You can view configured Ethernet Devices that have been successfully applied to the device (saved to flash) in the Ethernet Device Status table. This page is accessed by clicking the **Ethernet Device Status Table** button located at the bottom of the Ethernet Devices table. The Ethernet Device Status table can also be accessed from the Navigation tree (see "Viewing Ethernet Device Status" on page 663).



Note: You cannot delete an Ethernet Device that is associated with an IP network interface (in the IP Interfaces table). You can only delete it once you have disassociated it from the IP network interface.

The following procedure describes how to configure Ethernet Devices through the Web interface. You can also configure it through ini file (DeviceTable) or CLI (configure network > network-dev).

➤ To configure an Ethernet Device:

1. Open the Ethernet Devices table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **Ethernet Devices**).

2. Click **New**; the following dialog box appears:

3. Configure an Ethernet Device according to the parameters described in the table below.
4. Click **Apply**.

Table 14-4: Ethernet Devices Table Parameter Descriptions

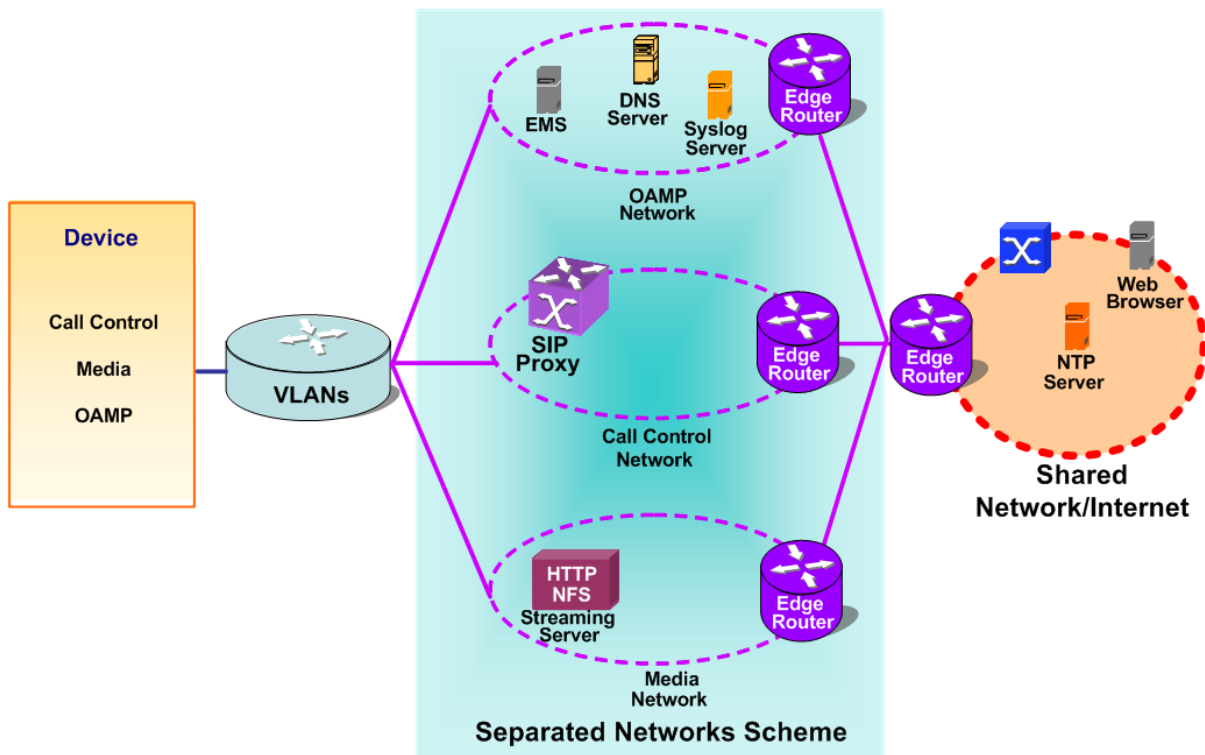
Parameter	Description
Index [DeviceTable_Index]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
Name name [DeviceTable_DeviceName]	Defines a name for the Ethernet Device. The name is used to associate the Ethernet Device with an IP network interface in the IP Interfaces table ('Underlying Device' field - see "Configuring IP Network Interfaces" on page 130) and/or with a static route in the Static Routes table ('Device Name' field - see "Configuring Static IP Routing" on page 138).
VLAN ID vlan-id [DeviceTable_VlanID]	Defines a VLAN ID for the Ethernet Device. The valid value is 1 to 3999. The default is 1. Note: Each Ethernet Device must have a unique VLAN ID.
Underlying Interface underlying-if [DeviceTable_UnderlyingInterface]	Assigns an Ethernet Group to the Ethernet Device. To configure Ethernet Groups, see Configuring Ethernet Port Groups on page 126. Note: The parameter is mandatory.
Tagging tagging [DeviceTable_Tagging]	Defines VLAN tagging for the Ethernet Device. <ul style="list-style-type: none"> ▪ [0] Untagged = (Default for pre-configured Ethernet Device) The Ethernet Device accepts untagged packets and packets with the same VLAN ID as the Ethernet Device. Incoming untagged packets are assigned the VLAN ID of the Ethernet Device. The Ethernet Device sends these VLAN packets untagged (i.e., removes the VLAN ID). ▪ [1] Tagged = (Default for new Ethernet Devices) The Ethernet Device accepts packets that have the same VLAN ID as the Ethernet Device and sends packets with this VLAN ID. For all Ethernet Devices that are associated with the same Ethernet Group (see 'Underlying Interface' parameter above) and configured to Tagged, incoming untagged packets received

Parameter	Description
	<p>on this Ethernet Group are discarded.</p> <p>Note: Only one Ethernet Device can be configured as Untagged per associated Ethernet Group. In other words, if multiple Ethernet Devices are associated with the same Ethernet Group, only one of these Ethernet Devices can be configured to Untagged; all the others must be configured to Tagged.</p>

14.5 Configuring IP Network Interfaces

You can configure a single VoIP network interface for all applications, including OAMP (management traffic), call control (SIP signaling messages), and media (RTP traffic), or you can configure multiple logical, IP network interfaces for these applications. You may need to 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, each representing 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 14-2: Multiple Network Interfaces



The device is shipped with a default OAMP interface (see "Default OAMP IP Address" on page 31). The IP Interfaces table lets you change this OAMP interface and configure additional network interfaces for control and media, if necessary. You can configure up to 1,024 interfaces, consisting of up to 1,023 Control and Media interfaces including a Maintenance interface if your device is deployed in a High Availability (HA) mode, and 1 OAMP interface. Each IP interface is configured with the following:

- Application type allowed on the interface:

- Control: call control signaling traffic (i.e., SIP)
 - Media: RTP traffic
 - Operations, Administration, Maintenance and Provisioning (OAMP): management (i.e., Web, CLI, and SNMP based management)
 - Maintenance: This interface is used in HA mode when two devices are deployed for redundancy, and represents one of the LAN interfaces or Ethernet Groups on each device used for the Ethernet connectivity between the two devices. For more information on HA and the Maintenance interface, see [Configuring High Availability](#) on page 553.
- IP address (IPv4 or IPv6) and subnet mask (prefix length)
 - To configure Quality of Service (QoS), see ["Configuring the QoS Settings"](#) on page 148.
 - Default Gateway: Traffic from this interface destined to a subnet that does not meet any of the routing rules (local or static) are forwarded to this gateway
 - (Optional) Primary and secondary domain name server (DNS) addresses for resolving FQDNs into IP addresses.
 - Ethernet Device: Layer-2 bridging device and assigned a VLAN ID. As the Ethernet Device is associated with an Ethernet Group, this is useful for setting trusted and untrusted networks on different physical Ethernet ports. Multiple entries in the IP Interfaces table may be associated with the same Ethernet Device, providing multi-homing IP configuration (i.e., multiple IP addresses on the same interface/VLAN).

Complementing the IP Interfaces table is the Static Routes table, which lets you configure static routing rules for non-local hosts/subnets. For more information, see ["Configuring Static IP Routing"](#) on page 138.



Note: Before configuring IP interfaces, it is recommended that you read the IP interface configuration guidelines in ["IP Interfaces Table Configuration Guidelines"](#) on page 134.

The following procedure describes how to configure IP network interfaces through the Web interface. You can also configure it through ini file (InterfaceTable) or CLI (`configure network > interface network-if`).

➤ **To configure IP network interfaces:**

1. Open the IP Interfaces table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **IP Interfaces**).

- Click **New**; the following dialog box appears:

Figure 14-3: IP Interfaces Table - Dialog Box

- Configure the IP network interface according to the parameters described in the table below.
- Click **Apply**.



Note:

- If you edit or delete an IP interface, current calls using the interface are immediately terminated.
- If you delete an IP interface, row indices of other tables (e.g., Media Realms table) that are associated with the deleted IP interface, lose their association with the interface ('Interface Name' field displays "None") and the row indices become invalid.
- When editing or deleting the Maintenance interface for HA mode, you must reset the device for your changes to take effect.

To view configured IP network interfaces that are currently active, click the **IP Interface Status Table** link located at the bottom of the table. For more information, see "Viewing Active IP Interfaces" on page 663.

Table 14-5: IP Interfaces Table Parameters Description

Parameter	Description
General	
Index network-if [InterfaceTable_Index]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
Name name [InterfaceTable_InterfaceName]	Defines a name for the interface. The valid value is a string of up to 16 characters. If you do not configure a name, the device automatically assigns the name using the syntax "InterfaceTable_<row index>". For example, if you add a new interface to row index 2, the name is "InterfaceName_2". The name of the default OAMP interface is "O+M+C+P". Note: Each row must be configured with a unique name.
Application Type	Defines the applications allowed on the IP interface.

Parameter	Description
application-type [InterfaceTable_ApplicationTypes]	<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.
Ethernet Device underlying-dev [InterfaceTable_UnderlyingDevice]	Assigns an Ethernet Device to the IP interface. An Ethernet Device is a VLAN associated with a physical Ethernet port (Ethernet Group). To configure Ethernet Devices, see Configuring Underlying Ethernet Devices on page 128. By default, no value is defined. Note: The parameter is mandatory.
IP Address	
Interface Mode mode [InterfaceTable_InterfaceMode]	Defines the method that the interface uses to acquire its IP address. <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 = (Default) IPv4 manual IP address (32 bits) assignment.
IP Address ip-address [InterfaceTable_IPAddress]	Defines the IPv4/IPv6 address in dotted-decimal notation. By default, no value is defined. Note: The parameter is mandatory.
Prefix Length prefix-length [InterfaceTable_PrefixLength]	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). 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 blocks, it uses the

Parameter	Description
	variable-length subnet masking technique to allow allocation on arbitrary-length prefixes. The prefix length for IPv4 must be set to a value from 0 to 30. The prefix length for IPv6 must be set to a value from 0 to 64. The default is 16.
Default Gateway gateway [InterfaceTable_Gateway]	Defines the IP address of the default gateway for the IP 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. By default, no value is defined.
DNS	
Primary DNS primary-dns [InterfaceTable_PrimaryDNSServerIPAddress]	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. By default, no IP address is defined.
Secondary DNS secondary-dns [InterfaceTable_SecondaryDNSServerIPAddress]	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. By default, no IP address is defined.

14.5.1 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. For more information on NTP, see "Configuring Automatic Date and Time using SNTP" on page 115.

14.5.2 IP Interfaces Table Configuration Guidelines

Adhere to the following guidelines when configuring network interfaces in the IP Interfaces table:

- 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 0-64 for IPv6 addresses.
- **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.
- At least one Media interface **must** be configured.
- Multiple 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
 - 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

- Example 3:
 - ◆ One OAMP with an IPv4 address
 - ◆ One combined Media-Control interface with IPv4 address
 - ◆ One combined Media-Control interface with IPv6 address
- 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 Static Routes table.
- The interface name **must** be configured (mandatory) and must be unique for each interface.
- Each network interface must be assigned an Ethernet Device.
- For IPv4 addresses, the 'Interface Mode' column must be set to IPv4 Manual. For IPv6 addresses, this column must be set to IPv6 Manual or IPv6 Manual Prefix.



Note: Upon device start up, the IP Interfaces 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 without VLANs. Ensure that you view the Syslog messages that the device sends in system startup to see if any errors occurred.

14.5.3 Networking Configuration Examples

This section provides configuration examples of networking interfaces.

14.5.3.1 One VoIP Interface for All Applications

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

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

Table 14-6: Example of Single VoIP Interface in IP Interfaces table

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

2. **Static Routes 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 14-7: Example of Static Routes Table

Destination	Prefix Length	Gateway
201.201.0.0	16	192.168.11.10
202.202.0.0	16	192.168.11.1

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

14.5.3.2 VoIP Interface per Application Type

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

1. **IP Interfaces 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 14-8: Example of VoIP Interfaces per Application Type in IP Interfaces table

Index	Application Type	Interface Mode	IP Address	Prefix Length	Default Gateway	Ethernet Device	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. **Static Routes table:** A routing rule is required to allow remote management from a host in 176.85.49.0 / 24:

Table 14-9: Example Static Routes Table

Destination	Prefix Length	Gateway
176.85.49.0	24	192.168.11.1

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

14.5.3.3 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. **IP Interfaces table:**

Table 14-10: Example of VoIP Interfaces of Combined Application Types in IP Interfaces table

Index	Application Type	Interface Mode	IP Address	Prefix Length	Default Gateway	Ethernet Device	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 &	IPv6	2000::1:200:200:86:1	64	::	202	V6CntrlMedia

Index	Application Type	Interface Mode	IP Address	Prefix Length	Default Gateway	Ethernet Device	Name
	Control	Manual	4				2

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

Table 14-11: Example of Static Routes Table

Destination	Prefix Length	Gateway
176.85.49.0	24	192.168.0.10

3. The NTP application is configured (through 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

14.5.3.4 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 14-12: Configured Default Gateway Example

Index	Application Type	Interface Mode	IP Address	Prefix Length	Default Gateway	Ethernet Device	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 Static Routes table lets you 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 14-13: Separate Static Routes Table Example

Destination	Prefix Length	Gateway	Underlying Device
17.17.0.0	16	192.168.10.1	100
171.79.39.0	24	200.200.85.10	200

14.6 Configuring Static IP Routes

The Static Routes table lets you configure up to 30 static IP routing rules. Static routes let you communicate with LAN networks that are not located behind the Default Gateway that is specified for an IP network interface in the IP Interfaces table, from which the packets are sent. Before sending an IP packet, the device searches the Static Routes table for an entry that matches the requested destination host/network. If an entry is found, the device sends the packet to the gateway that is configured for the static route. If no explicit entry is found, the packet is sent to the Default Gateway as configured for the IP interface in the IP Interfaces table.

You can view the status of configured static routes in the IP Routing Status table. This table can be accessed by clicking the **Static Routes Status Table** link located at the bottom of the Static Routes table (see "Viewing Static Routes Status" on page 664).

The following procedure describes how to configure static routes through the Web interface. You can also configure it through ini file (StaticRouteTable) or CLI (configure network > static).

➤ **To configure static IP routes:**

1. Open the Static Routes table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **Static Routes**).
2. Click **New**; the following dialog box appears:

The screenshot shows a configuration window titled "Static Routes". It has a "GENERAL" tab selected. The fields are as follows:

- Index:** 1
- Destination:** 0.0.0.0
- Prefix Length:** 16
- Ethernet Output Device:** Unknown
- Gateway:** 0.0.0.0
- Description:** (empty text box)

3. Configure a static route according to the parameters described in the table below. The address of the host/network you want to reach is determined by an AND operation that is applied to the fields 'Destination' and 'Prefix Length'. For example, to reach network 10.8.x.x, enter "10.8.0.0" in the 'Destination' field and "16" in the 'Prefix Length'. As a result of the AND operation, the value of the last two octets in the 'Destination' field are ignored. To reach a specific host, enter its IP address in the 'Destination' field and "32" in the 'Prefix Length' field.

- Click **Apply**, and then reset the device with a save-to-flash for your settings to take effect.



Note: Only static routing rules that are inactive can be deleted.

Table 14-14: Static Routes Table Parameter Descriptions

Parameter	Description
Index [StaticRouteTable_Index]	Defines an index number for the new table row. The valid value is 0 to 29. Note: Each row must be configured with a unique index.
Description description [StaticRouteTable_Description]	Defines a name for the rule. The valid value is a string of up to 20 characters.
Destination destination [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 prefix-length [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, the value 16 represents subnet 255.255.0.0. The value must be 0 to 31 for IPv4 interfaces and a value of 0 to 64 for IPv6 interfaces.
Ethernet Output Name device-name [StaticRouteTable_DeviceName]	Associates an IP network interface through which the static route's Gateway is reached. The association is done by assigning the parameter the same Ethernet Device that is assigned to the IP network interface in the IP Interfaces table ('Ethernet Device' parameter). To configure IP network interface, see Configuring IP Network Interfaces on page 130. To configure Ethernet Devices, see Configuring Underlying Ethernet Devices on page 128.
Gateway gateway [StaticRouteTable_Gateway]	Defines the IP address of the Gateway (next hop) used for traffic destined to the subnet/host defined in the 'Destination' / 'Prefix Length' field. Note: <ul style="list-style-type: none"> The Gateway's address must be in the same subnet as the IP address of the network interface that is associated with the static route (using the 'Device Name' parameter - see above). The IP network interface associated with the static route must be of the same IP address family (IPv4 or IPv6).

14.6.1 Configuration Example of Static IP Routes

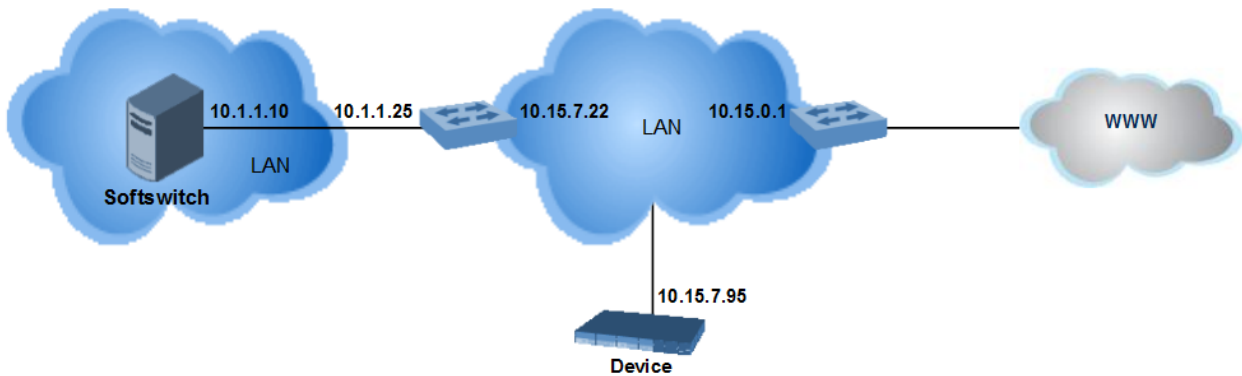
An example of the use for static routes is shown in the figure below. In the example, the device needs to communicate with a softswitch at IP address 10.1.1.10. However, the IP network interface from which packets destined for 10.1.1.10 is sent, is configured to send

the packets to a Default Gateway at 10.15.0.1. Therefore, the packets do not reach the softswitch. To resolve this problem, a static route is configured to specify the correct gateway (10.15.7.22) in order to reach the softswitch.

Note the following configuration:

- The static route is configured with a subnet mask of 24 (255.255.255.0), enabling the device to use the static route to send all packets destined for 10.1.1.x to this gateway and therefore, to the network in which the softswitch resides.
- The static route in the Static Routes table must be associated with the IP network interface in the IP Interfaces table. This is done by configuring the 'Ethernet Output Name' field in the Static Routes table to the same value as configured in the 'Ethernet Device' field in the IP Interfaces table.
- The static route's Gateway address in the Static Routes table is in the same subnet as the IP address of the IP network interface in the IP Interfaces table.

Figure 14-4: Example of using a Static Route



No Static Route:

The device sends packets to 10.15.0.1, which is the Default Gateway defined for this IP network interface in the IP Interfaces table. Therefore, the device will not succeed in reaching the softswitch.

INDEX	NAME	APPLICATION TYPE	INTERFACE MODE	IP ADDRESS	PREFIX LENGTH	DEFAULT GATEWAY	PRIMARY DNS	SECONDARY DNS	ETHERNET DEVICE
0	O+M+C	OAMP + Media	IPv4 Manual	10.15.7.95	16	10.15.0.1	0.0.0.0	0.0.0.0	vlan 1

Static Route Configured:

A static route with the correct gateway is needed for routing to the softswitch. The device communicates with the softswitch (10.1.1.0/24) using the gateway 10.15.7.22. Note that the device first searches for a matching route in the Static Routes table. If not found, it uses the default gateway defined in the IP Interfaces table.

INDEX	DESTINATION	PREFIX LENGTH	ETHERNET OUTPUT DEVICE	GATEWAY	DESCRIPTION
0	10.1.1.0	24	vlan 1	10.15.7.22	Softswitch

14.6.2 Troubleshooting the Static Routes Table

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

Common static routing configuration errors may include the following:

- The IP address specified in the 'Gateway' field is unreachable from the IP network interface associated with the static route.
- The same destination has been configured in two different static routing rules.
- More than 30 static routes have been configured.



Note: If a static route 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.

14.7 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.

14.7.1 Device Located behind NAT

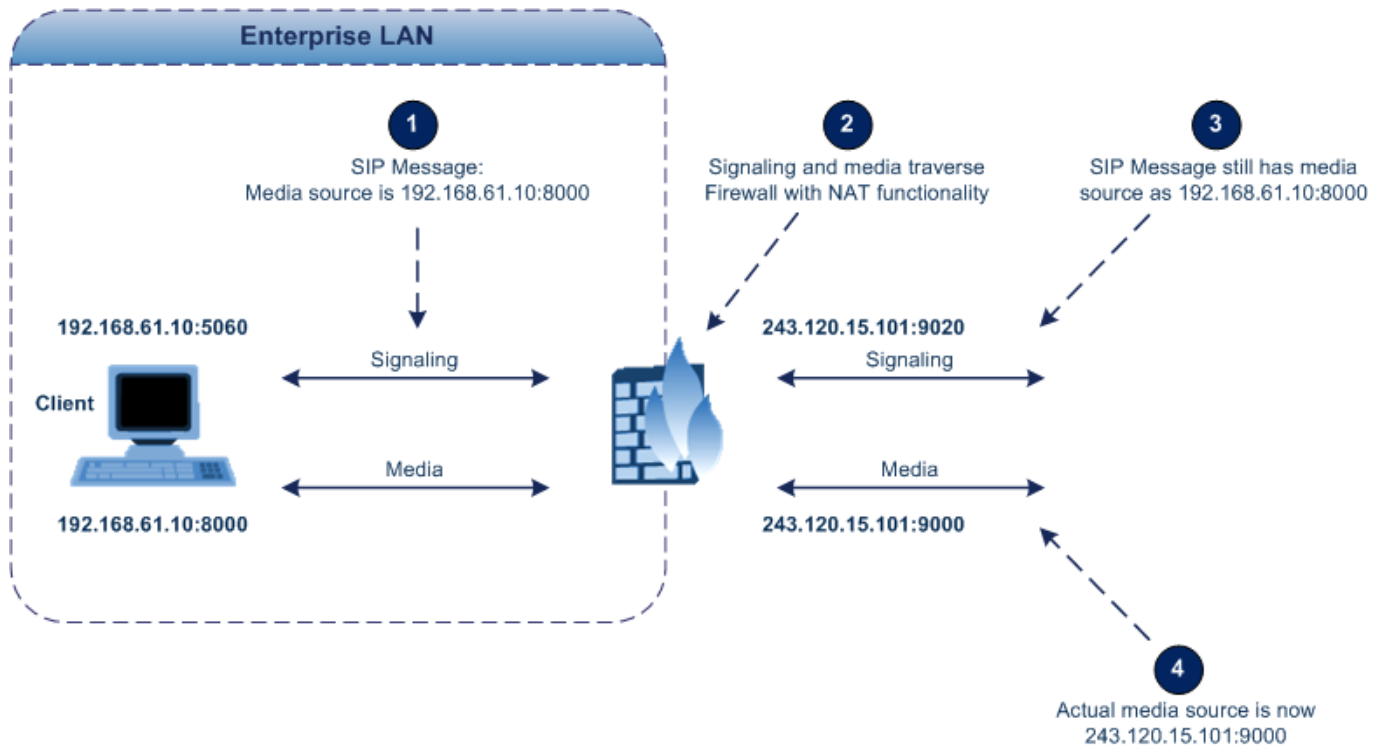
Two different streams traverse through NAT: signaling and media. A device located behind a NAT that initiates a signaling path has problems receiving incoming signaling responses as they are blocked by the NAT server. Therefore, the initiating device must inform the receiving device where to send the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

1. If configured, uses the NAT Translation table which configures NAT per IP network interface - see Configuring NAT Translation per IP Interface on page 142.

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 IP Interfaces table.

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

Figure 14-5: Device behind NAT and NAT Issues



14.7.1.1 Configuring NAT Translation per IP Interface

The NAT Translation table lets you configure up to 32 network address translation (NAT) rules for translating source IP addresses per VoIP interface (SIP control and RTP media traffic) into NAT IP addresses (*global - public*) when the device is located behind NAT. 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. This allows, for example, the separation of VoIP traffic between different ITSPs and topology hiding of internal IP addresses from the “public” network. Each IP network interface, configured in the IP Interfaces table can be associated with a NAT rule, translating the source IP address and port of the outgoing packet into the NAT address (IP address and port range).

The following procedure describes how to configure NAT translation rules through the Web interface. You can also configure it through ini file (NATtranslation) or CLI (configure network > nat-translation).

➤ **To configure NAT translation rules:**

1. Open the NAT Translation table (**Setup** menu > **IP Network** tab > **Core Entities** folder > **NAT Translation**).

- Click **New**; the following dialog box appears:

Figure 14-6: NAT Translation Table - Dialog Box

- Configure a NAT translation rule according to the parameters described in the table below.
- Click **Apply**, and then save your settings to flash memory.

Table 14-15: NAT Translation Table Parameter Descriptions

Parameter	Description
Source	
Index index [NATTranslation_Index]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
Source Interface src-interface-name [NATTranslation_SrcInterfaceName]	Assigns an IP network interface (configured in the IP Interfaces table) to the rule. Outgoing packets sent from the specified network interface are NAT'ed. By default, no value is defined. To configure IP network interfaces, see "Configuring IP Network Interfaces" on page 130.
Source Start Port src-start-port [NATTranslation_SourceStartPort]	Defines the optional starting port range (1-65536) of the IP interface, used as matching criteria for the 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 src-end-port [NATTranslation_SourceEndPort]	Defines the optional ending port range (1-65536) of the IP interface, used as matching criteria for the 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	
Target IP Address target-ip-address [NATTranslation_TargetIPAddress]	Defines the global (public) IP address. The device adds the address in the outgoing packet to the SIP Via header, Contact header, 'o=' SDP field, and 'c=' SDP field.
Target Start Port target-start-port [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 and in the 'o=' and 'c=' SDP fields.

Parameter	Description
Target End Port target-end-port [NATTranslation_TargetEndPort]	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 and in the 'o=' and 'c=' SDP fields.

14.7.2 Remote UA behind NAT

This section describes configuration for scenarios where the device sends signaling and media packets to a remote UA that is located behind NAT.

14.7.2.1 SIP Signaling Messages

By default, the device resolves NAT issues for SIP signaling, using its NAT Detection mechanism. The NAT Detection mechanism checks whether the endpoint is located behind NAT by comparing the incoming packet's source IP address with the SIP Contact header's IP address. If the packet's source IP address is a public address and the Contact header's IP address is a local address, the device considers the endpoint as located behind NAT. In this case, the device sends the SIP messages to the endpoint using the packet's source IP address. Otherwise (or if you have disabled the NAT Detection mechanism), the device sends the SIP messages according to the SIP standard (RFC 3261), where requests within the SIP dialog are sent using the IP address in the Contact header, and responses to INVITEs are sent using the IP address in the Via header.

If necessary, you can also configure the device to always consider incoming SIP INVITE messages as sent from endpoints that are located behind NAT. When this is enabled, the device sends responses to the INVITE (to the endpoint), using the the source IP address of the packet (INVITE) initially received from the endpoint. This is useful in scenarios where the endpoint is located behind a NAT firewall and the device (for whatever reason) is unable to identify NAT using its regular NAT Detection mechanism. This feature is enabled per specific calls using IP Groups. To configure this feature, use the 'Always Use Source Address' parameter in the IP Groups table (see "Configuring IP Groups" on page 329). If this feature is disabled, the device's NAT detection is according to the settings of the global parameter, 'SIP NAT Detection' parameter (see below procedure).

- **To enable the NAT Detection feature (global):**
- 1. Open the Transport Settings page (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Transport Settings**).
- 2. From the 'SIP NAT Detection' drop-down list (SIPNatDetection), select **Enable**:

Figure 14-7: Enabling SIP NAT Detection



- 3. Click **Apply**.

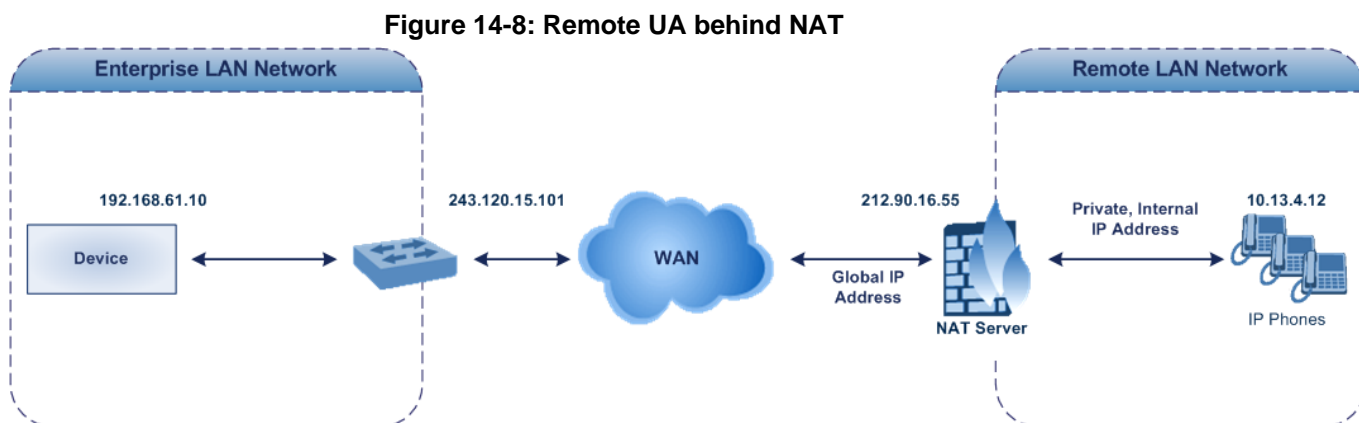
14.7.2.2 Media (RTP/RTCP/T.38)

When a remote UA initiates a call and is not located behind a NAT server, the device sends the media (RTP, RTCP, and T.38) packets to the remote UA using the IP address:port (UDP) indicated in the SDP body of the SIP message received from the UA.

However, if the UA is located behind NAT, the device sends the RTP with the IP address of the UA (i.e., private IP address) as the destination instead of that of the NAT server. Thus, the RTP will not reach the UA. To resolve this NAT traversal problem, the device offers the following features:

- First Incoming Packet Mechanism - see "First Incoming Packet Mechanism" on page 145
- RTP No-Op packets according to the avt-rtp-noop draft - see "No-Op Packets" on page 146

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



14.7.2.2.1 First Incoming Packet Mechanism

In scenarios where the remote user agent (UA) resides behind a NAT server, it's possible that the device, if not configured for NAT traversal, will send the media (RTP, RTCP and T.38) streams to an invalid IP address and UDP port. In other words, it will send the media to the private IP address:port of the UA and not the public address (of the NAT server) and therefore, the media will not reach the UA. When the UA is located behind NAT, although the UA sends its private IP address:port in the original SIP message (INVITE), the device receives the media packets with a source address of a public IP address:port (i.e., allocated by the NAT server). Therefore, to ensure that the media reaches the UA, the device must send it to the public address.

The device identifies whether the UA is located behind NAT by comparing the source IP address of the first received media packet with the IP address and UDP port of the first received SIP message (INVITE) when the SIP session was started. This is done for each media type--RTP, RTCP and T.38--and therefore, they can have different destination IP addresses and UDP ports than one another.

You can configure the device's NAT feature to operate in one of the following modes:

- [0] Enable NAT Only if Necessary: NAT traversal is performed only if the UA is located behind NAT:
 - UA behind NAT: The device sends the media packets to the IP address:port obtained from the source address of the first media packet received from the UA.
 - UA not behind NAT: The device sends the packets to the IP address:port specified in the SDP 'c=' line (Connection) of the first received SIP message.

Note: If the SIP session is established (ACK) and the device (not the UA) sends the first packet, it sends it to the address obtained from the SIP message and only after the device receives the first packet from the UA does it determine whether the UA is behind NAT.

- [1] Disable NAT: (Default) The device considers the UA as not located behind NAT

and sends media packets to the UA using the IP address:port specified in the SDP 'c=' line (Connection) of the first received SIP message.

- [2] Force NAT: The device always considers the UA as behind NAT and sends the media packets to the IP address:port obtained from the source address of the first media packet received from the UA. The device only sends packets to the UA after it receives the first packet from the UA (to obtain the IP address).
- [3] NAT by Signaling = The device identifies whether or not the UA is located behind NAT based on the SIP signaling. The device assumes that if signaling is behind NAT that the media is also behind NAT, and vice versa. If located behind NAT, the device sends media as described in option [2] Force NAT; if not behind NAT, the device sends media as described in option [1] Disable NAT. This option is applicable only to SBC calls. If the parameter is configured to this option, Gateway calls use option [0] Enable NAT Option, by default.

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

1. Open the Media Settings page (**Setup** menu > **Signaling & Media** tab > **Media** folder > **Media Settings**), and then from the 'NAT Traversal' drop-down list (NATMode), select the required NAT option:

Figure 14-9: Configuring NAT Traversal for Media



2. Click **Apply**.

14.7.2.2.2 No-Op Packets

The device can send No-Op packets to verify Real-Time Transport Protocol (RTP) and T.38 connectivity, and to keep NAT bindings and Firewall pinholes open. The No-Op packets can be sent in RTP and T.38 formats:

- **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"). The IETF document defines a No-Op payload format for RTP. The draft defines the RTP payload type as dynamic. You can configure the payload type as described in the following procedure (default 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).

➤ **To configure the No-Op packet feature:**

1. Enable the feature, using the NoOpEnable *ini* file parameter.
2. Configure the time interval during which the device sends No-Op packets when silence occurs (i.e., no RTP or T.38 traffic), using the NoOpInterval *ini* file parameter.
3. For RTP No-Op packets, configure the payload type of the No-Op packets, using the RTPNoOpPayloadType *ini* file parameter.



Note:

- The No-OP Packet feature requires DSP resources.
- Receipt of No-Op packets is always supported.

14.7.2.2.3 Fax Transmission behind NAT

The device supports transmission from fax machines (connected to the device) located inside (behind) a Network Address Translation (NAT). Generally, the firewall blocks T.38 (and other) packets received from the WAN, unless the device behind the NAT sends at least one IP packet from the LAN to the WAN through the firewall. If the firewall blocks T.38 packets sent from the termination IP fax, the fax fails.

To overcome this, the device sends No-Op ("no-signal") packets to open a pinhole in the NAT for the answering fax machine. The originating fax does not wait for an answer, but immediately starts sending T.38 packets to the terminating fax machine upon receipt of a re-INVITE with T.38 only in the SDP, or T.38 and audio media in the SDP. This feature is configured using the T38FaxSessionImmediateStart parameter. The No-Op packets are enabled using the NoOpEnable and NoOpInterval parameters.

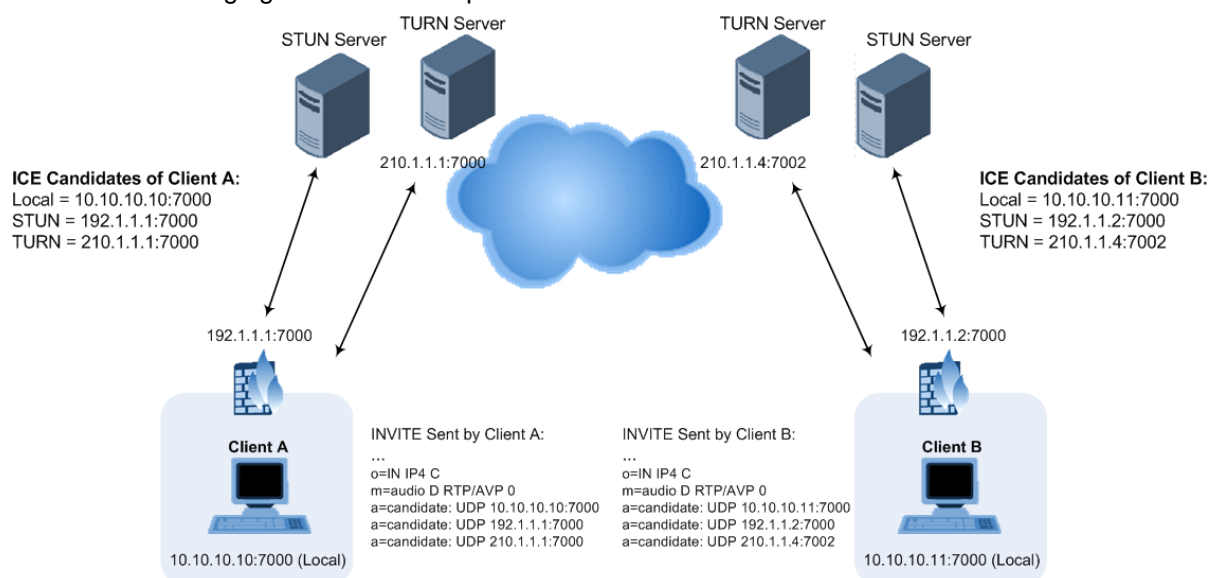
14.7.2.2.4 ICE Lite

The device supports Interactive Connectivity Establishment (ICE) Lite for SBC calls. ICE is a methodology for NAT traversal, enabling VoIP interoperability across networks to work better across NATs and firewalls. It employs Session Traversal Utilities for NAT (STUN) and Traversal Using Relays around NAT (TURN) protocols to provide a peer with a public IP address and port that can be used to connect to a remote peer.

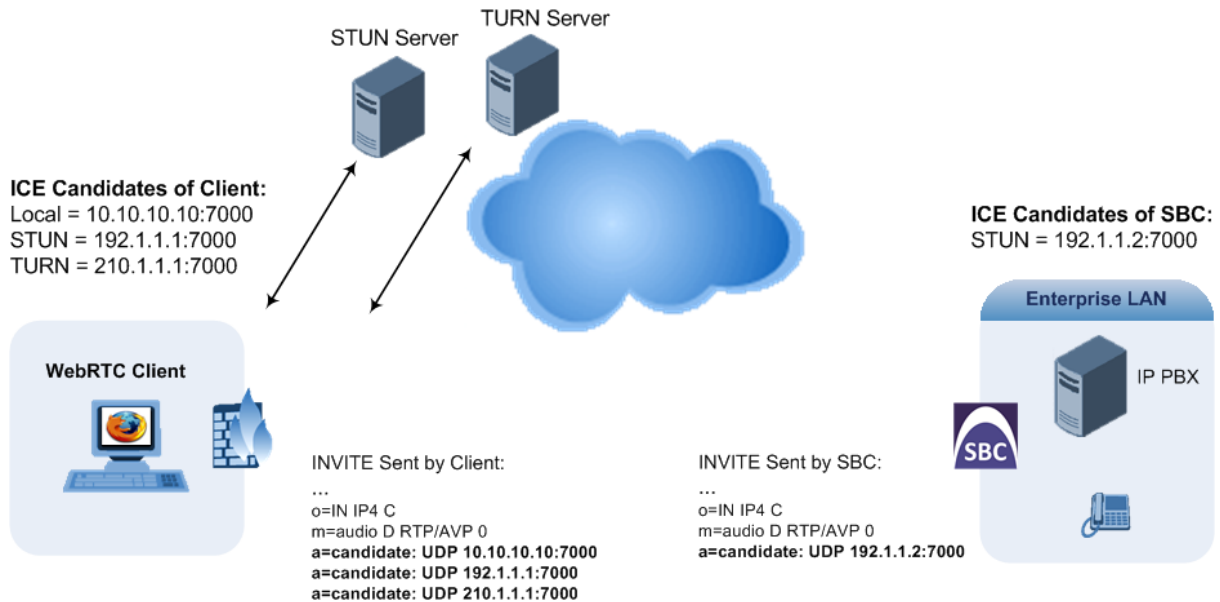
In order for clients behind NATs and/or firewalls to send media (RTP) between one another, they need to discover each others P address and port as seen by the "outside" world. If both peers are located in different private networks behind a NAT, the peers must coordinate to determine the best communication path between them.

ICE first tries to make a connection using the client's private local address. If that fails (which it will for clients behind NAT), ICE obtains an external (public) address using a STUN server. If that fails, traffic is routed through a TURN relay server (which has a public address).

These addresses:ports (local, STUN, TURN and any other network address) of the client are termed "candidates". Each client sends its' candidates to the other in the SDP body of the INVITE message. Peers then perform connectivity checks per candidate of the other peer, using STUN binding requests sent on the RTP and RTCP ports. ICE tries each candidate and selects the one that works (i.e., media can flow between the clients). The following figure shows a simple illustration of ICE:



The device's support for ICE-Lite means that it does not initiate the ICE process. Instead, it supports remote endpoints that initiate ICE to discover their workable public IP address with the device. Therefore, the device supports the receipt of STUN binding requests for connectivity checks of ICE candidates and responds to them with STUN responses. Note that in the response to the INVITE message received from the remote endpoint, the device sends only a single candidate for its' own IP address. This is the IP address of the device that the client uses. To support ICE, the SBC leg interfacing with the ICE-enabled client (SIP entity) must be enabled for ICE. This is done using the IP Profile parameter, IPProfile_SBCIceMode (see "Configuring IP Profiles" on page 388).



As the ICE technique has been defined by the WebRTC standard as mandatory for communication with the WebRTC client, ICE support by the device is important for deployments implementing WebRTC. For more information on WebRTC, see "WebRTC" on page 524. Once a WebRTC session (WebSocket) is established for SIP signaling between the device and the WebRTC client, the client's IP address needs to be discovered by the SBC device using the ICE technique.

14.8 Configuring Quality of Service

This section describes how to configure Layer-2 and Layer-3 Quality of Service (QoS).

14.8.1 Configuring Class-of-Service QoS

The QoS Settings page lets you configure Layer-3 Class-of-Service Quality of Service (QoS). This configures Differentiated Services (DiffServ) values for each CoS. 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 priority, 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 the following class of services (CoS):

-
- Media Premium: RTP packets sent to the LAN
- Control Premium: Control protocol (SIP) packets sent to the LAN
- Gold: HTTP streaming packets sent to the LAN

- Bronze: OAMP packets sent to the LAN

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

Table 14-16: Traffic/Network Types and Priority

Application	Traffic / Network Types	Class-of-Service (Priority)
Debugging interface	Management	Bronze
Telnet	Management	Bronze
Web server (HTTP)	Management	Bronze
SNMP GET/SET	Management	Bronze
Web server (HTTPS)	Management	Bronze
RTP traffic	Media	Media Premium
RTCP traffic	Media	Media Premium
T.38 traffic	Media	Media Premium
SIP	Control	Control Premium
SIP over TLS (SIPS)	Control	Control Premium
Syslog	Management	Bronze
SNMP Traps	Management	Bronze
DNS client	Varies according to DNS settings: <ul style="list-style-type: none"> ■ OAMP ■ Control 	Depends on traffic type: <ul style="list-style-type: none"> ■ Control: Control Premium ■ Management: Bronze
NTP	Varies according to the interface type associated with NTP (see "Assigning NTP Services to Application Types" on page 134): <ul style="list-style-type: none"> ■ OAMP ■ Control 	Depends on traffic type: <ul style="list-style-type: none"> ■ Control: Control Premium ■ Management: Bronze

➤ **To configure DiffServ (Layer-3 QoS) values per CoS:**

1. Open the QoS Settings page (**Setup** menu > **IP Network** tab > **Quality** folder > **QoS Settings**).
2. Click **New**; the following dialog box appears:

Figure 14-10: Configuring Class of Service

GENERAL

Media Premium QoS	46
Control Premium QoS	40
Gold QoS	26
Bronze QoS	10

3. Configure DiffServ values per CoS according to the parameters described in the table below.

4. Click **Apply**, and then save your settings to flash memory.

Table 14-17: QoS Settings Parameter Descriptions

Parameter	Description
Media Premium QoS media-qos [PremiumServiceClassMediaDiffServ]	Defines the DiffServ value for Premium Media CoS content. The valid range is 0 to 63. The default is 46. Note: You can also configure the the parameter per IP Profile (IpProfile_IPDiffServ) or Tel Profile (TelProfile_IPDiffServ).
Control Premium QoS control-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. Note: You can also configure the the parameter per IP Profile (IpProfile_SigIPDiffServ) or Tel Profile (TelProfile_SigIPDiffServ).
Gold QoS gold-qos [GoldServiceClassDiffServ]	Defines the DiffServ value for Gold CoS content (streaming applications). The valid range is 0 to 63. The default is 26.
Bronze QoS bronze-qos [BronzeServiceClassDiffServ]	Defines the DiffServ value for Bronze CoS content (OAMP applications). The valid range is 0 to 63. The default is 10.

14.8.2 Configuring DiffServ-to-VLAN Priority Mapping

The QoS Mapping table lets you configure up to 64 DiffServ-to-VLAN priority mapping for Layer 3 and Layer-2 Quality of Service (QoS). 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. Layer-2 802.1Q frames have a 2-byte field called Tag Control Information. The three most significant bits of this 2-byte field represents the Class of Service (CoS) value. Layer-2 QoS is represented by this CoS value which is from 0 to 7 (thus 8 values). Layer-2 QoS parameters define the values for the 3 priority bits in the VLAN tag according to the value of the DiffServ field in the packet IP header (according to the IEEE 802.1p standard). 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 priority, 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.

The following procedure describes how to configure DiffServ-to-VLAN priority mapping through the Web interface. You can also configure it through ini file (DiffServToVlanPriority) or CLI (configure network > qos vlan-mapping).

➤ **To configure DiffServ-to-VLAN priority mapping:**

1. Open the QoS Mapping table (**Setup** menu > **IP Network** tab > **Quality** folder > **QoS Mapping**).

2. Click **New**; the following dialog box appears:

Figure 14-11: QoS Mapping Table - Add Dialog Box

The screenshot shows a dialog box titled "QoS Mapping" with a "GENERAL" tab. It contains three input fields:

- Index:** 1
- Differentiated Services:** 0
- VLAN Priority:** 0

3. Configure a DiffServ-to-VLAN priority mapping rule according to the parameters described in the table below.
4. Click **Apply**, and then save your settings to flash memory.

Table 14-18: QoS Mapping Table Parameter Descriptions

Parameter	Description
Index	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
Differentiated Services diff-serv [DiffServToVlanPriority_DiffServ]	Defines a DiffServ value. The valid value is 0 to 63. The default is 0.
VLAN Priority vlan-priority [DiffServToVlanPriority_VlanPriority]	Defines the VLAN priority level. The valid value is 0 to 7. The default is 0.

14.9 Configuring ICMP Messages

Internet Control Message Protocol (ICMP) is one of the core protocols of the Internet Protocol suite. It is used by network devices such as routers to send error messages indicating, for example, that a requested service is unavailable.

You can configure the device to handle ICMP messages as follows:

- Send and receive ICMP Redirect messages.
- Send ICMP Destination Unreachable messages. The device sends this message in response to a packet that cannot be delivered to its destination for reasons other than congestion. The device sends a Destination Unreachable message upon any of the following:
 - Address unreachable
 - Port unreachable

This feature is applicable to IPv4 and IPv6 addressing schemes.

The following procedure describes how to configure ICMP messaging through the Web interface. You can also configure it through ini file - DisableICMPUnreachable (ICMP Unreachable messages) and DisableICMPRedirects (ICMP Redirect messages).

- **To configure handling of ICMP messages:**
- 1. Open the Network Settings page (**Setup** menu > **IP Network** tab > **Advanced** folder > **Network Settings**).

Figure 14-12: Configuring ICMP Messaging

ICMP	
Send and Receive ICMP Redirect Messages	Enable
Send ICMP Unreachable Messages	Enable

- 2. Under the ICMP group, do the following:
 - To enable sending and receipt of ICMP Redirect messages, configure the 'Send and Received ICMP Redirect Messages' parameter to **Enable**.
 - To enable sending of ICMP Destination Unreachable messages, configure the 'Send ICMP Unreachable Messages' parameter to **Enable**.
- 3. Click **Apply**.

14.10 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 152
- Internal SRV table - see "Configuring the Internal SRV Table" on page 153

14.10.1 Configuring the Internal DNS Table

The Internal DNS table, similar to a DNS resolution can translate 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 in a routing rule. Up to three different IP addresses can be assigned to the same host name.



Note: The device first attempts to resolve a domain name using the table. If the domain name is not configured in the table, the device performs a DNS resolution using an external DNS server for the related IP network interface (see "Configuring IP Network Interfaces" on page 130).

The following procedure describes how to configure the DNS table through the Web interface. You can also configure it through ini file (DNS2IP) or CLI (configure network > dns dns-to-ip).

- **To configure the device's DNS table:**
- 1. Open the Internal DNS table (**Setup** menu > **IP Network** tab > **DNS** folder > **Internal DNS**).

- Click **New**; the following dialog box appears:

Figure 14-13: Internal DNS Table - Add Dialog Box

The screenshot shows a dialog box titled "Internal DNS" with a "GENERAL" tab. The dialog contains the following fields:

- Index:** A text box containing the value "0".
- Domain Name:** An empty text box.
- First IP Address:** A text box containing the value "0.0.0.0".
- Second IP Address:** A text box containing the value "0.0.0.0".
- Third IP Address:** A text box containing the value "0.0.0.0".

- Configure a DNS rule according to the parameters described in the table below.
- Click **Apply**.

Table 14-19: Internal DNS Table Parameter Description

Parameter	Description
Index	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
Domain Name domain-name [Dns2Ip_DomainName]	Defines the host name to be translated. The valid value is a string of up to 31 characters.
First IP Address first-ip-address [Dns2Ip_FirstIpAddress]	Defines the first IP address (in dotted-decimal format notation) to which the host name is translated. The IP address can be configured as an IPv4 and/or IPv6 address.
Second IP Address second-ip-address [Dns2Ip_SecondIpAddress]	Defines the second IP address (in dotted-decimal format notation) to which the host name is translated.
Third IP Address third-ip-address [Dns2Ip_ThirdIpAddress]	Defines the third IP address (in dotted-decimal format notation) to which the host name is translated.

14.10.2 Configuring the Internal SRV Table

The Internal SRV table 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.



Note: The device first attempts to resolve a domain name using the table. If the domain is not configured in the table, the device performs a Service Record (SRV) resolution using an external DNS server, configured in the IP Interfaces table (see "Configuring IP Network Interfaces" on page 130).

The following procedure describes how to configure the Internal SRV table through the Web interface. You can also configure it through ini file (SRV2IP) or CLI (configure network > dns srv2ip).

➤ **To configure the device's SRV table:**

1. Open the Internal SRV table (**Setup** menu > **IP Network** tab > **DNS** folder > **Internal SRV**).
2. Click **New**; the following dialog box appears:

Figure 14-14: Internal SRV Table - Add Dialog Box

The dialog box is titled 'Internal SRV' and has a dark blue header. It is divided into four main sections:

- GENERAL:** Includes fields for 'Index' (value: 0), 'Domain Name' (empty), and 'Transport Type' (dropdown menu showing 'UDP').
- 1ST ENTRY:** Includes fields for 'DNS Name 1', 'Priority 1' (value: 0), 'Weight 1' (value: 0), and 'Port 1' (value: 0).
- 2ND ENTRY:** Includes fields for 'DNS Name 2', 'Priority 2' (value: 0), 'Weight 2' (value: 0), and 'Port 2' (value: 0).
- 3RD ENTRY:** Includes fields for 'DNS Name 3', 'Priority 3' (value: 0), 'Weight 3' (value: 0), and 'Port 3' (value: 0).

3. Configure an SRV rule according to the parameters described in the table below.
4. Click **Apply**, and then save your settings to flash memory.

Table 14-20: Internal SRV Table Parameter Descriptions

Parameter	Description
General	
Index	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
Domain Name domain-name [Srv2Ip_InternalDomain]	Defines the host name to be translated. The valid value is a string of up to 31 characters. By default, no value is defined.
Transport Type transport-type [Srv2Ip_TransportType]	Defines the transport type. <ul style="list-style-type: none"> ▪ [0] UDP (default) ▪ [1] TCP ▪ [2] TLS
1st/2nd/3rd Entry	

Parameter	Description
DNS Name (1-3) dns-name-1 2 3 [Srv2lp_Dns1/2/3]	Defines the first, second or third DNS A-Record to which the host name is translated. By default, no value is defined.
Priority (1-3) priority-1 2 3 [Srv2lp_Priority1/2/3]	Defines the priority of the target host. A lower value means that it is more preferred. By default, no value is defined.
Weight (1-3) weight-1 2 3 [Srv2lp_Weight1/2/3]	Defines a relative weight for records with the same priority. By default, no value is defined.
Port (1-3) port-1 2 3 [Srv2lp_Port1/2/3]	Defines the TCP or UDP port on which the service is to be found. By default, no value is defined.

14.11 Robust Receipt of Media Streams by Media Latching

The Robust Media mechanism (or media latching) is an AudioCodes proprietary mechanism to filter out unwanted media (RTP, RTCP, SRTP, SRTCP, and T.38) streams that are sent to the same port number of the device. Media ports may receive additional multiple unwanted media streams (from multiple sources of traffic) as result of traces of previous calls, call control errors, or deliberate malicious attacks (e.g., Denial of Service). When the device receives more than one media stream on the same port, the Robust Media mechanism detects the valid media stream and ignores the rest. Thus, this can prevent an established call been stolen by a malicious attacker on the media stream.

For the involved voice channel, the device latches onto the first stream of the first received packet. All packets (of any media type) received from the same IP address and SSRC are accepted (for T.38 packets, the device considers only the IP address). If the channel receives subsequent packets from a non-latched source, the device can either ignore this new stream and remain latched to the first original stream (IP address:port), or it can latch onto this new stream. The media latch mode is configured using the InboundMediaLatchMode parameter. If this mode is configured to latch onto new streams, you also need to configure the following:

- Minimum number of continuous media packets that need to be received from a different source(s) before the channel can latch onto this new incoming stream.
- Period (msec) during which if no packets are received from the current stream, the channel latches onto the next packet received from any other stream.

Depending on media latch mode, if the device has latched onto a new stream and a packet from the original (first latched onto) IP address:port is received at any time, the device latches onto this original stream.

Latching onto a new T.38 stream is reported in CDR using the CDR fields, LatchedT38Ip (new IP address) and LatchedT38Port (new port). In addition, the SIP PUBLISH message updates the latched RTP SSRC, for example:

```
RemoteAddr: IP=10.33.2.55 Port=4000 SSRC=0x66d510ec
```

➤ To configure media latching:

1. Open the Media Settings page (**Setup** menu > **Signaling & Media** tab > **Media** folder > **Media Settings**), and then from the 'Inbound Media Latch Mode' drop-down list (InboundMediaLatchMode), configure the media latch mode:

Inbound Media Latch Mode

2. If you configure the parameter to Dynamic or Dynamic-Strict::
 - Define the minimum number of continuous media (RTP, RTCP, SRTP, and SRTCP) packets that need to be received by the channel before it can latch onto this new incoming stream:
 - ◆ 'New RTP Stream Packets'
 - ◆ 'New RTCP Stream Packets'
 - ◆ 'New SRTP Stream Packets'
 - ◆ 'New SRTCP Stream Packets'
 - Define a period (msec) during which if no packets are received from the current media session, the channel can re-latch onto another stream:
 - ◆ 'Timeout To Relatch RTP'
 - ◆ 'Timeout To Relatch SRTP'
 - ◆ 'Timeout To Relatch Silence'
 - ◆ 'Timeout To Relatch RTCP'
 - ◆ 'Fax Relay Rx/Tx Timeout'

ROBUSTNESS	
New RTP Stream Packets	<input type="text" value="3"/>
New RTCP Stream Packets	<input type="text" value="3"/>
New SRTP Stream Packets	<input type="text" value="3"/>
New SRTCP Stream Packets	<input type="text" value="3"/>
Timeout To Relatch RTP (msec)	<input type="text" value="200"/>
Timeout To Relatch SRTP (msec)	<input type="text" value="200"/>
Timeout To Relatch Silence (msec)	<input type="text" value="10000"/>
Timeout To Relatch RTCP (msec)	<input type="text" value="10000"/>

3. Click **Apply**, and then save your settings to flash memory.

14.12 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.

15 Security

This section describes the VoIP security-related configuration.

15.1 Configuring Firewall Settings

The Firewall table lets you configure up to 500 firewall rules, which define network traffic filtering rules (*access list*). 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 device searches the table from top to bottom until the first matching rule is found. The matched rule can 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.


Note:

- The rules configured by the Firewall table apply to a very low-level network layer and overrides all 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 device's Web and Telnet management interfaces in the Access List table (see "Configuring Web and Telnet Access List" on page 69), you must configure a firewall rule that permits traffic from these IP addresses.
- Only users with Security Administrator or Master access levels can configure firewall rules.
- The device supports dynamic firewall pinholes for media (RTP/RTCP) traffic negotiated in the SDP offer-answer of SIP calls. The pinhole allows the device to ignore its firewall and accept the traffic on the negotiated port. The device automatically closes the pinhole once the call terminates. Therefore, it is unnecessary to configure specific firewall rules to allow traffic through specific ports. For example, if you have configured a firewall rule to block all media traffic in the port range 6000 to 7000 and a call is negotiated to use the local port 6010, the device automatically opens port 6010 to allow the call.
- 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. Thus, it is highly recommended to set the 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, ensure that you also add "allow" rules for HA traffic. For more information, see Configuring Firewall Allowed Rules on page 567.

The following procedure describes how to configure firewall rules through the Web interface. You can also configure it through ini file (AccessList) or CLI (configure network > access-list).

➤ **To configure a firewall rule:**

1. Open the Firewall table (**Setup** menu > **IP Network** tab > **Security** folder > **Firewall**).

- Click **New**; the following dialog box appears:

Figure 15-1: Firewall Table - Add Dialog Box

- Configure a firewall rule according to the parameters described in the table below.
- Click **Apply**, and then reset the device with a save-to-flash for your settings to take effect.

Table 15-1: Firewall Table Parameter Descriptions

Parameter	Description
Match	
Index	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
Source IP source-ip [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). The default is 0.0.0.0.
Source Port src-port [AccessList_Source_Port]	Defines the source UDP/TCP ports (of the remote host) from where packets are sent to the device. The valid range is 0 to 65535. The default is 0. Note: When set to 0, this field is ignored and any source port matches the rule.
Prefix Length prefixLen [AccessList_PrefixLen]	(Mandatory) 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"> A value of 8 corresponds to IPv4 subnet class A (network mask of 255.0.0.0). A value of 16 corresponds to IPv4 subnet class B (network mask of 255.255.0.0). A value of 24 corresponds to IPv4 subnet class C (network mask of 255.255.255.0). 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'. The default is 0 (i.e., applies to all packets). You must change this value to any of the above options. Note: A value of 0 applies to all packets, regardless of the defined IP address. Therefore, you must set the parameter to a value other than

Parameter	Description
	0.
Start Port start-port [AccessList_Start_Port]	Defines the destination UDP/TCP start port (on this device) to where packets are sent. The valid range is 0 to 65535. Note: When the protocol type isn't TCP or UDP, the entire range must be provided.
End Port end-port [AccessList_End_Port]	Defines the destination UDP/TCP end port (on this device) to where packets are sent. The valid range is 0 to 65535 (default). Note: When the protocol type isn't TCP or UDP, the entire range must be provided.
Protocol protocol [AccessList_Protocol]	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. The default is Any . Note: The parameter 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.
Use Specific Interface use-specific-interface [AccessList_Use_Specific_Int erface]	Determines whether you want to apply the rule to a specific network interface defined in the IP Interfaces table (i.e., packets received from that defined in the Source IP field and received on this network interface): <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable Note: <ul style="list-style-type: none"> ▪ If enabled, then in the 'Interface Name' field (described below), select the interface to which the rule is applied. ▪ If disabled, then the rule applies to all interfaces.
Interface Name network-interface-name [AccessList_Interface_x]	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 IP Interfaces table in "Configuring IP Network Interfaces" on page 130.
Action	
Action Upon Match allow-type [AccessList_Allow_Type]	Defines the firewall action to be performed upon rule match. <ul style="list-style-type: none"> ▪ "Allow" = (Default) Permits the packets. ▪ "Block" = Rejects the packets
Packet Size packet-size [AccessList_Packet_Size]	Defines the maximum allowed packet size. The valid range is 0 to 65535. Note: When filtering fragmented IP packets, this field relates to the overall (re-assembled) packet size, and not to the size of each fragment.
Byte Rate byte-rate [AccessList_Byte_Rate]	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

Parameter	Description
	being interrupted. 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 replenished within 5 seconds.
Burst Bytes byte-burst [AccessList_Byte_Burst]	Defines the tolerance of traffic rate limit (number of bytes). The default is 0.
Statistics	
Match Count [AccessList_MatchCount]	(Read-only) Displays the number of packets accepted or rejected by the rule.

The table below provides an example of configured firewall rules:

Table 15-2: Configuration Example of Firewall Rules

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

15.2 Configuring TLS for SIP

The device uses TLS over TCP to encrypt and optionally, authenticate SIP messages. This is referred to as Secure SIP (SIPS). SIPS uses the X.509 certificate exchange process, as described in "Configuring SSL/TLS Certificates" on page 99, where you need to configure certificates (TLS Context).



Note: When a TLS connection with the device is initiated by a SIP client, the device also responds using TLS, regardless of whether or not TLS was configured.

➤ **To configure SIPS:**

1. Configure a TLS Context as required (see "Configuring TLS Certificate Contexts" on page 99).
2. Assign the TLS Context to a Proxy Set or SIP Interface (see "Configuring Proxy Sets" on page 341 and "Configuring SIP Interfaces" on page 321, respectively).
3. Configure a SIP Interface with a TLS port number.
4. Configure various SIPS parameters in the Security Settings page (**Setup** menu > **IP Network** tab > **Security** folder > **Security Settings**).

Figure 15-2: Configuring TLS

SIP OVER TLS	TLS GENERAL
TLS Client Re-Handshake Interval: <input type="text" value="0"/>	Strict Certificate Extension Validation: <input type="text" value="Disable"/>
TLS Mutual Authentication: <input type="text" value="Disable"/>	TLS Expiry Check Start (days): <input type="text" value="60"/>
Peer Host Name Verification Mode: <input type="text" value="Disable"/>	TLS Expiry Check Period (days): <input type="text" value="7"/>
TLS Client Verify Server Certificate: <input type="text" value="Disable"/>	
TLS Remote Subject Name: <input type="text"/>	
	ADVANCED
	FIPS140 Mode: <input type="text" value="Disable"/>
MANAGEMENT	
Enable Management Two Factor Authentication: <input type="text" value="Disable"/>	

For a description of the TLS parameters, see "TLS Parameters" on page 771.

5. By default, the device initiates a TLS connection only for the next network hop. To enable TLS all the way to the destination (**over multiple hops**), configure the 'Enable SIPS' (EnableSIPS) parameter to **Enable** on the Transport Settings page (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Transport Settings**):

Figure 15-3: Enabling SIPS

Enable SIPS

15.3 Intrusion Detection System

The device's Intrusion Detection System (IDS) feature detects malicious attacks on the device and reacts accordingly. A remote host is considered malicious if it has reached or exceeded a user-defined threshold (counter) of specified malicious attacks.

If malicious activity is detected, the device can do the following:

- Block (blacklist) remote hosts (IP addresses / ports) considered by the device as malicious. The device automatically blacklists the malicious source for a user-defined period after which it is removed from the blacklist.
- Send SNMP traps to notify of malicious activity and/or whether an attacker has been added to or removed from the blacklist. For more information, see "Viewing IDS Alarms" on page 170.

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.

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).

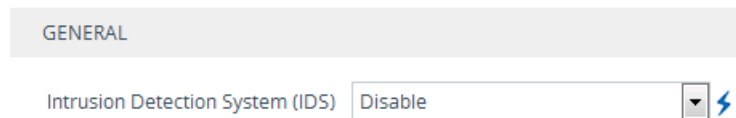
15.3.1 Enabling IDS

The following procedure describes how to enable IDS.

➤ **To enable IDS:**

1. Open the IDS General Settings page (**Setup** menu > **Signaling & Media** tab > **Intrusion Detection** folder > **IDS General Settings**).

Figure 15-4: Enabling IDS



2. From the 'Intrusion Detection System' drop-down list, select **Enable**.
3. Click **Apply**, and then reset the device with a save-to-flash for the setting to take effect.

15.3.2 Configuring IDS Policies

Configuring IDS Policies is a two-stage process that includes the following tables:

1. **IDS Policies (parent table):** Defines a name and provides a description for the IDS Policy. You can configure up to 20 IDS Policies.
2. **IDS Rules table (child table):** Defines the actual rules for the IDS Policy. Each IDS 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).

The device provides the following pre-configured IDS Policies that can be used in your deployment (if they meet your requirements):

- "DEFAULT_FEU": IDS Policy for far-end users in the WAN
- "DEFAULT_PROXY": IDS Policy for proxy server
- "DEFAULT_GLOBAL": IDS Policy with global thresholds



Note: The default IDS Policies are read-only and cannot be modified.

The following procedure describes how to configure IDS Policies through the Web interface. You can also configure it through ini file or CLI:

- IDS Policy table: IDSPolicy (ini file) or configure voip > ids policy (CLI)
- IDS Rules table: IDSRule (ini file) or configure voip > ids rule (CLI)

➤ **To configure an IDS Policy:**

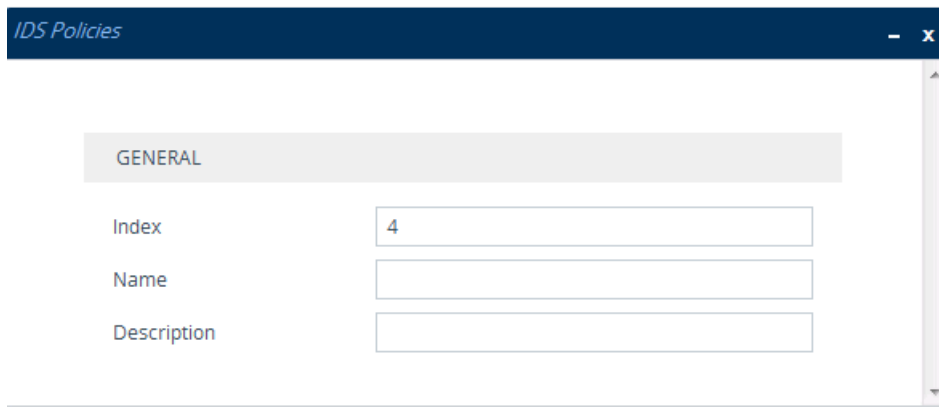
1. Open the IDS Policies table (**Setup** menu > **Signaling & Media** tab > **Intrusion Detection** folder > **IDS Policies**); the table displays the pre-configured IDS policies:

Figure 15-5: IDS Policies Table with Default Rules

INDEX ↕	NAME	DESCRIPTION
0	DOS	dos-attacks
1	DEFAULT_FEU	Default policy for FEU
2	DEFAULT_PROXY	Default policy for proxies
3	DEFAULT_GLOBAL	Default policy for global scope

2. Click **New**; the following dialog box appears:

Figure 15-6: IDS Policies Table - Add Dialog Box



3. Configure an IDS Policy name according to the parameters described in the table below.
4. Click **Apply**.

Table 15-3: IDS Policies Table Parameter Descriptions

Parameter	Description
Index policy [IDSPolicy_Index]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
Name rule [IDSPolicy_Name]	Defines an arbitrary name to easily identify the row. The valid value is a string of up to 40 characters.
Description description [IDSPolicy_Description]	Defines a brief description for the IDS Policy. The valid value is a string of up to 100 characters.

5. In the IDS Policies table, select the required IDS Policy row, and then click the **IDS Rule** link located below the table; the IDS Rule table opens.

- Click **New**; the following dialog box appears:

Figure 15-7: IDS Rule Table - Add Dialog Box

The figure above shows a configuration example: If 15 malformed SIP messages ('Reason') are received within a period of 30 seconds ('Threshold Window'), a minor alarm is sent ('Minor-Alarm Threshold'). Every 30 seconds, the rule's counters are cleared ('Threshold Window'). If more than 25 malformed SIP messages are received within this period, the device blacklists for 60 seconds the remote IP host ('Deny Threshold') from where the messages were received.

- Configure an IDS Rule according to the parameters described in the table below.
- Click **Apply**, and then save your settings to flash memory.
- For example

Table 15-4: IDS Rule Table Parameter Descriptions

Parameter	Description
General	
Index rule-id [IDSRule_RuleID]	Defines an index number for the new table record.
Reason reason [IDSRule_Reason]	<p>Defines the type of intrusion attack (malicious event).</p> <ul style="list-style-type: none"> ▪ [0] Any = All events listed below are considered as attacks and are counted together. ▪ [1] Connection abuse = (Default) TLS authentication failure. ▪ [2] Malformed message = <ul style="list-style-type: none"> ✓ Message exceeds a user-defined maximum message length (50K) ✓ Any SIP parser error ✓ Message Policy match (see "Configuring SIP Message Policy Rules") ✓ Basic headers not present ✓ Content length header not present (for TCP) ✓ Header overflow ▪ [3] Authentication failure = <ul style="list-style-type: none"> ✓ Local authentication ("Bad digest" errors) ✓ Remote authentication (SIP 401/407 is sent if original

Parameter	Description
	<p>message includes authentication)</p> <ul style="list-style-type: none"> ▪ [4] Dialog establish failure = <ul style="list-style-type: none"> ✓ Classification failure (see "Configuring Classification Rules" on page 461). This also applies to calls rejected by the device based on a registered users policy (configured by the SRD_BlockUnRegUsers or SIPInterface_BlockUnRegUsersblocks parameters). ✓ Routing failure ✓ Other local rejects (prior to SIP 180 response) ✓ Remote rejects (prior to SIP 180 response) ✓ Malicious signature pattern detected (see "Configuring Malicious Signatures" on page 517) ▪ [5] Abnormal flow = <ul style="list-style-type: none"> ✓ Requests and responses without a matching transaction user (except ACK requests) ✓ Requests and responses without a matching transaction (except ACK requests)
<p>Threshold Scope threshold-scope [IDSRule_ThresholdScope]</p>	<p>Defines the source of the attacker to consider in the device's detection count.</p> <ul style="list-style-type: none"> ▪ [0] Global = All attacks regardless of source are counted together during the threshold window. ▪ [2] IP = Attacks from each specific IP address are counted separately during the threshold window. ▪ [3] 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.
<p>Threshold Window threshold-window [IDSRule_ThresholdWindow]</p>	<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>
Alarms	
<p>Minor-Alarm Threshold minor-alm-thr [IDSRule_MinorAlarmThreshold]</p>	<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>
<p>Major-Alarm Threshold major-alm-thr [IDSRule_MajorAlarmThreshold]</p>	<p>Defines the threshold that if crossed a major 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>
<p>Critical-Alarm Threshold critical-alm-thr [IDSRule_CriticalAlarmThreshold]</p>	<p>Defines the threshold that if crossed a critical 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>
Deny	
<p>Deny Threshold</p>	<p>Defines the threshold that if crossed, the device blocks (blacklists)</p>

Parameter	Description
deny-thr [IDSRule_DenyThreshold]	the remote host (attacker). The default is -1 (i.e., not configured). Note: The parameter is applicable only if the 'Threshold Scope' parameter is set to IP or IP+Port .
Deny Period deny-period [IDSRule_DenyPeriod]	Defines the duration (in sec) to keep the attacker on the blacklist, if configured using the 'Deny Threshold' parameter. The valid range is 0 to 1,000,000. The default is -1 (i.e., not configured). Note: The parameter is applicable only if the 'Threshold Scope' parameter is set to IP or IP+Port .

15.3.3 Assigning IDS Policies

The IDS Matches table lets you implement your configured IDS Policies. You do this by assigning IDS Policies to any, or a combination of the following configuration entities:

- **SIP Interface:** For detection of malicious attacks on specific SIP Interface(s). To configure SIP Interfaces, see "Configuring SIP Interfaces" on page 321.
- **Proxy Sets:** For detection of malicious attacks from specified Proxy Set(s). To configure Proxy Sets, see "Configuring Proxy Sets" on page 341.
- **Subnet addresses:** For detection of malicious attacks from specified subnet addresses.

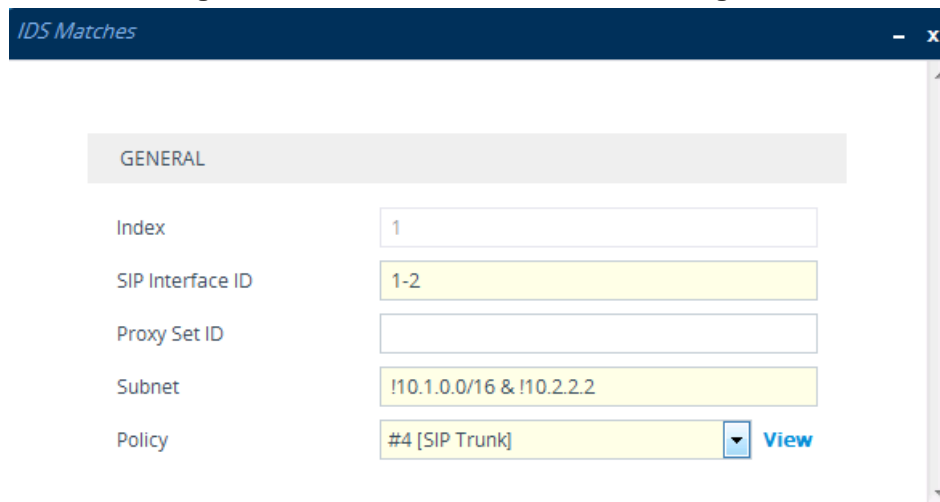
You can configure up to 20 IDS Policy-Matching rules.

The following procedure describes how to configure the IDS Match table through the Web interface. You can also configure it through ini file (IDSMatch) or CLI (configure voip > ids match).

➤ **To configure an IDS Policy-Matching rule:**

1. Open the IDS Matches table (**Setup** menu > **Signaling & Media** tab > **Intrusion Detection** folder > **IDS Matches**).
2. Click **New**; the following dialog box appears:

Figure 15-8: IDS Matches Table - Add Dialog Box



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

3. Configure a rule according to the parameters described in the table below.
4. Click **Apply**, and then save your settings to flash memory.

Table 15-5: IDS Matches Table Parameter Descriptions

Parameter	Description
Index [IDSMATCH_Index]	Defines an index number for the new table record.
SIP Interface ID sip-interface [IDSMATCH_SIPInterface]	<p>Defines the SIP Interface(s) to which you want to assign the IDS Policy. This indicates the SIP Interfaces that are being attacked.</p> <p>The valid value is the ID of the SIP Interface. The following syntax is supported:</p> <ul style="list-style-type: none"> ▪ A comma-separated list of SIP Interface IDs (e.g., 1,3,4) ▪ A hyphen "-" indicates a range of SIP Interfaces (e.g., 3,4-7 means IDs 3, and 4 through 7) ▪ 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)
Proxy Set ID proxy-set [IDSMATCH_ProxySet]	<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"> ▪ A comma-separated list of Proxy Set IDs (e.g., 1,3,4) ▪ A hyphen "-" indicates a range of Proxy Sets (e.g., 3,4-7 means IDs 3, and 4 through 7) ▪ 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) <p>Note:</p> <ul style="list-style-type: none"> ▪ Only the IP address of the Proxy Set is considered (not port). ▪ 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.
Subnet subnet [IDSMATCH_Subnet]	<p>Defines the subnet 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"> ▪ 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) ▪ An IP address can be specified without the prefix length to refer to the specific IP address. ▪ Each subnet can be negated by prefixing it with "!", which means all IP addresses outside that subnet. ▪ Multiple subnets can be specified by separating them with "&" (and) or " " (or) operations. For example: <ul style="list-style-type: none"> ✓ 10.1.0.0/16 10.2.2.2: includes subnet 10.1.0.0/16 and IP address 10.2.2.2. ✓ !10.1.0.0/16 & !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. ✓ 10.1.0.0/16 & !10.1.1.1: includes subnet 10.1.0.0/16, except IP address 10.1.1.1.

Parameter	Description
Policy policy [IDSMATCH_Policy]	Assigns an IDS Policy (configured in "Configuring IDS Policies" on page 164).

15.3.4 Viewing IDS Alarms

For the IDS feature, the device sends the following SNMP traps:

- Traps that notify the detection of malicious attacks:
 - **acIDSPolicyAlarm:** The device sends this alarm whenever a threshold of a specific IDS Policy rule is crossed. The trap displays the crossed severity threshold (Minor or Major), IDS Policy and IDS Rule, and the IDS Policy-Match index.
 - **acIDSThresholdCrossNotification:** The device sends this event for each scope (IP address) that crosses the threshold. In addition to the crossed severity threshold (Minor or Major) of the IDS Policy-Match index, this event shows the IP address (or IP address:port) of the malicious attacker.

If the severity level is raised, the alarm of the former severity is cleared and the device sends a new alarm with the new severity. The alarm is cleared after a user-defined period (configured by the ini file parameter, IDSAAlarmClearPeriod) 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 164). For example, if you set IDSAAlarmClearPeriod to 20 sec and 'Threshold Window' to 15 sec, the IDSAAlarmClearPeriod parameter is ignored and the alarm is cleared only after 30 seconds (2 x 15 sec).

The figure below displays an example of IDS alarms in the Active Alarms table ("Viewing Active Alarms" on page 643). In this example, a Minor threshold alarm is cleared and replaced by a Major threshold alarm:

Figure 15-9: 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

- acIDSBlacklistNotification event: The device sends this event whenever an attacker (remote host at IP address and/or port) is added to or removed from the blacklist.

You can also view IDS alarms through CLI:

- To view all active IDS alarms:
show voip ids active-alarm all
- To view all IP addresses that have crossed the threshold for an active IDS alarm:
show voip ids active-alarm match <IDS Match Policy ID> rule <IDS Rule ID>

The IP address is displayed only if the 'Threshold Scope' parameter is set to IP or IP+Port; otherwise, only the alarm is displayed.

- To view the blacklist:
show voip ids blacklist active

For example:

```
Active blacklist entries:
10.33.5.110(NI:0) remaining 00h:00m:10s in blacklist
```

Where SI is the SIP Interface and NI is the network interface.

The device also sends IDS notifications and alarms in Syslog messages to a Syslog server. This occurs only if you have configured Syslog (see "Enabling Syslog" on page 703). An example of a Syslog message with IDS alarms and notifications is shown below:

Figure 15-10: Syslog Message Example with IDS Alarms and Notifications

```
[S=92159] [SID:438286865] ( lgr_ids|97420 ) IDS Event: reason=establish-fail,event=14003(establish-classify-fail),ip=10.13.45.200:5060(SII),transport=udp
[S=92160] [SID:438286865] ( lgr_ids|97421 ) IDS Counter (0,19995): IDSMatch#0/IDSRule#0,policy=3(TEST),reason=establish-fail,scope=ip,scope-val=10.13.45.200(SII),value=6
[S=92161] [SID:438286865] ( lgr_ids|97422 ) ?? [WARNING] IDS Rule (0): Threshold cross. IDSMatch#0/IDSRule#0,policy=3(TEST),value=6,severity=2(major)
[S=92162] [SID:438286865] ( lgr_ids|97423 ) ?? [WARNING] IDS Rule (0): Threshold cross. IDSMatch#0/IDSRule#0,policy=3(TEST),value=6,severity=4(blacklist)
[S=92163] [SID:438286865] ( lgr_ids|97424 ) ?? [WARNING] IDS Blacklist: Added IP 10.13.45.200(NI0) to blacklist
[S=92164] [SID:438286865] ( lgr_psbrdif|97425 ) SNMP EVENT: IDS_BLACKLIST_NOTIFY "Added IP 10.13.45.200(NI0) to blacklist"
[S=92165] RAISE-ALARM:aciDSBlacklistNotification; Textual Description: Added IP 10.13.45.200(NI0) to blacklist; Severity:indeterminate; Source; Unique ID:30;
[S=92166] [SID:438286865] ( lgr_psbrdex|97426 ) InsertBoardEvent- event ADD BLACKLIST EV inserted channel -100
```

The table below lists the Syslog text messages per malicious event:

Table 15-6: Types of Malicious Events and Syslog Text String

Reason	Description	Syslog String
Connection Abuse	TLS authentication failure	abuse-tls-auth-fail
Malformed Messages	<ul style="list-style-type: none"> Message exceeds a user-defined maximum message length (50K) Any SIP parser error Message policy match Basic headers not present Content length header not present (for TCP) Header overflow 	<ul style="list-style-type: none"> malformed-invalid-msg-len malformed-parse-error malformed-message-policy malformed-miss-header malformed-miss-content-len malformed-header-overflow
Authentication Failure	<ul style="list-style-type: none"> Local authentication ("Bad digest" errors) Remote authentication (SIP 401/407 is sent if original message includes authentication) 	<ul style="list-style-type: none"> auth-establish-fail auth-reject-response
Dialog Establishment Failure	<ul style="list-style-type: none"> Classification failure Routing failure Other local rejects (prior to SIP 180 response) Remote rejects (prior to SIP 180 response) Malicious signature pattern detected 	<ul style="list-style-type: none"> establish-classify-fail establish-route-fail establish-local-reject establish-remote-reject establish-malicious-signature-db-reject
Abnormal Flow	<ul style="list-style-type: none"> Requests and responses without a matching transaction user (except ACK requests) Requests and responses without a matching transaction (except ACK requests) 	<ul style="list-style-type: none"> flow-no-match-tu flow-no-match-transaction

This page is intentionally left blank.

16 Media

This section describes the media-related configuration.

16.1 Configuring Voice Settings

The section describes various voice-related configuration such as voice volume, silence suppression, and DTMF transport type. For a detailed description of these parameters, see "Configuration Parameters Reference" on page 733.

16.1.1 Configuring Voice Gain (Volume) Control

The device allows you to configure the level of the received (input gain) IP-to-IP signal and the level of the transmitted (output gain) IP-to-IP signal. The gain can be set between -32 and 31 decibels (dB).

The following procedure describes how to configure gain control through the Web interface.

➤ **To configure gain control through the Web interface:**

1. Open the Voice Settings page (**Setup** menu > **Signaling & Media** tab > **Media** folder > **Voice Settings**).
2. Configure the following parameters:
 - 'Voice Volume' (*VoiceVolume*): Defines the voice gain control (in decibels) of the transmitted signal.
 - 'Input Gain' (*InputGain*): Defines the PCM input gain control (in decibels) of the received signal.
3. Click **Apply**.

16.1.2 Silence Suppression (Compression)

Silence suppression (compression) is a method for conserving bandwidth on VoIP calls by not sending packets when silence is detected. The device uses its VAD feature to detect periods of silence in the voice channel during an established call. When silence is detected, it stops sending packets in the channel.

The following procedure describes how to enable silence suppression using the Web interface.

➤ **To enable silence suppression using the Web interface:**

1. Open the Voice Settings page (**Setup** menu > **Signaling & Media** tab > **Media** folder > **Voice Settings**).
2. From the 'Silence Suppression' drop-down list (*EnableSilenceCompression*), select **Enable**.
3. Click **Apply**.

16.1.3 Configuring Echo Cancellation

The device supports adaptive linear (line) echo cancellation according to G.168-2002. Echo cancellation is a mechanism that removes echo from the voice channel. Echoes are reflections of the transmitted signal.

In this line echo, echoes are generated when two-wire telephone circuits (carrying both transmitted and received signals on the same wire pair) are converted to a four-wire circuit.

Echoes are reflections of the transmitted signal, which result from impedance mismatch in the hybrid (bi-directional 2-wire to 4-wire converting device).

An estimated echo signal is built by feeding the decoder output signal to an RLS-like adaptive filter, which adapts itself to the characteristics of the echo path. The 'estimated echo signal' (the output of this filter) is then subtracted from the input signal (which is the sum of the desired input signal and the undesired echo) to provide a clean signal. To suppress the remaining residual echo, a Non Linear Processor (NLP) is used, as well as a double-talk (two people speak at the same time) detector that prevents false adaptation during near-end speech.

The device also supports acoustic echo cancellation for SBC calls. These echoes are composed of undesirable acoustical reflections (non-linear) of the received signal (i.e., from the speaker) which find their way from multiple reflections such as walls and windows into the transmitted signal (i.e., microphone). Therefore, the party at the far end hears his / her echo. The device removes these echoes and sends only the near-end's desired speech signal to the network (i.e., to the far-end party). The echo is composed of a linear part and a nonlinear part. However, in the Acoustic Echo Canceller, a substantial part of the echo is non-linear echo. To support this feature, the Forced Transcoding feature must be enabled so that the device uses DSPs.

The following procedure describes how to configure echo cancellation through the Web interface:

➤ **To configure echo cancellation:**

1. Configure line echo cancellation:
 - a. Open the Voice Settings page (**Setup** menu > **Signaling & Media** tab > **Media** folder > **Voice Settings**).

Figure 16-1: Enabling Echo Cancellation



- b. From the 'Echo Canceller' drop-down list (*EnableEchoCanceller*), select **Enable**.
2. Enable acoustic echo cancellation for SBC calls:
 - a. Open the Voice Settings page (Setup menu > Signaling & Media tab > Media folder > Voice Settings).
 - b. Under the Network Echo Suppressor group:
 - c. In the Voice Settings page, configure the following parameters:
 - ◆ 'Network Echo Suppressor Enable' (AcousticEchoSuppressorSupport) - enables the network Acoustic Echo Suppressor
 - ◆ 'Echo Canceller Type' (EchoCancellerType) - defines the echo canceller type
 - ◆ 'Attenuation Intensity' (AcousticEchoSuppAttenuationIntensity) - defines the acoustic echo suppressor signals identified as echo attenuation intensity
 - ◆ 'Max ERL Threshold' (AcousticEchoSuppMaxERLThreshold) - defines the acoustic echo suppressor maximum ratio between signal level and returned echo from the phone
 - ◆ 'Min Reference Delay' (AcousticEchoSuppMinRefDelayx10ms) - defines the acoustic echo suppressor minimum reference delay
 - ◆ 'Max Reference Delay' (AcousticEchoSuppMaxRefDelayx10ms) - defines the acoustic echo suppressor maximum reference delay
 - d. Open the IP Profiles table, and configure the 'Echo Canceller' parameter to Acoustic (see Configuring IP Profiles on page 388).
 - e. Enable the Forced Transcoding feature (using the TranscodingMode parameter) to allow the device to use DSP channels, which are required for acoustic echo cancellation.



Note: The following additional echo cancellation parameters are configurable only through the *ini* file:

- *ECHybridLoss* - defines the four-wire to two-wire worst-case Hybrid loss
- *ECNLPMode* - defines the echo cancellation Non-Linear Processing (NLP) mode
- *EchoCancellerAggressiveNLP* - enables Aggressive NLP at the first 0.5 second of the call

16.2 Fax and Modem Capabilities

This section describes the device's fax and modem capabilities and corresponding configuration. The fax and modem configuration is done in the Fax/Modem/CID Settings page.



Note:

- Unless otherwise specified, the configuration parameters mentioned in this section are available on this page.
- Some SIP parameters override these fax and modem parameters. For example, the *IsFaxUsed* parameter and V.152 parameters in Section "V.152 Support" on page 185.
- For a detailed description of the parameters appearing on this page, see "Configuration Parameters Reference" on page 733.

➤ To access the fax and modem parameters:

1. Open the Fax/Modem/CID Settings page (**Setup** menu > **Signaling & Media** tab > **Media** folder > **Fax/Modem/CID Settings**).

Figure 16-2: Fax/Modem/CID Settings Page

GENERAL		FAX RELAY	
Fax Transport Mode	T.38 Relay	Fax Relay Redundancy Depth	0
T.38 Version	T.38 version 0	Fax Relay Enhanced Redundancy Depth	4
Caller ID Transport Type	Mute	Fax Relay ECM Enable	Enable
Caller ID Type	Standard Bellcore	Fax Relay Max Rate (bps)	14400bps
V.21 Modem Transport Type	Disable	Fax Relay Rx/Tx Timeout (sec)	10
V.22 Modem Transport Type	Enable Bypass	FAX/MODEM BYPASS	
V.23 Modem Transport Type	Enable Bypass	Fax/Modem Bypass Coder Type	G711Alaw_64
V.32 Modem Transport Type	Enable Bypass	Fax/Modem Bypass Packing Factor	1
V.34 Modem Transport Type	Enable Bypass	Fax Bypass Output Gain	0
Fax CNG Mode	Doesn't send T.38 re-INV	Modem Bypass Output Gain	0
CNG Detector Mode	Disable		

2. Configure the parameters, as required.
3. Click **Apply**.

16.2.1 Fax/Modem Operating Modes

The device supports two modes of operation:

- Fax/modem negotiation that is not performed during the establishment of the call.
- Voice-band data (VBD) mode for V.152 implementation (see "V.152 Support" on page 185): fax/modem capabilities are negotiated between the device and the remote endpoint at the establishment of the call. During a call, when a fax/modem signal is detected, transition from voice to VBD (or T.38) is automatically performed and no additional SIP signaling is required. If negotiation fails (i.e., no match is achieved for any of the transport capabilities), fallback to existing logic occurs (according to the parameter `IsFaxUsed`).

16.2.2 Fax/Modem Transport Modes

The device supports the following transport modes for fax per modem type (V.22/V.23/Bell/V.32/V.34):

- T.38 fax relay (see "T.38 Fax Relay Mode" on page 176)
- G.711 Transport: switching to G.711 when fax/modem is detected (see "G.711 Fax / Modem Transport Mode" on page 179)
- Fax fallback to G.711 if T.38 is not supported (see "Fax Fallback" on page 179)
- Fax and modem bypass: a proprietary method that uses a high bit rate coder (see "Fax/Modem Bypass Mode" on page 180)
- NSE Cisco's Pass-through bypass mode for fax and modem (see "Fax / Modem NSE Mode" on page 181)
- Transparent with events: passing the fax / modem signal in the current voice coder with adaptations (see "Fax / Modem Transparent with Events Mode" on page 182)
- Transparent: passing the fax / modem signal in the current voice coder (see "Fax / Modem Transparent Mode" on page 182)
- RFC 2833 ANS Report upon Fax/Modem Detection (see "RFC 2833 ANS Report upon Fax/Modem Detection" on page 183)

'Adaptations' refer to automatic reconfiguration of certain DSP features for handling fax/modem streams differently than voice.

16.2.2.1 T.38 Fax Relay Mode

In Fax Relay mode, fax signals are transferred using the T.38 protocol. T.38 is the ITU standard for sending fax across IP networks in real-time mode. The device currently supports only the T.38 UDP syntax.

T.38 can be configured in the following ways:

- Switching to T.38 mode using SIP Re-INVITE messages (see "Switching to T.38 Mode using SIP Re-INVITE" on page 177)
- Automatically switching to T.38 mode without using SIP Re-INVITE messages (see "Automatically Switching to T.38 Mode without SIP Re-INVITE" on page 177)

When fax transmission ends, the reverse switching from fax relay to voice is automatically performed at both the local and remote endpoints.

You can change the fax rate declared in the SDP, using the 'Fax Relay Max Rate' parameter (`FaxRelayMaxRate`). The parameter does not affect the actual transmission rate. You can also enable or disable Error Correction Mode (ECM) fax mode using the 'Fax Relay ECM Enable' parameter (`FaxRelayECMEnable`).

When using T.38 mode, you can define a redundancy feature to improve fax transmission over congested IP networks. This feature is activated using the 'Fax Relay Redundancy

Depth' parameter (FaxRelayRedundancyDepth) and the 'Fax Relay Enhanced Redundancy Depth' parameter (FaxRelayEnhancedRedundancyDepth). Although this is a proprietary redundancy scheme, it should not create problems when working with other T.38 decoders.

16.2.2.1.1 Switching to T.38 Mode using SIP Re-INVITE

In the Switching to T.38 Mode using SIP Re-INVITE mode, upon detection of a fax signal the terminating device negotiates T.38 capabilities using a Re-INVITE message. If the far-end device doesn't support T.38, the fax fails. In this mode, the 'Fax Transport Mode' parameter (FaxTransportMode) is ignored.

➤ To configure T.38 mode using SIP Re-INVITE messages:

1. Open the Gateway General Settings page (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Gateway General Settings**), and then from the 'Fax Signaling Method' drop-down list (IsFaxUsed), select **T.38 Relay**:

Figure 16-3: Configuring Fax Signaling to T.38

Fax Signaling Method

2. On the Fax/Modem/CID Settings page, configure the following optional parameters:
 - 'Fax Relay Redundancy Depth' (FaxRelayRedundancyDepth)
 - 'Fax Relay Enhanced Redundancy Depth' (FaxRelayEnhancedRedundancyDepth)
 - 'Fax Relay ECM Enable' (FaxRelayECMEnable)
 - 'Fax Relay Max Rate' (FaxRelayMaxRate)



Note: The terminating gateway sends T.38 packets immediately after the T.38 capabilities are negotiated in SIP. However, the originating device by default, sends T.38 (assuming the T.38 capabilities are negotiated in SIP) only after it receives T.38 packets from the remote device. This default behavior cannot be used when the originating device is located behind a firewall that blocks incoming T.38 packets on ports that have not yet received T.38 packets from the internal network. To resolve this problem, the device should be configured to send CNG packets in T.38 upon CNG signal detection (CNGDetectorMode = 1).

16.2.2.1.2 Automatically Switching to T.38 Mode without SIP Re-INVITE

In the Automatically Switching to T.38 Mode without SIP Re-INVITE mode, when a fax signal is detected, the channel automatically switches from the current voice coder to answer tone mode and then to T.38-compliant fax relay mode.

➤ To configure automatic T.38 mode:

1. Open the Gateway General Settings page (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Gateway General Settings**), and then from the 'Fax Signaling Method' drop-down list (IsFaxUsed), select **No Fax**:

Figure 16-4: Configuring Fax Signaling to None

Fax Signaling Method

2. On the Fax/Modem/CID Settings page, set the 'Fax Transport Mode' parameter to **T.38 Relay** (FaxTransportMode = 1).

3. Configure the following optional parameters:
 - 'Fax Relay Redundancy Depth' (FaxRelayRedundancyDepth)
 - 'Fax Relay Enhanced Redundancy Depth' (FaxRelayEnhancedRedundancyDepth)
 - 'Fax Relay ECM Enable' (FaxRelayECMEnable)
 - 'Fax Relay Max Rate' (FaxRelayMaxRate)

16.2.2.1.3 Fax over IP using T.38 Transmission over RTP

The device supports Fax-over-IP (FoIP) transmission using T.38 over RTP, whereby the T.38 payload is encapsulated in the RTP packet, instead of being sent in dedicated T.38 packets (out-of-band). To configure this support, set the coder type to T.38 Over RTP.

To indicate T.38 over RTP, the SDP body uses "udptl" (Facsimile UDP Transport Layer) in the 'a=fmtp' line. The device supports T.38 over RTP according to this standard as well as according to AudioCodes proprietary method:

- **Call Parties belong to AudioCodes Devices:** AudioCodes proprietary T.38-over-RTP method is used, whereby the device encapsulates the entire T.38 packet (payload with all its headers) in the sent RTP. For T.38 over RTP, AudioCodes devices use the proprietary identifier "AcUdptl" in the 'a=fmtp' line of the SDP. For example:

```
v=0
o=AudiocodesGW 1357424688 1357424660 IN IP4 10.8.6.68
s=Phone-Call
c=IN IP4 10.8.6.68
t=0 0
m=audio 6080 RTP/AVP 18 100 96
a=ptime:20
a=sendrecv
a=rtpmap:18 G729/8000
a=fmtp:18 annexb=no
a=rtpmap:100 t38/8000
a=fmtp:100 T38FaxVersion=0
a=fmtp:100 T38MaxBitRate=0
a=fmtp:100 T38FaxMaxBuffer=3000
a=fmtp:100 T38FaxMaxDatagram=122
a=fmtp:100 T38FaxRateManagement=transferredTCF
a=fmtp:100 T38FaxUdpEC=t38UDPRedundancy
a=fmtp:100 AcUdptl
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
```

- **AudioCodes Call Party with non-AudioCodes Party:** The device uses the standard T.38-over-RTP method, which encapsulates the T.38 payload only, without its headers (i.e., includes only fax data) in the sent RTP packet (RFC 4612).

The T.38-over-RTP method also depends on call initiator:

- **Device initiates a call:** The device always sends the SDP offer with the proprietary token "AcUdpTI" in the 'fmtp' attribute. If the SDP answer includes the same token, the device employs AudioCodes proprietary T.38-over-RTP mode; otherwise, the standard mode is used.
- **Device answers a call:** If the SDP offer from the remote party contains the 'fmtp' attribute with "AcUdpTI", the device answers with the same attribute and employs AudioCodes proprietary T.38-over-RTP mode; otherwise, the standard mode is used.



Note: If both T.38 (regular) and T.38 Over RTP coders are negotiated between the call parties, the device uses T.38 Over RTP.

16.2.2.2 G.711 Fax / Modem Transport Mode

In this mode, when the terminating device detects fax or modem signals (CED or AnsAM), it sends a Re-INVITE message to the originating device, requesting it to re-open the channel in G.711 VBD with the following adaptations:

- Echo Canceller = off
- Silence Compression = off
- Echo Canceller Non-Linear Processor Mode = off
- Dynamic Jitter Buffer Minimum Delay = 40
- Dynamic Jitter Buffer Optimization Factor = 13

After a few seconds upon detection of fax V.21 preamble or super G3 fax signals, the device sends a second Re-INVITE enabling the echo canceller (the echo canceller is disabled only on modem transmission).

A 'gpmd' attribute is added to the SDP according to the following format:

- **For G.711 A-law:**

```
a=gpmd:0 vbd=yes;ecan=on (or off for modems)
```

- **For G.711 μ -law:**

```
a=gpmd:8 vbd=yes;ecan=on (or off for modems)
```

The following parameters are ignored and automatically set to **Events Only**:

- 'Fax Transport Mode' (FaxTransportMode)
- 'Vxx ModemTransportType' (VxxModemTransportType)

➤ **To configure fax / modem transparent mode:**

1. Open the Gateway General Settings page (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Gateway General Settings**), and then from the 'Fax Signaling Method' drop-down list (IsFaxUsed), select **G.711 Transport**:

Figure 16-5: Configuring Fax Signaling to G.711



2. Click **Apply**.

16.2.2.3 Fax Fallback

In this mode, when the terminating device detects a fax signal, it sends a Re-INVITE message to the originating device with T.38. If the remote device doesn't support T.38 (replies with SIP response 415 "Media Not Supported"), the device sends a new Re-INVITE with G.711 VBD with the following adaptations:

- Echo Canceller = on
- Silence Compression = off
- Echo Canceller Non-Linear Processor Mode = off
- Dynamic Jitter Buffer Minimum Delay = 40
- Dynamic Jitter Buffer Optimization Factor = 13

When the device initiates a fax session using G.711, a 'gpmd' attribute is added to the SDP according to the following format:

■ **For G.711A-law:**

```
a=gpmd:0 vbd=yes;ecan=on
```

■ **For G.711 μ-law:**

```
a=gpmd:8 vbd=yes;ecan=on
```

In this mode, the 'Fax Transport Mode' (FaxTransportMode) parameter is ignored and automatically set to **Disable** (transparent mode).

➤ **To configure fax fallback mode:**

1. Open the Gateway General Settings page (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Gateway General Settings**), and then from the 'Fax Signaling Method' drop-down list (IsFaxUsed), select **Fax Fallback**:

Figure 16-6: Configuring Fax Signaling to Fallback



2. Click **Apply**.

16.2.2.4 Fax/Modem Bypass Mode

In this proprietary mode, when fax or modem signals are detected, the channel automatically switches from the current voice coder to a high bit-rate coder, according to the 'Fax/Modem Bypass Coder Type' parameter (FaxModemBypassCoderType). The channel is also automatically reconfigured with the following fax / modem adaptations:

- Disables silence suppression
- Enables echo cancellation for fax
- Disables echo cancellation for modem
- Performs certain jitter buffering optimizations

The network packets generated and received during the bypass period are regular voice RTP packets (per the selected bypass coder), but with a different RTP payload type according to the following parameters:

- 'Fax Bypass Payload Type' (FaxBypassPayloadType)
- ModemBypassPayloadType (ini file)

During the bypass period, the coder uses the packing factor, configured by the 'Fax/Modem Bypass Packing Factor' parameter (FaxModemBypassM). The packing factor determines the number of coder payloads (each the size of FaxModemBypassBasicRTTPacketInterval) that are used to generate a single fax/modem bypass packet. When fax/modem transmission ends, the reverse switching, from bypass coder to regular voice coder is performed.

➤ **To configure fax / modem bypass mode:**

1. Open the Gateway General Settings page (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Gateway General Settings**), and then from the 'Fax Signaling Method' drop-down list (IsFaxUsed), select **No Fax**.
2. On the Fax/Modem/CID Settings page, do the following:
 - a. Set the 'Fax Transport Mode' parameter to **Bypass** (FaxTransportMode = 2).
 - b. Set the 'V.21 Modem Transport Type' parameter to **Enable Bypass** (V21ModemTransportType = 2).
 - c. Set the 'V.22 Modem Transport Type' parameter to **Enable Bypass** (V22ModemTransportType = 2).

- d. Set the 'V.23 Modem Transport Type' parameter to **Enable Bypass** (V23ModemTransportType = 2).
 - e. Set the 'V.32 Modem Transport Type' parameter to **Enable Bypass** (V32ModemTransportType = 2).
 - f. Set the 'V.34 Modem Transport Type' parameter to **Enable Bypass** (V34ModemTransportType = 2).
3. Set the ini file parameter, BellModemTransportType to 2 (Bypass).
 4. Configure the following optional parameters:
 - 'Fax/Modem Bypass Coder Type' (FaxModemBypassCoderType).
 - 'Fax Bypass Payload Type' (FaxBypassPayloadType).
 - ModemBypassPayloadType (ini file).
 - FaxModemBypassBasicRTPPacketInterval (ini file).
 - FaxModemBypasDJBuMinDelay (ini file).



Note: When the device is configured for modem bypass and T.38 fax, V.21 low-speed modems are not supported and fail as a result.



Tip: When the remote (non-AudioCodes) gateway uses the G.711 coder for voice and doesn't change the coder payload type for fax or modem transmission, it is recommended to use the Bypass mode with the following configuration:

- EnableFaxModemInbandNetworkDetection = 1.
- 'Fax/Modem Bypass Coder Type' = same coder used for voice.
- 'Fax/Modem Bypass Packing Factor'(FaxModemBypassM) = same interval as voice.
- ModemBypassPayloadType = 8 if voice coder is A-Law or 0 if voice coder is Mu-Law.

16.2.2.5 Fax / Modem NSE Mode

In this mode, fax and modem signals are transferred using Cisco-compatible Pass-through bypass mode. Upon detection of fax or modem answering tone signal, the terminating device sends three to six special NSE RTP packets (configured by the NSEpayloadType parameter; usually to 100). These packets signal the remote device to switch to G.711 coder, according to the 'Fax/Modem Bypass Packing Factor' parameter. After a few NSE packets are exchanged between the devices, both devices start using G.711 packets with standard payload type (8 for G.711 A-Law and 0 for G.711 Mu-Law). In this mode, no Re-INVITE messages are sent. The voice channel is optimized for fax/modem transmission (same as for usual bypass mode).

The parameters defining payload type for AudioCodes proprietary Bypass mode -- 'Fax Bypass Payload Type' (RTP/RTCP Settings page) and ModemBypassPayloadType (ini file) -- are not used with NSE Bypass.

When configured for NSE mode, the device includes in its SDP the following line:

```
a=rtpmap:100 X-NSE/8000
```

Where 100 is the NSE payload type.

The Cisco gateway must include the following definition:

```
modem passthrough nse payload-type 100 codec g711alaw
```

- **To configure NSE mode:**
- 1. Open the Gateway General Settings page (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Gateway General Settings**), and then from the 'Fax Signaling Method' drop-down list (IsFaxUsed), select **No Fax**.
- 2. On the Fax/Modem/CID Settings page, do the following:
 - a. Set the 'Fax Transport Mode' parameter to **Bypass** (FaxTransportMode = 2).
 - b. Set the 'V.21 Modem Transport Type' parameter to **Enable Bypass** (V21ModemTransportType = 2).
 - c. Set the 'V.22 Modem Transport Type' parameter to **Enable Bypass** (V22ModemTransportType = 2).
 - d. Set the 'V.23 Modem Transport Type' parameter to **Enable Bypass** (V23ModemTransportType = 2).
 - e. Set the 'V.32 Modem Transport Type' parameter to **Enable Bypass** (V32ModemTransportType = 2).
 - f. Set the 'V.34 Modem Transport Type' parameter to **Enable Bypass** (V34ModemTransportType = 2).
- 3. Set the ini file parameter, BellModemTransportType to 2 (Bypass).
- 4. Set the ini file parameter, NSEMode parameter to 1 (enables NSE).
- 5. Set the ini file parameter, NSEPayloadType parameter to 100.

16.2.2.6 Fax / Modem Transparent with Events Mode

In this mode, fax and modem signals are transferred using the current voice coder with the following automatic adaptations:

- Echo Canceller = on (or off for modems)
- Echo Canceller Non-Linear Processor Mode = off
- Jitter buffering optimizations

- **To configure fax / modem transparent with events mode:**
- 1. Open the Gateway General Settings page (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Gateway General Settings**), and then from the 'Fax Signaling Method' drop-down list (IsFaxUsed), select **No Fax**.
- 2. On the Fax/Modem/CID Settings page, do the following:
 - a. Set the 'Fax Transport Mode' parameter to **Events Only** (FaxTransportMode = 3).
 - b. Set the 'V.21 Modem Transport Type' parameter to **Events Only** (V21ModemTransportType = 3).
 - c. Set the 'V.22 Modem Transport Type' parameter to **Events Only** (V22ModemTransportType = 3).
 - d. Set the 'V.23 Modem Transport Type' parameter to **Events Only** (V23ModemTransportType = 3).
 - e. Set the 'V.32 Modem Transport Type' parameter to **Events Only** (V32ModemTransportType = 3).
 - f. Set the 'V.34 Modem Transport Type' parameter to **Events Only** (V34ModemTransportType = 3).
- 3. Set the ini file parameter, BellModemTransportType to 3 (transparent with events).

16.2.2.7 Fax / Modem Transparent Mode

In this mode, fax and modem signals are transferred using the current voice coder without notifications to the user and without automatic adaptations. It's possible to use Profiles (see

"Coders and Profiles" on page 379) to apply certain adaptations to the channel used for fax / modem. For example, to use the coder G.711, to set the jitter buffer optimization factor to 13, and to enable echo cancellation for fax and disable it for modem.

➤ **To configure fax / modem transparent mode:**

1. Open the Gateway General Settings page (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Gateway General Settings**), and then from the 'Fax Signaling Method' drop-down list (IsFaxUsed), select **No Fax**.
2. On the Fax/Modem/CID Settings page, do the following:
 - a. Set the 'Fax Transport Mode' parameter to **Disable** (FaxTransportMode = 0).
 - b. Set the 'V.21 Modem Transport Type' parameter to **Disable** (V21ModemTransportType = 0).
 - c. Set the 'V.22 Modem Transport Type' parameter to **Disable** (V22ModemTransportType = 0).
 - d. Set the 'V.23 Modem Transport Type' parameter to **Disable** (V23ModemTransportType = 0).
 - e. Set the 'V.32 Modem Transport Type' parameter to **Disable** (V32ModemTransportType = 0).
 - f. Set the 'V.34 Modem Transport Type' parameter to **Disable** (V34ModemTransportType = 0).
3. Set the ini file parameter, BellModemTransportType to 0 (transparent mode).
4. Configure the following optional parameters:
 - a. Coders in the Coders table - see "Configuring Coder Groups" on page 379.
 - b. 'Dynamic Jitter Buffer Optimization Factor' (DJBufOptFactor) - "Configuring the Dynamic Jitter Buffer" on page 186.
 - c. 'Silence Suppression' (EnableSilenceCompression) - "Configuring Silence Suppression" on page 173.
 - d. 'Echo Canceller' (EnableEchoCanceller) - see "Configuring Echo Cancellation" on page 173.



Note: This mode can be used for fax, but is not recommended for modem transmission. Instead, use the Bypass (see "Fax/Modem Bypass Mode" on page 180) or Transparent with Events modes (see "Fax / Modem Transparent with Events Mode" on page 182) for modem.

16.2.2.8 RFC 2833 ANS Report upon Fax/Modem Detection

The device (terminator gateway) sends RFC 2833 ANS/ANSam events upon detection of fax and/or modem answer tones (i.e., CED tone). This causes the originator to switch to fax/modem. The parameter is applicable only when the fax or modem transport type is set to bypass, Transparent-with-Events, V.152 VBD, or G.711 transport. When the device is located on the originator side, it ignores these RFC 2833 events

➤ **To configure RFC 2833 ANS Report upon fax/modem detection:**

1. Open the Gateway General Settings page (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Gateway General Settings**), and then from the 'Fax Signaling Method' drop-down list (IsFaxUsed), select **No Fax** or **Fax Fallback**.
2. On the Fax/Modem/CID Settings page, do the following:
 - a. Set the 'Fax Transport Mode' parameter to **Bypass** (FaxTransportMode = 2).

- b. Set the 'V.xx Modem Transport Type' parameters to **Enable Bypass** (VxxModemTransportType = 2).
3. Set the ini file parameter, FaxModemNTEMode to 1 (enables this feature).

16.2.3 V.34 Fax Support

V.34 fax machines can transmit data over IP to the remote side using various methods. The device supports the following modes for transporting V.34 fax data over IP:

- Bypass mechanism for V.34 fax transmission (see "Bypass Mechanism for V.34 Fax Transmission" on page 184)
- T.38 Version 0 relay mode, i.e., fallback to T.38 (see "Relay Mode for T.30 and V.34 Faxes" on page 184)



Note: The CNG detector is disabled in all the subsequent examples. To disable the CNG detector, set the 'CNG Detector Mode' parameter (CNGDetectorMode) to **Disable**.

16.2.3.1 Bypass Mechanism for V.34 Fax Transmission

In this proprietary scenario, the device uses bypass (or NSE) mode to transmit V.34 faxes, enabling the full utilization of its speed.

- **To use bypass mode for T.30 and V.34 faxes:**
 1. On the Fax/Modem/CID Settings page, do the following:
 - a. Set the 'Fax Transport Mode' parameter to **Bypass** (FaxTransportMode = 2).
 - b. Set the 'V.22 Modem Transport Type' parameter to **Enable Bypass** (V22ModemTransportType = 2).
 - c. Set the 'V.23 Modem Transport Type' parameter to **Enable Bypass** (V23ModemTransportType = 2).
 - d. Set the 'V.32 Modem Transport Type' parameter to **Enable Bypass** (V32ModemTransportType = 2).
 - e. Set the 'V.34 Modem Transport Type' parameter to **Enable Bypass** (V34ModemTransportType = 2).
- **To use bypass mode for V.34 faxes, and T.38 for T.30 faxes:**
 1. On the Fax/Modem/CID Settings page, do the following:
 - a. Set the 'Fax Transport Mode' parameter to **T.38 Relay** (FaxTransportMode = 1).
 - b. Set the 'V.22 Modem Transport Type' parameter to **Enable Bypass** (V22ModemTransportType = 2).
 - c. Set the 'V.23 Modem Transport Type' parameter to **Enable Bypass** (V23ModemTransportType = 2).
 - d. Set the 'V.32 Modem Transport Type' parameter to **Enable Bypass** (V32ModemTransportType = 2).
 - e. Set the 'V.34 Modem Transport Type' parameter to **Enable Bypass** (V34ModemTransportType = 2).

16.2.3.2 Relay Mode for T.30 and V.34 Faxes

In this scenario, V.34 fax machines are forced to use their backward compatibility with T.30 faxes and operate in the slower T.30 mode.

➤ **To use T.38 mode for V.34 and T.30 faxes:**

1. On the Fax/Modem/CID Settings page, do the following:
 - a. Set the 'Fax Transport Mode' parameter to **T.38 Relay** (FaxTransportMode = 1).
 - b. Set the 'V.22 Modem Transport Type' parameter to **Disable** (V22ModemTransportType = 0).
 - c. Set the 'V.23 Modem Transport Type' parameter to **Disable** (V23ModemTransportType = 0).
 - d. Set the 'V.32 Modem Transport Type' parameter to **Disable** (V32ModemTransportType = 0).
 - e. Set the 'V.34 Modem Transport Type' parameter to **Disable** (V34ModemTransportType = 0).

16.2.4 V.152 Support

The device supports the ITU-T recommendation V.152 (Procedures for Supporting Voice-Band Data over IP Networks). Voice-band data (VBD) is the transport of modem, facsimile, and text telephony signals over a voice channel of a packet network with a codec appropriate for such signals.

For V.152 capability, the device supports T.38 as well as VBD codecs (i.e., G.711 A-law and G.711 μ -law). The selection of capabilities is performed using the Coder Groups table (see "Configuring Coder Groups" on page 379).

When in VBD mode for V.152 implementation, support is negotiated between the device and the remote endpoint at the establishment of the call. During this time, initial exchange of call capabilities is exchanged in the outgoing SDP. These capabilities include whether VBD is supported and associated RTP payload types ('gpmd' SDP attribute), supported codecs, and packetization periods for all codec payload types ('ptime' SDP attribute). After this initial negotiation, no Re-INVITE messages are necessary as both endpoints are synchronized in terms of the other side's capabilities. If negotiation fails (i.e., no match was achieved for any of the transport capabilities), fallback to existing logic occurs (according to the parameter IsFaxUsed).

Below is an example of media descriptions of an SDP indicating support for V.152. In the example, V.152 implementation is supported (using the dynamic payload type 96 and G.711 u-law as the VBD codec) as well as the voice codecs G.711 μ -law and G.729.

```
v=0
o=- 0 0 IN IPV4 <IPAddressA>
s=-
t=0 0
p=+1
c=IN IP4 <IPAddressA>
m=audio <udpPort A> RTP/AVP 18 0
a=ptime:10
a=rtpmap:96 PCMU/8000
a=gpmd: 96 vbd=yes
```

Instead of using VBD transport mode, the V.152 implementation can use alternative relay fax transport methods (e.g., fax relay over IP using T.38). The preferred V.152 transport method is indicated by the SDP 'pmft' attribute. Omission of this attribute in the SDP content means that VBD mode is the preferred transport mechanism for voice-band data.

16.3 Configuring RTP/RTCP Settings

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

16.3.1 Configuring the Dynamic Jitter Buffer

Voice frames are transmitted at a fixed rate. If the frames arrive at the other end at the same rate, voice quality is perceived as good. However, some frames may arrive slightly faster or slower than the other frames. This is called jitter (delay variation) and degrades the perceived voice quality. To minimize this problem, the device uses a jitter buffer. The jitter buffer collects voice packets, stores them and sends them to the voice processor in evenly spaced intervals.

The device uses a dynamic jitter buffer that can be configured with the following:

- **Minimum delay:** Defines the starting jitter capacity of the buffer. For example, at 0 msec, there is no buffering at the start. At the default level of 10 msec, the device always buffers incoming packets by at least 10 msec worth of voice frames.
- **Optimization Factor:** Defines how the jitter buffer tracks to changing network conditions. When set at its maximum value of 12, the dynamic buffer aggressively tracks changes in delay (based on packet loss statistics) to increase the size of the buffer and doesn't decay back down. This results in the best packet error performance, but at the cost of extra delay. At the minimum value of 0, the buffer tracks delays only to compensate for clock drift and quickly decays back to the minimum level. This optimizes the delay performance but at the expense of a higher error rate.

The default settings of 10 msec Minimum delay and 10 Optimization Factor should provide a good compromise between delay and error rate. The jitter buffer 'holds' incoming packets for 10 msec before making them available for decoding into voice. The coder polls frames from the buffer at regular intervals in order to produce continuous speech. As long as delays in the network do not change (jitter) by more than 10 msec from one packet to the next, there is always a sample in the buffer for the coder to use. If there is more than 10 msec of delay at any time during the call, the packet arrives too late. The coder tries to access a frame and is not able to find one. The coder must produce a voice sample even if a frame is not available. It therefore compensates for the missing packet by adding a Bad-Frame-Interpolation (BFI) packet. This loss is then flagged as the buffer being too small. The dynamic algorithm then causes the size of the buffer to increase for the next voice session. The size of the buffer may decrease again if the device notices that the buffer is not filling up as much as expected. At no time does the buffer decrease to less than the minimum size configured by the Minimum delay parameter.

In certain scenarios, the **Optimization Factor is set to 13**: One of the purposes of the Jitter Buffer mechanism is to compensate for clock drift. If the two sides of the VoIP call are not synchronized to the same clock source, one RTP source generates packets at a lower rate, causing under-runs at the remote Jitter Buffer. In normal operation (optimization factor 0 to 12), the Jitter Buffer mechanism detects and compensates for the clock drift by occasionally dropping a voice packet or by adding a BFI packet.

Fax and modem devices are sensitive to small packet losses or to added BFI packets. Therefore, to achieve better performance during modem and fax calls, the Optimization Factor should be set to 13. In this special mode the clock drift correction is performed less frequently - only when the Jitter Buffer is completely empty or completely full. When such condition occurs, the correction is performed by dropping several voice packets simultaneously or by adding several BFI packets simultaneously, so that the Jitter Buffer returns to its normal condition.

The following procedure describes how to configure the jitter buffer using the Web interface.

➤ **To configure jitter buffer using the Web interface:**

1. Open the RTP/RTCP Settings page (**Setup** menu > **Signaling & Media** menu > **Media** folder > **RTP/RTCP Settings**). The relevant parameters are listed under the General group, as shown below:
2. Set the 'Dynamic Jitter Buffer Minimum Delay' parameter (DJBufMinDelay) to the minimum delay (in msec) for the Dynamic Jitter Buffer.

3. Set the 'Dynamic Jitter Buffer Optimization Factor' parameter (DJBufOptFactor) to the Dynamic Jitter Buffer frame error/delay optimization factor.
4. Click **Apply**.

16.3.2 Configuring RFC 2833 Payload

The following procedure describes how to configure the RFC 2833 payload through the Web interface:

➤ **To configure RFC 2833 payload:**

1. Open the RTP/RTCP Settings page (**Setup** menu > **Signaling & Media** tab > **Media** folder > **RTP/RTCP Settings**).
2. Configure the following parameters:
 - 'RTP Redundancy Depth' (RTPRedundancyDepth) - enables the device to generate RFC 2198 redundant packets.
 - 'RFC 2833 TX Payload Type' (RFC2833TxPayloadType) - defines the Tx RFC 2833 DTMF relay dynamic payload type.
 - 'RFC 2833 RX Payload Type' (RFC2833RxPayloadType) - defines the Rx RFC 2833 DTMF relay dynamic payload type.
 - 'RFC 2198 Payload Type' (RFC2198PayloadType) - defines the RTP redundancy packet payload type according to RFC 2198.
3. Click **Apply**.

16.3.3 Configuring RTP Base UDP Port

You can configure the range (pool) of local UDP ports from which the device allocates ports to media (RTP, RTCP, and T.38) channels (legs). The maximum range of UDP ports is from 6,000 through to 65,535.

The consecutive port offset from the RTP port for RTCP and T.38 traffic is one and two, respectively. For example, if the voice session uses RTP port 6000, the device allocates ports 6001 and 6002 for RTCP and T.38, respectively. However, you can configure the device to use the same port for RTP and T.38 packets, by configuring the T38UseRTPPort parameter to 1.

Within the port range, the device allocates the UDP ports per media channel (leg) in "jumps" (spacing) of 4, 5 (default) or 10, configured by the UdpPortSpacing parameter. For example, if the port range starts at 6000 and the UDP port spacing is 10, the available ports are 6000, 6010, 6020, 6030, and so on. Within the port range, the device assigns these ports **randomly** to the different media channels. For example, it allocates port 6000 to leg 1, port 6030 to leg 2, and port 6010 to leg 3.

You can configure the starting port (lower boundary) of the port range (default is 6000), using the BaseUDPPort parameter. Once configured, the port range is according to the following equation:

```
<BaseUDPPort parameter value> to 65,535
```

Where, *number of channels* is the maximum number of purchased channels for the device (included in the installed License Key).

For example, if you configure the BaseUDPPort parameter to 6000, the port range is 6000 to 65,535.

You can also configure specific port ranges for specific SIP entities, using Media Realms (see "Configuring Media Realms" on page 303). You can configure each Media Realm with a different UDP port range and then associate the Media Realm with a specific IP Group, for example. However, the port range of the Media Realm **must be within the range** configured by the BaseUDPPort parameter.

The following procedure describes how to configure the RTP base UDP port through the Web interface.

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

1. Open the RTP/RTCP Settings page (**Setup** menu > **Signaling & Media** tab > **Media** folder > **RTP/RTCP Settings**).
2. In the 'RTP Base UDP Port' field, configure the lower boundary of the UDP port range.

Figure 16-7: Configuring RTP Base UDP Port

RTP Base UDP Port ⚡

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



Note:

- The RTP port must be different from ports configured for SIP signaling traffic (i.e., ports configured for SIP Interfaces). For example, if the RTP port range is 6000 to 6999, the SIP port can either be less than 6000 or greater than 6999.
- The base UDP port number (BaseUDPPort parameter) must be greater than the highest UDP port configured for a SIP Interface (see "Configuring SIP Interfaces" on page 321). For example, if your highest configured UDP port for a SIP Interface is 6060, you must configure the BaseUDPPort parameter to any value greater than 6060.

16.4 Event Detection and Notification using X-Detect Header

The device can detect certain events in the media stream and notify of their detection to a remote application server, using the SIP X-Detect header. The request for event notification is done by the application server when establishing a SIP dialog (i.e., INVITE message) or during an already established call using a re-INVITE message.

The device can detect the following event types:

- Answering Machine Detection (AMD): Detects events that are related to the AMD feature. AMD detects whether an answering machine or live voice has answered the call. It can also be used to detect silence, or the beep sound played by an answering machine to indicate the end of the greeting message after which a voice message can be left. For more information on AMD, see "Answering Machine Detection (AMD)" on page 192.
- Call Progress Tone (CPT): Detects whether a specific tone, defined in the installed CPT file is received from the call. It can be used to detect the beep sound played by an answering machine (as mentioned above) and the busy, reorder and ring tones.



Note: Event detection is supported only for calls using the G.711 coder.

The X-Detect header is used for event detection as follows:

- X-Detect header in the INVITE message received from the application server requesting a specific event detection:

```
X-Detect: Request=[event type to detect]
```
- X-Detect header in the SIP response message -- SIP 183 (for early dialogs) or 200 OK (for confirmed dialogs) -- sent by the device to the application server specifying which of the requested events it can detect (absence of the X-Detect header indicates that the device cannot detect any of the events):

```
X-Detect: Response=[supported event types]
```
- Each time the device detects the supported event, it sends an INFO message to the remote party with the following message body:

```
Content-Type: Application/X-Detect
Type = [event type]
Subtype = [subtype of each event type]
```

The table below lists the event types and subtypes that can be detected by the device. The text shown in the table are the strings used in the X-Detect header. The table also provides a summary of the required configuration. For SBC calls, event detection is enabled using the IPProfile_SBCHandleXDetect parameter in the IP Profiles table (see Configuring IP Profiles on page 388).

Table 16-1: Supported X-Detect Event Types

Event Type	Subtype	Description and Required Configuration
AMD	<ul style="list-style-type: none"> ▪ Voice (live voice) ▪ Automata (answering machine) ▪ Silence (no voice) ▪ Unknown ▪ Beep (greeting message of answering machine) 	Event detection using the AMD feature. For more information, see Answering Machine Detection (AMD) on page 192.
CPT	<ul style="list-style-type: none"> ▪ Busy ▪ Reorder ▪ Ringtone ▪ Beep (greeting message of answering message) 	Event detection of tones using the CPT file. <ol style="list-style-type: none"> 1 Create a CPT file with the required tone types of the events that you want to detect. 2 Install the CPT file on the device. <p>Note: To configure beep detection, see Detecting Answering Machine Beep on page 189.</p>

16.4.1 Detecting Answering Machine Beeps

The device can detect the "beep" sound played by an answering machine that indicates the end of the answering machine's greeting message. This is useful in that the device can then notify, for example, a third-party, application server that it can now leave a voice message on the answering machine. The device supports the following methods for detecting and reporting beeps:

- **AMD-based Detection:** The device uses its beep detector that is integrated in the AMD feature. You can configure the beep detection timeout and beep detection sensitivity level (for more information, see "Configuring AMD" on page 195). To enable the AMD beep detection, the received INVITE message must contain an X-Detect header with the value "Request=AMD",

```
X-Detect: Request=AMD
```

and the `AMDBeepDetectionMode` parameter must be set to 1 or 2. If set to 1, the beep is detected only after the answering machine is detected. If set to 2, the beep is detected even if the answering machine was not detected.

- **Tone-based Detection (Call Progress Tone):** The device detects the beep according to a call progress tone (CPT). This is enabled if the device receives a specific beep tone (Tone Type #46) that is also defined in the installed CPT file and the received INVITE message contains an X-Detect header with the value "Request=CPT":

```
X-Detect: Request=CPT
```

For more information on the CPT file, see "Call Progress Tones File" on page 587.

The device reports beep detections to application servers, by sending a SIP INFO message that contains a body with one of the following values, depending on the method used for detecting the beep:

- **AMD-detected Beep:**

```
Type= AMD
SubType= Beep
```

- **CPT-detected Beep:**

```
Type= CPT
SubType=Beep
```

16.4.2 SIP Call Flow Examples of Event Detection and Notification

Two SIP call flow examples are provided below of event detection and notification:

- The following example shows a SIP call flow of the device's AMD and event detection feature, whereby the device detects an answering machine and the subsequent start and end of the greeting message, enabling the third-party application server to know when to play a recorded voice message to an answering machine:

1. Upon detection of the answering machine, the device sends the following SIP INFO message to the application server:

```
INFO sip:sipp@172.22.2.9:5060 SIP/2.0
Via: SIP/2.0/UDP 172.22.168.249;branch=z9hG4bKac1566945480
Max-Forwards: 70
From: sut <sip:3000@172.22.168.249:5060>;tag=1c1505895240
To: sipp <sip:sipp@172.22.2.9:5060>;tag=1
Call-ID: 1-29758@172.22.2.9
CSeq: 1 INFO
Contact: <sip:56700@172.22.168.249>
Supported: em,timer,replaces,path,resource-priority
Allow:
REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
User-Agent: Audiocodes-Sip-Gateway/v.7.20A.000.038
Content-Type: application/x-detect
Content-Length: 30
Type= AMD
SubType= AUTOMATA
```

2. Upon detection of the start of voice (i.e., the greeting message of the answering machine), the device sends the following INFO message to the application server:

```
INFO sip:sipp@172.22.2.9:5060 SIP/2.0
Via: SIP/2.0/UDP 172.22.168.249;branch=z9hG4bKac482466515
Max-Forwards: 70
From: sut <sip:3000@172.22.168.249:5060>;tag=1c419779142
```

```
To: sipp <sip:sipp@172.22.2.9:5060>;tag=1
Call-ID: 1-29753@172.22.2.9
CSeq: 1 INFO
Contact: <sip:56700@172.22.168.249>
Supported: em,timer,replaces,path,resource-priority
Allow:
REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
User-Agent: Audiocodes-Sip-Gateway/v.7.20A.000.038
Content-Type: application/x-detect
Content-Length: 34
Type= PTT
SubType= SPEECH-START
```

3. Upon detection of the end of voice (i.e., end of the greeting message of the answering machine), the device sends the following INFO message to the application server:

```
INFO sip:sipp@172.22.2.9:5060 SIP/2.0
Via: SIP/2.0/UDP 172.22.168.249;branch=z9hG4bKac482466515
Max-Forwards: 70
From: sut <sip:3000@172.22.168.249:5060>;tag=1c419779142
To: sipp <sip:sipp@172.22.2.9:5060>;tag=1
Call-ID: 1-29753@172.22.2.9
CSeq: 1 INFO
Contact: <sip:56700@172.22.168.249>
Supported: em,timer,replaces,path,resource-priority
Allow:
REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
User-Agent: Audiocodes-Sip-Gateway/v.7.20A.000.038
Content-Type: application/x-detect
Content-Length: 34
Type= PTT
SubType= SPEECH-END
```

4. The application server sends its message to leave on the answering message.

- The following example shows a SIP call flow for event detection and notification of the beep of an answering machine:

1. The device receives a SIP message containing the X-Detect header from the remote application requesting beep detection:

```
INVITE sip:101@10.33.2.53;user=phone SIP/2.0
Via: SIP/2.0/UDP 10.33.2.53;branch=z9hG4bKac5906
Max-Forwards: 70
From: "anonymous"
<sip:anonymous@anonymous.invalid>;tag=1c25298
To: <sip:101@10.33.2.53;user=phone>
Call-ID: 11923@10.33.2.53
CSeq: 1 INVITE
Contact: <sip:100@10.33.2.53>
X-Detect: Request=AMD,CPT
```

2. The device sends a SIP response message to the remote party, listing the events in the X-Detect header that it can detect:

```
SIP/2.0 200 OK
Via: SIP/2.0/UDP 10.33.2.53;branch=z9hG4bKac5906
From: "anonymous"
<sip:anonymous@anonymous.invalid>;tag=1c25298
To: <sip:101@10.33.2.53;user=phone>;tag=1c19282
Call-ID: 11923@10.33.2.53
```

```
CSeq: 1 INVITE
Contact: <sip:101@10.33.2.53>
X-Detect: Response=AMD,CPT
```

3. The device detects the beep of an answering machine and sends an INFO message to the remote party:

```
INFO sip:101@10.33.2.53;user=phone SIP/2.0
Via: SIP/2.0/UDP 10.33.2.53;branch=z9hG4bKac5906
Max-Forwards: 70
From: "anonymous"
<sip:anonymous@anonymous.invalid>;tag=1c25298
To: <sip:101@10.33.2.53;user=phone>
Call-ID: 11923@10.33.2.53
CSeq: 1 INVITE
Contact: <sip:100@10.33.2.53>
X-Detect: Response=AMD,CPT
Content-Type: Application/X-Detect
Content-Length: xxx
Type = CPT
Subtype = Beep
```

16.5 Answering Machine Detection (AMD)

The device's Answering Machine Detection (AMD) feature can detect whether an outbound call has been answered by a human (including fax) or an answering machine. The device analyzes the sound (speech) patterns received in the first few seconds of the call to determine whether a human (live person) or machine has answered the call. Typically, when a human answers the call, there is a short "hello ..." followed by silence to wait for the other party to respond. In contrast, when an answering machine answers the call, there is constant speech (answering message) followed by a beep to leave a voice-mail message.

When the device detects what answered the call (human or machine), it can notify this detection type to, for example, a third-party application server used for automatic dialing applications. The X-Detect SIP header is used for requesting event detection and notification. For more information, see "Event Detection and Notification using X-Detect Header" on page 188. The device can also detect beeps played by an answering machine at the end of its greeting message. For more information, see "Detecting Answering Machine Beeps" on page 189.

The device's default AMD feature is based on voice detection for North American English (see note below). It uses AudioCodes' sophisticated speech detection algorithms which are based on hundreds of real-life recordings of answered calls by live voice and answering machines in English. The algorithms are used to detect whether it's human or machine based on voice and silence duration as well as speech patterns. The algorithms of the language-based recordings are compiled into a file called AMD Sensitivity. This file is provided by default, pre-installed on the device.



Note: As the main factor (algorithm) for detecting human and machine is the voice pattern and silence duration, the language on which the detection algorithm is based, is in most cases not important as these factors are similar across most languages. Therefore, the default, pre-installed AMD Sensitivity file, which is based on North American English, may suffice your deployment even if the device is located in a region where a language other than English is used.

However, if (despite the information stated in the note above) you wish to implement AMD in a different language or region, or if you wish to fine-tune the default AMD algorithms to suit your specific deployment, please contact your AudioCodes sales representative for more information on this service. You will be typically required to provide AudioCodes with

a database of recorded voices (calls) in the language on which the device's AMD feature can base its voice detector algorithms. The data needed for an accurate calibration should be recorded under the following guidelines:

- **Statistical accuracy:** The number of recorded calls should be as high as possible (at least 100) and varied. The calls must be made to different people. The calls must be made in the specific location in which the device's AMD feature is to operate.
- **Real-life recording:** The recordings should simulate real-life answering of a called person picking up the phone, and without the caller speaking.
- **Normal environment interferences:** The environment in which the recordings are done should simulate real-life scenarios, in other words, not sterile but not too noisy either. Interferences, for example, could include background noises of other people talking, spikes, and car noises.

Once you have provided AudioCodes with your database of recordings, AudioCodes compiles it into a loadable file. For a brief description of the file format and for installing the file on the device, see "AMD Sensitivity File" on page 597.

The device supports up to eight AMD algorithm suites called *Parameter Suites*, where each suite defines a range of detection sensitivity levels. Sensitivity levels refer to how accurately, based on AudioCodes' voice detection algorithms, the device can detect whether a human or machine has answered the call. Each level supports a different detection sensitivity to human and machine. For example, a specific sensitivity level may be more sensitive to detecting human than machine. In deployments where the likelihood of a call answered by an answering machine is low, it would be advisable to configure the device to use a sensitivity level that is more sensitive to human than machine. In addition, this allows you to tweak your sensitivity to meet local regulatory rules designed to protect consumers from automatic dialers (where, for example, the consumer picks up the phone and hears silence). Each suite can support up to 16 sensitivity levels (0 to 15), except for Parameter Suite 0, which supports up to 8 levels (0 to 7). The default, pre-installed AMD Sensitivity file, based on North American English, provides the following Parameter Suites:

- **Parameter Suite 0 (normal sensitivity)** - contains 8 sensitivity detection levels
- **Parameter Suite 1 (high sensitivity)** - contains 16 sensitivity detection levels

As Parameter Suite 1 provides a greater range of detection sensitivity levels (i.e., higher detection resolution), this may be the preferable suite to use in your deployment. The detected AMD type (human or machine) and success of detecting it correctly are sent in CDR and Syslog messages. For more information, see "Syslog Fields for Answering Machine Detection (AMD)" on page 702.

The Parameter Suite and sensitivity level can be applied globally for all calls, or for specific calls using IP Profiles. For enabling AMD and selecting the Parameter Suite and sensitivity level, see "Configuring AMD" on page 195.

The tables below show the success rates of the default, pre-installed AMD Sensitivity file (based on North American English) for correctly detecting "live" human voice and answering machine:

Table 16-2: Approximate AMD Normal Detection Sensitivity - Parameter Suite 0 (Based on North American English)

AMD Detection Sensitivity	Performance	
	Success Rate for Live Calls	Success Rate for Answering Machine
0 (Best for Answering Machine)	-	-
1	82.56%	97.10%

AMD Detection Sensitivity	Performance	
	Success Rate for Live Calls	Success Rate for Answering Machine
2	85.87%	96.43%
3	88.57%	94.76%
4	88.94%	94.31%
5	90.42%	91.64%
6	90.66%	91.30%
7 (Best for Live Calls)	94.72%	76.14%

Table 16-3: Approximate AMD High Detection Sensitivity - Parameter Suite 1 (Based on North American English)

AMD Detection Sensitivity	Performance	
	Success Rate for Live Calls	Success Rate for Answering Machine
0 (Best for Answering Machine)	72%	97%
1	77%	96%
2	79%	95%
3	80%	95%
4	84%	94%
5	86%	93%
6	87%	92%
7	88%	91%
8	90%	89%
9	90%	88%
10	91%	87%
11	94%	78%
12	94%	73%
13	95%	65%
14	96%	62%
15 (Best for Live Calls)	97%	46%

16.5.1 Configuring AMD

You can configure AMD for all calls using global AMD parameters or for specific calls using IP Profiles. The procedure below describes how to configure AMD for all calls. To configure AMD for specific calls, use the AMD parameters in the IP Profiles table (see "Configuring IP Profiles" on page 388).

➤ **To configure AMD for all calls:**

1. Open the DSP Settings page (**Setup** menu > **Signaling & Media** tab > **Media** folder > **DSP Settings**):
2. From the 'IPMedia Detectors' drop-down list (EnableDSPIPMDetectors), select **Enable** to enable AMD.
3. Scroll down to the Answer Machine Detector group:

Figure 16-8: Configuring AMD

ANSWER MACHINE DETECTOR	
Answer Machine Detector Sensitivity Parameter Suite	0
Answer Machine Detector Sensitivity	3
Answer Machine Detector Sensitivity Level	8
Answer Machine Detector Beep Detection Timeout	200
Answer Machine Detector Beep Detection Sensitivity	0

4. Select the AMD algorithm suite:
 - a. In the 'Answer Machine Detector Sensitivity Parameter Suite' field, select the required Parameter Suite included in the installed AMD Sensitivity file.
 - b. In the 'Answer Machine Detector Sensitivity' field, enter the required detection sensitivity level of the selected Parameter Suite.
5. Configure the answering machine beep detection:
 - a. In the 'Answer Machine Detector Beep Detection Timeout' field (AMDBeepDetectionTimeout), enter the duration that the beep detector operates from when detection is initiated.
 - b. In the 'Answer Machine Detector Beep Detection Sensitivity' field (AMDBeepDetectionSensitivity), enter the AMD beep detection sensitivity level.
6. Click **Apply**, and then reset the device with a save-to-flash for your settings to take effect.

For a complete list of AMD-related parameters, see "IP Media Parameters" on page 830.

16.6 Automatic Gain Control (AGC)

Automatic Gain Control (AGC) adjusts the energy of the output signal to a required level (volume). This feature compensates for near-far gain differences. AGC estimates the energy of the incoming signal from the IP, determined by the 'AGC Redirection' parameter, calculates the essential gain, and then performs amplification. Feedback ensures that the output signal is not clipped. You can configure the required Gain Slope in decibels per second using the 'AGC Slope' parameter and the required signal energy threshold using the 'AGC Target Energy' parameter.

When the AGC first detects an incoming signal, it begins operating in Fast Mode, which allows the AGC to adapt quickly when a conversation starts. This means that the Gain Slope is 8 dB/sec for the first 1.5 seconds. After this period, the Gain Slope is changed to the user-defined value. You can disable or enable the AGC's Fast Mode feature, using the *ini* file parameter *AGCDisableFastAdaptation*. After Fast Mode is used, the signal should be off for two minutes in order to have the feature turned on again.

The following procedure describes how to configure AGC using the Web interface:

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

1. Open the DSP Settings page (**Setup** menu > **Signaling & Media** tab > **Media** folder > **DSP Settings**):

Figure 16-9: AGC Parameters

AGC	
Enable AGC	Disable
AGC Slope	3
AGC Redirection	0
AGC Target Energy	19
AGC Minimum Gain	20
AGC Maximum Gain	15
AGC Disable Fast Adaptation	Disable

2. Configure the following parameters:
 - 'Enable AGC' (*EnableAGC*) - Enables the AGC mechanism.
 - 'AGC Slope' (*AGCGainSlope*) - Determines the AGC convergence rate.
 - 'AGC Redirection' (*AGCRedirection*) - Determines the AGC direction.
 - 'AGC Target Energy' - Defines the signal energy value (dBm) that the AGC attempts to attain.
 - 'AGC Minimum Gain' (*AGCMinGain*) - Defines the minimum gain (in dB) by the AGC when activated.
 - 'AGC Maximum Gain' (*AGCMaxGain*) - Defines the maximum gain (in dB) by the AGC when activated.
 - 'AGC Disable Fast Adaptation' (*AGCDisableFastAdaptation*) - Enables the AGC Fast Adaptation mode.
3. When using AGC with the SBC application, the 'Transcoding Mode' (*TranscodingMode*) parameter must be set to Force. The parameter can either be the global parameter or per IP Profile.
4. Click **Apply**.

16.7 Configuring Media (SRTP) 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 cryptographic key exchange mechanism to negotiate the keys. To negotiate the keys, the device supports the Session Description Protocol Security Descriptions (SDS) protocol (according to RFC 4568) or Datagram Transport Layer Security (DTLS) protocol for SBC calls. For more information on DTLS, see SRTP using DTLS Protocol on page 199. The key exchange is done by adding the '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 (SDP offer), it can generate a Master Key Identifier (MKI). You can configure the MKI size globally (using the SRTPTxPacketMKISize parameter) or per SIP entity (using the IP Profile parameter, IpProfile_MKISize). The length of the MKI is limited to four bytes. If the remote side sends a longer MKI, the key is ignored.



Note: The device can forward MKI size transparently for SRTP-to-SRTP media flows or override the MKI size during negotiation (inbound or outbound leg).

The key lifetime field is not supported. However, if it is included in the key it is ignored and the call does not fail. For SBC calls belonging to a specific SIP entity, you can configure the device to remove the lifetime field in the 'a=crypto' attribute (using the IP Profile parameter, IpProfile_SBCRemoveCryptoLifetimeInSDP).

For SDES, the keys are sent in the SDP body ('a=crypto') of the SIP message and are typically secured using SIP over TLS (SIPS). The encryption of the keys is in plain text in the SDP. The device supports the following session parameters:

- 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 forward the MKI size received in the SDP offer 'a=crypto' line in the SDP answer. You can enable symmetric MKI globally (using the EnableSymmetricMKI parameter) or per SIP entity (using the IP Profile parameter, IpProfile_EnableSymmetricMKI and IpProfile_SBCEnforceMKISize). For more information on symmetric MKI, see "Configuring IP Profiles" on page 388.

You can configure the enforcement policy of SRTP, using the IpProfile_SBCMediaSecurityBehaviour parameter. For example, if negotiation of the cipher suite fails or if incoming calls exclude encryption information, the device can be configured to reject the calls.



Note:

- For a detailed description of the SRTP parameters, see "Configuring IP Profiles" on page 388 and "SRTP Parameters" on page 769.
- When SRTP is used, the channel capacity may be reduced.

The procedure below describes how to configure SRTP through the Web interface.

➤ **To enable and configure SRTP:**

1. Open the Media Security page (**Setup** menu > **Signaling & Media** tab > **Media** folder > **Media Security**).

Figure 16-10: Configuring Media Security

GENERAL		AUTHENTICATION & ENCRYPTION	
Media Security	Disable	Authentication On Transmitted RTP Packets	Active
Media Security Behavior	Preferable	Encryption On Transmitted RTP Packets	Active
Offered SRTP Cipher Suites	All	Encryption On Transmitted RTCP Packets	Active
MASTER KEY IDENTIFIER		SRTP Tunneling Authentication for RTP	Disable
Master Key Identifier (MKI) Size	0	SRTP Tunneling Authentication for RTCP	Disable
Symmetric MKI	Disable	GATEWAY SETTINGS	
		Enable Rekey After 181	Disable

2. From the 'Media Security' drop-down list (EnableMediaSecurity), select **Enable** to enable SRTP.
3. Configure the other SRTP parameters as required.
4. Click **Apply**, and then reset the device with a save-to-flash for your settings to take effect.

16.7.1 SRTP using DTLS Protocol

For SBC calls, you can configure the device to use the Datagram Transport Layer Security (DTLS) protocol to secure UDP-based media streams (according to RFC 5763 and 5764) for specific SIP entities, using IP Profiles. DTLS allows datagram-based applications to communicate in a way that is designed to prevent eavesdropping, tampering or message forgery. The DTLS protocol is based on the stream-oriented TLS protocol, providing similar security. The device can therefore, interwork in mixed environments where one network may require DTLS and the other may require Session Description Protocol Security Descriptions (SDES) or even non-secure RTP. The device supports DTLS negotiation for RTP-to-SRTP and SRTP-to-SRTP calls.

DTLS support is important for deployments with WebRTC. WebRTC requires that media channels be encrypted through DTLS for SRTP key exchange. Negotiation of SRTP keys through DTLS is done during the DTLS handshake between WebRTC client and peer. For more information on WebRTC, see "WebRTC" on page 524.

In contrast to SDDES, DTLS key encryption is done over the media channel (UDP), not signaling. Thus, DTLS-SRTP is generally known as "secured key exchange over media". DTLS is similar to TLS, but runs over UDP, whereas TLS is over TCP. Before the DTLS handshake, the peers exchange DTLS parameters (fingerprint and setup) and algorithm types in the SDP body of the SIP messages exchanged for establishing the call (INVITE request and response). The peers participate in a DTLS handshake during which they exchange certificates. These certificates are used to derive a symmetric key, which is used to encrypt data (SRTP) flow between the peers. A hash value calculated over the certificate is transported in the SDP using the 'a=fingerprint' attribute. At the end of the handshake, each side verifies that the certificate it received from the other side fits the fingerprint from the SDP. To indicate DTLS support, the SDP offer/answer of the SIP message uses the 'a=setup' attribute. The 'a=setup:actpass' attribute value is used in the SDP offer by the device. This indicates that the device is willing to be either a client ('act') or a server ('pass') in the handshake. The 'a=setup:active' attribute value is used in the SDP answer by the device. This means that the device wishes to be the client ('active') in the handshake.

```
a=setup:actpass
a=fingerprint:SHA-1
\4A:AD:B9:B1:3F:82:18:3B:54:02:12:DF:3E:5D:49:6B:19:E5:7C:AB
```

DTLS cipher suite reuses the TLS cipher suite. The DTLS handshake is done for every new call configured for DTLS. In other words, unlike TLS where the connection remains "open" for future calls, a new DTLS connection is required for every new call. Note that the entire authentication and key exchange for securing the media traffic is handled in the media path through DTLS. The signaling path is used only to verify the peers' certificate fingerprints. DTLS messages are multiplexed onto the same ports that are used for the media.

➤ To configure DTLS:

1. In the TLS Context table (see "Configuring TLS Certificate Contexts" on page 99), configure a TLS Context for DTLS.
2. Open the IP Groups table (see "Configuring IP Groups" on page 329) and for the IP Group associated with the SIP entity, assign it the TLS Context for DTLS, using the 'DTLS Context' parameter (IPGroup_DTLSContext).
3. Open the IP Profiles table (see "Configuring IP Profiles" on page 388) and for the IP Profile associated with the SIP entity, configure the following:
 - Configure the 'SBC Media Security Mode' parameter (IPProfile_SBCMediaSecurityBehavior) to **SRTP** or **Both**.
 - Configure the 'Media Security Method' parameter (IPProfile_SBCMediaSecurityMethod) to **DTLS**.

- Configure the 'RTCP Mux' parameter (IpProfile_SBCRTCPMux) to **Supported**. Multiplexing is required as the DTLS handshake is done for the port used for RTP and thus, RTCP and RTP must be multiplexed onto the same port.
- Configure the ini file parameter, SbcDtlsMtu (or CLI command configure voip > sbc settings > sbc-dtls-mtu) to define the maximum transmission unit (MTU) size for the DTLS handshake.

**Note:**

- The 'Cipher Server' parameter must be configured to "ALL".
- The device does not support forwarding of DTLS transparently between endpoints.

17 Services

This section describes configuration for various supported services.

17.1 DHCP Server Functionality

The device can serve as a Dynamic Host Configuration Protocol (DHCP) server that assigns and manages IP addresses from a user-defined address pool for DHCP clients. The DHCP server can also be configured to supply additional information to the requesting client such as the IP address of the TFTP server, DNS server, NTP server, and default router (gateway). The DHCP server functionality complies with IETF RFC 2131 and RFC 2132.

The DHCP server can service up to 25,000 DHCP clients. The DHCP clients are typically IP phones that are connected to the device's LAN port.

The DHCP server is activated when you configure a valid entry in the DHCP Servers table (see "Configuring the DHCP Server" on page 201) and associate it with an active IP network interface (listed in the IP Interfaces table). When an IP phone on the LAN requests an IP address, the DHCP server allocates one from the address pool. In scenarios of duplicated IP addresses on the LAN (i.e., an unauthorized network device using one of the IP addresses of the DHCP address pool), the DHCP server detects this condition using an Address Resolution Protocol (ARP) request and temporarily blacklists the duplicated address.

You can also configure the DHCP server to respond **only** to DHCPDiscover requests from DHCP clients that contain a specific value for Option 60 (Vendor Class Identification). For more information, see "Configuring the Vendor Class Identifier" on page 206.

17.1.1 Configuring the DHCP Server

The DHCP Servers table lets you configure the device's DHCP server. The DHCP Server table configures the DHCP server implementation. This includes configuring the DHCP IP address pool from where IP addresses are allocated to requesting DHCP clients, as well as configuring other information such as IP addresses of the DNS server, NTP server, default router (gateway), and SIP proxy server. The DHCP server sends the information in DHCP Options. The table below lists the DHCP Options that the DHCP server sends to the DHCP client and which are configurable in the DHCP Servers table.

Table 17-1: Configurable DHCP Options in DHCP Servers Table

DHCP Option Code	DHCP Option Name
Option 53	DHCP Message Type
Option 54	DHCP Server Identifier
Option 51	IP Address Lease Time
Option 1	Subnet Mask
Option 3	Router
Option 6	Domain Name Server
Option 44	NetBIOS Name Server
Option 46	NetBIOS Node Type
Option 42	Network Time Protocol Server

DHCP Option Code	DHCP Option Name
Option 2	Time Offset
Option 66	TFTP Server Name
Option 67	Boot file Name
Option 120	SIP Server

Once you have configured the DHCP server, you can configure the following:

- DHCP Vendor Class Identifier names (DHCP Option 60) - see "Configuring the Vendor Class Identifier" on page 206
- Additional DHCP Options - see "Configuring Additional DHCP Options" on page 207
- Static IP addresses for DHCP clients - see "Configuring Static IP Addresses for DHCP Clients" on page 209



Note: If you configure additional DHCP Options in the DHCP Option table, they override the default ones, which are configured in the DHCP Servers table. For example, if you configure Option 67 in the DHCP Option table, the device uses the value configured in the DHCP Option table instead of the value configured in the DHCP Servers table.

To view and delete currently serviced DHCP clients, see "Viewing and Deleting DHCP Clients" on page 210.

The following procedure describes how to configure the DHCP server through the Web interface. You can also configure it through ini file (DhcpServer) or CLI (configure network > dhcp-server server <index>).

➤ **To configure the device's DHCP server:**

1. Open the DHCP Servers page (**Setup** menu > **IP Network** tab > **Advanced** folder > **DHCP Servers**).

- Click **New**; the following dialog box appears:

Figure 17-1: DHCP Servers Table - Add Dialog Box

The screenshot shows a dialog box titled "DHCP Servers" with the following sections and fields:

- GENERAL:** Index (0), Interface Name (dropdown menu with "--" and a "View" link), Start IP Address (192.168.0.100), End IP Address (192.168.0.149), Subnet Mask (255.255.255.0), Lease Time (1440).
- TIME AND DATE:** NTP Server 1 (0.0.0.0), NTP Server 2 (0.0.0.0), Time Offset (0).
- DNS:** DNS Server 1 (0.0.0.0), DNS Server 2 (0.0.0.0).
- BOOT FILE:** TFTP Server Name (empty), Boot File Name (empty), Expand Boot-File Name (Yes).
- ROUTER:** Override Router (0.0.0.0).

- Configure a DHCP server according to the parameters described in the table below.
- Click **Apply**.

Table 17-2: DHCP Servers Table Parameter Descriptions

Parameter	Description
General	
Index dhcp server <index>	Defines an index number for the new table row. Note: <ul style="list-style-type: none"> Each row must be configured with a unique index. Currently, only one index row can be configured.
Interface Name network-if [DhcpServer_InterfaceName]	Associates an IP interface on which the DHCP server operates. The IP interfaces are configured in the IP Interfaces table (see "Configuring IP Network Interfaces" on page 130). By default, no value is defined.
Start IP Address start-address [DhcpServer_StartIPAddress]	Defines the starting IP address (IPv4 address in dotted-decimal format) of the IP address pool range used by the DHCP server to allocate addresses. The default value is 192.168.0.100. Note: The IP address must belong to the same subnet as the associated interface's IP address.
End IP Address end-address	Defines the ending IP address (IPv4 address in dotted-decimal format) of the IP address pool range used by the DHCP server

Parameter	Description
[DhcpServer_EndIPAddress]	to allocate addresses. The default value is 192.168.0.149. Note: The IP address must belong to the same subnet as the associated interface's IP address and must be "greater or equal" to the starting IP address defined in 'Start IP Address'.
Subnet Mask subnet-mask [DhcpServer_SubnetMask]	Defines the subnet mask (for IPv4 addresses) for the DHCP client. The value is sent in DHCP Option 1 (Subnet Mask). The default value is 0.0.0.0. Note: The value must be "narrower" or equal to the subnet mask of the associated interface's IP address. If set to "0.0.0.0", the subnet mask of the associated interface is used.
Lease Time lease-time [DhcpServer_LeaseTime]	Defines the duration (in minutes) of the lease time to a DHCP client for using an assigned IP address. The client needs to request a new address before this time expires. The value is sent in DHCP Option 51 (IP Address Lease Time). The valid value range is 0 to 214,7483,647. The default is 1440. When set to 0, the lease time is infinite.
DNS	
DNS Server 1 dns-server-1 [DhcpServer_DNSServer1]	Defines the IP address (IPv4) of the primary DNS server that the DHCP server assigns to the DHCP client. The value is sent in DHCP Option 6 (Domain Name Server). The default value is 0.0.0.0.
DNS Server 2 dns-server-2 [DhcpServer_DNSServer2]	Defines the IP address (IPv4) of the secondary DNS server that the DHCP server assigns to the DHCP client. The value is sent in DHCP Option 6 (Domain Name Server). The default value is 0.0.0.0.
NetBIOS	
NetBIOS Name Server netbios-server [DhcpServer_NetbiosNameServer]	Defines the IP address (IPv4) of the NetBIOS WINS server that is available to a Microsoft DHCP client. The value is sent in DHCP Option 44 (NetBIOS Name Server). The default value is 0.0.0.0.
NetBIOS Node Type netbios-node-type [DhcpServer_NetbiosNodeType]	Defines the node type of the NetBIOS WINS server for a Microsoft DHCP client. The value is sent in DHCP Option 46 (NetBIOS Node Type). <ul style="list-style-type: none"> ▪ [0] Broadcast (default) ▪ [1] peer-to-peer ▪ [4] Mixed ▪ [8] Hybrid
Time and Date	
NTP Server 1 ntp-server-1 [DhcpServer_NTPServer1]	Defines the IP address (IPv4) of the primary NTP server that the DHCP server assigns to the DHCP client. The value is sent in DHCP Option 42 (Network Time Protocol Server). The default value is 0.0.0.0.
NTP Server 2 ntp-server-2 [DhcpServer_NTPServer2]	Defines the IP address (IPv4) of the secondary NTP server that the DHCP server assigns to the DHCP client. The value is sent in DHCP Option 42 (Network Time Protocol Server).

Parameter	Description
	The default value is 0.0.0.0.
Time Offset time-offset [DhcpServer_TimeOffset]	Defines the Greenwich Mean Time (GMT) offset (in seconds) that the DHCP server assigns to the DHCP client. The value is sent in DHCP Option 2 (Time Offset). The valid range is -43200 to 43200. The default is 0.
Boot File	
TFTP Server Name tftp-server-name [DhcpServer_TftpServer]	Defines the IP address or name of the TFTP server that the DHCP server assigns to the DHCP client. The TFTP server typically stores the boot file image, defined in the 'Boot file name' parameter (see below). The value is sent in DHCP Option 66 (TFTP Server Name). The valid value is a string of up to 80 characters. By default, no value is defined.
Boot File Name boot-file-name [DhcpServer_BootFileName]	Defines the name of the boot file image for the DHCP client. The boot file stores the boot image for the client. The boot image is typically the operating system the client uses to load (downloaded from a boot server). The value is sent in DHCP Option 67 (Bootfile Name). To define the server storing the file, use the 'TFTP Server' parameter (see above). The valid value is a string of up to 256 characters. By default, no value is defined. The name can also include the following case-sensitive placeholder strings that are replaced with actual values if the 'Expand Boot-file Name' parameter is set to Yes : <ul style="list-style-type: none"> ▪ <MAC>: Replaced by the MAC address of the client (e.g., <i>boot_<MAC>.ini</i>). The MAC address is obtained in the client's DHCP request. ▪ <IP>: Replaced by the IP address assigned by the DHCP server to the client.
Expand Boot-File Name expand-boot-file-name [DhcpServer_ExpandBootfileName]	Enables the use of the placeholders in the boot file name, defined in the 'Boot file name' parameter. <ul style="list-style-type: none"> ▪ [0] No ▪ [1] Yes (default)
Router	
Override Router override-router-address [DhcpServer_OverrideRouter]	Defines the IP address (IPv4 in dotted-decimal notation) of the default router that the DHCP server assigns the DHCP client. The value is sent in DHCP Option 3 (Router). The default value is 0.0.0.0. If not specified (empty or "0.0.0.0"), the IP address of the default gateway configured in the IP Interfaces table for the IP network interface that you associated with the DHCP server (see the 'Interface Name' parameter above) is used.
SIP	
SIP Server sip-server [DhcpServer_SipServer]	Defines the IP address or DNS name of the SIP server that the DHCP server assigns the DHCP client. The client uses this SIP server for its outbound SIP requests. The value is sent in DHCP Option 120 (SIP Server). After defining the parameter, use the 'SIP server type' parameter (see below) to define the type of

Parameter	Description
	address (FQDN or IP address). The valid value is a string of up to 256 characters. The default is 0.0.0.0.
SIP Server Type sip-server-type [DhcpServer_SipServerType]	Defines the type of SIP server address. The actual address is defined in the 'SIP server' parameter (see above). Encoding is done per SIP Server Type, as defined in RFC 3361. <ul style="list-style-type: none"> [0] DNS names = (Default) The 'SIP server' parameter is configured with an FQDN of the SIP server. [1] IP address = The 'SIP server' parameter configured with an IP address of the SIP server.

17.1.2 Configuring the Vendor Class Identifier

The DHCP Vendor Class table lets you configure up to 10 Vendor Class Identifier (VCI) names (DHCP Option 60). When the table is configured, the device's DHCP server responds only to DHCPDiscover requests that contain Option 60 and that match one of the DHCP VCIs configured in the table. If you have not configured any entries in the table, the DHCP server responds to all DHCPDiscover requests, regardless of the VCI.

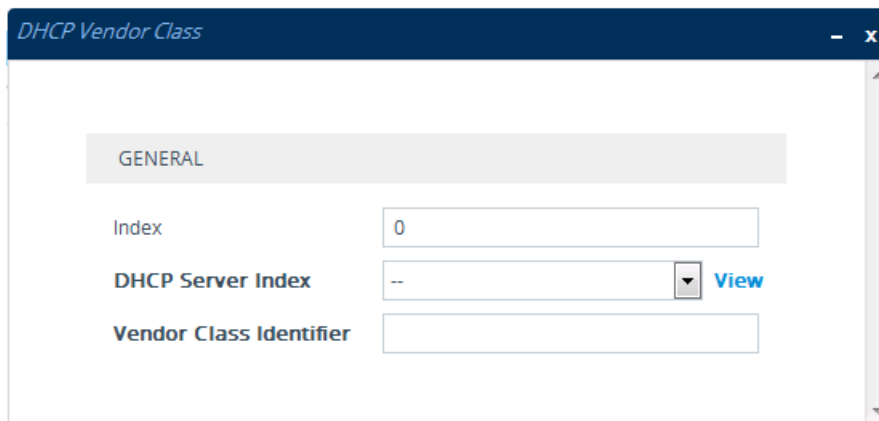
The VCI is a string that identifies the vendor and functionality of a DHCP client to the DHCP server. For example, Option 60 can show the unique type of hardware (e.g., "AudioCodes 440HD IP Phone") or firmware of the DHCP client. The DHCP server can then differentiate between DHCP clients and process their requests accordingly.

The following procedure describes how to configure the DHCP VCIs through the Web interface. You can also configure it through ini file (DhcpVendorClass) or CLI (configure network > dhcp-server vendor-class).

➤ **To configure DHCP Vendor Class Identifiers:**

1. Open the DHCP Servers table (see "Configuring the DHCP Server" on page 201).
2. Select the row of the desired DHCP server for which you want to configure VCIs, and then click the **DHCP Vendor Class** link located below the table; the DHCP Vendor Class table opens.
3. Click **New**; the following dialog box appears:

Figure 17-2: DHCP Vendor Class Table - Add Dialog Box



4. Configure a VCI for the DHCP server according to the parameters described in the table below.
5. Click **Apply**.

Table 17-3: DHCP Vendor Class Table Parameter Descriptions

Parameter	Description
Index dhcp vendor-class <index> [DhcpVendorClass_Index]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
DHCP Server Index dhcp-server-number [DhcpVendorClass_DhcpServerIndex]	Associates the VCI table entry with a DHCP server that you configured in "Configuring the DHCP Server" on page 201. Note: Currently, only one DHCP server (Index 0) can be configured and therefore, the parameter is always set at 0.
Vendor Class Identifier vendor-class [DhcpVendorClass_VendorClassId]	Defines the value of the VCI DHCP Option 60. The valid value is a string of up to 80 characters. By default, no value is defined.

17.1.3 Configuring Additional DHCP Options

The DHCP Option table lets you configure up to 10 additional DHCP Options that the DHCP server can use to service the DHCP client. These DHCP Options are included in the DHCP Offer response sent by the DHCP server.

The following procedure describes how to configure DHCP Options through the Web interface. You can also configure it through ini file (DhcpOption) or CLI (configure network > dhcp-server option).



Note: The additional DHCP Options configured in the DHCP Option table override the default ones, which are configured in the DHCP Servers table. In other words, if you configure Option 67 in the DHCP Option table, the device uses the value configured in the DHCP Option table instead of the value configured in the DHCP Servers table.

➤ **To configure DHCP Options:**

1. Open the DHCP Servers table (see "Configuring the DHCP Server" on page 201).
2. Select the row of the desired DHCP server for which you want to configure additional DHCP Options, and then click the **DHCP Option** link located below the table; the DHCP Option table opens.

- Click **New**; the following dialog box appears:

Figure 17-3: DHCP Option Table - Add Dialog Box

- Configure additional DHCP Options for the DHCP server according to the parameters described in the table below.
- Click **Apply**.

Table 17-4: DHCP Option Table Parameter Descriptions

Parameter	Description
Index dhcp option [DhcpOption_Index]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
DHCP Server Index dhcp-server-number [DhcpOption_DhcpServerIndex]	Associates the DHCP Option table entry with a DHCP server that you configured in "Configuring the DHCP Server" on page 201. Note: Currently, only one DHCP server (Index 0) can be configured and therefore, the parameter is always set at 0.
Option option [DhcpOption_Option]	Defines the code of the DHCP Option. The valid value is 1 to 254. The default is 159. For example, for DHCP Option 150 (Cisco proprietary for defining multiple TFTP server IP addresses), enter the value 150.
Type type [DhcpOption_Type]	Defines the format (type) of the DHCP Option value that is configured in the 'Value' parameter (see below). <ul style="list-style-type: none"> [0] ASCII = (Default) Plain-text string (e.g., when the value is a domain name). [1] IP address = IPv4 address. [2] Hexadecimal = Hexadecimal-encoded string. For example, if you set the 'Value' parameter to "company.com", you need to set the 'Type' parameter to ASCII .
Value value [DhcpOption_Value]	Defines the value of the DHCP Option. For example, if you are using Option 66, the parameter is used for specifying the TFTP provisioning server (e.g., http://192.168.3.155:5000/provisioning/). The valid value is a string of up to 256 characters. By default, no value is defined. For IP addresses, the value can be one or more

Parameter	Description
	<p>IPv4 addresses, each separated by a comma (e.g., 192.168.10.5,192.168.10.20). For hexadecimal values, the value is a hexadecimal string (e.g., c0a80a05).</p> <p>You can also configure the parameter with case-sensitive placeholder strings that are replaced with actual values if the 'Expand Value' parameter (see below) is set to Yes:</p> <ul style="list-style-type: none"> ▪ <MAC>: Replaced by the MAC address of the client. The MAC address is obtained from the client's DHCP request. For example, the parameter can be set to: http://192.168.3.155:5000/provisioning/cfg_<MAC>.txt ▪ <IP>: Replaced by the IP address assigned by the DHCP server to the client. For example, the parameter can be set to: http://192.168.3.155:5000/provisioning/cfg_<IP>.txt
Expand Value expand-value [DhcpOption_ExpandValue]	<p>Enables the use of the special placeholder strings, "<MAC>" and "<IP>" for configuring the 'Value' parameter (see above).</p> <ul style="list-style-type: none"> ▪ [0] No ▪ [1] Yes (default) <p>Note: The parameter is applicable only to values of type ASCII (see the 'Type' parameter above).</p>

17.1.4 Configuring Static IP Addresses for DHCP Clients

The DHCP Static IP table lets you configure up to 100 DHCP clients with static IP addresses. The static IP address is a "reserved" IP address for a specified DHCP client defined by MAC address. In other words, instead of assigning the DHCP client with a different IP address upon each IP address lease renewal request, the DHCP server assigns the client the same IP address. For DHCP clients that are not listed in the table, the DHCP server assigns a random IP address from its address pool, as in normal operation.

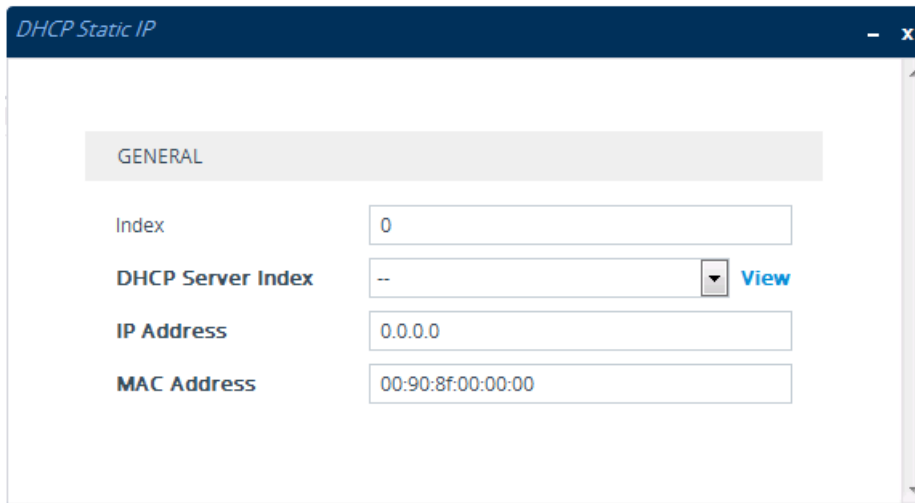
The following procedure describes how to configure static IP addresses for DHCP clients through the Web interface. You can also configure it through ini file (DhcpStaticIP) or CLI (configure network > dhcp-server static-ip <index>).

➤ **To configure static IP addresses for DHCP clients:**

1. Open the DHCP Servers table (see "Configuring the DHCP Server" on page 201).
2. Select the row of the desired DHCP server for which you want to configure static IP addresses for DHCP clients, and then click the **DHCP Static IP** link located below the table; the DHCP Static IP table opens.

- Click **New**; the following dialog box appears:

Figure 17-4: DHCP Static IP Table - Add Dialog Box



- Configure a static IP address for a specific DHCP client according to the parameters described in the table below.
- Click **Apply**.

Table 17-5: DHCP Static IP Table Parameter Descriptions

Parameter	Description
Index dhcp static-ip <index> [DhcpStaticIP_Index]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
DHCP Server Index dhcp-server-number [DhcpStaticIP_DhcpServerIndex]	Associates the DHCP Static IP table entry with a DHCP server that you configured in "Configuring the DHCP Server" on page 201. Note: Currently, only one DHCP server (Index 0) can be configured and therefore, the parameter is always set at 0.
IP Address ip-address [DhcpStaticIP_IPAddress]	Defines the "reserved", static IP address (IPv4) to assign the DHCP client. The default is 0.0.0.0.
MAC Address mac-address [DhcpStaticIP_MACAddress]	Defines the DHCP client by MAC address (in hexadecimal format). The valid value is a string of up to 20 characters. The format includes six groups of two hexadecimal digits, each separated by a colon. The default MAC address is 00:90:8f:00:00:00.

17.1.5 Viewing and Deleting DHCP Clients

The DHCP Clients table lets you view currently serviced DHCP clients by the DHCP server. The table also lets you delete DHCP clients. If you delete a client, the DHCP server ends the lease of the IP address to the client and the IP address becomes available for allocation by the DHCP server to another client.

The following procedure describes how to view DHCP clients through the Web interface. You can also view this through CLI:

- To view DHCP clients:

```
# show network dhcp clients
```

- To view DHCP clients according to IP address:

```
# show network dhcp ip
```

- To view DHCP clients according to MAC address:

```
# show network dhcp mac
```

- To view DHCP clients that have been blacklisted from DHCP implementation (due to duplicated IP addresses in the network, where another device is using the same IP address as the one assigned to the client):

```
# show network dhcp black-list
```

➤ **To view or delete DHCP clients:**

1. Open the DHCP Servers table (see "Configuring the DHCP Server" on page 201).
2. Select the row of the desired DHCP server for which you want to view DHCP clients, and then click the **DHCP Clients** link located below the table; the DHCP Clients table opens:

Figure 17-5: DHCP Clients Table

INDEX ↕	DHCP SERVER INDEX	IP ADDRESS	MAC ADDRESS	LEASE EXPIRATION
---------	-------------------	------------	-------------	------------------

The table displays the following per client:

- **Index:** Table index number.
 - **DHCP Server Index:** The index number of the configured DHCP server scope in the DHCP Server table (see "Configuring the DHCP Server" on page 201) with which the client is associated.
 - **IP Address:** IP address assigned to the DHCP client by the DHCP server.
 - **MAC Address:** MAC address of the DHCP client.
 - **Lease Expiration:** Date on which the lease of the DHCP client's IP address obtained from the DHCP server expires.
3. To delete a client:
 - a. Select the table row index of the DHCP client that you want to delete.
 - b. Click the **Action** button, and then from the drop-down menu, choose **Delete**; a confirmation message appears.
 - c. Click **OK** to confirm deletion.

17.2 SIP-based Media Recording

The device can record SIP-based media call sessions traversing it. The media recording support is in accordance with the Session Recording Protocol (siprec), which describes architectures for deploying session recording solutions and specifies requirements for extensions to SIP that will manage delivery of RTP media to a recording device. The siprec protocol is based on RFC 6341 (Use Cases and Requirements for SIP-Based Media Recording), Session Recording Protocol (draft-ietf-siprec-protocol-02), and Architecture (draft-ietf-siprec-architecture-03).



Warning for Deployments in France: The device supports SIP-based Media Recording (SIPREC) according to RFC 6341. As such, you must adhere to the Commission Nationale Informatique et Liberté's (CNIL) directive (<http://www.cnil.fr/english/data-protection/rights-and-obligations/>) and be aware that article R226-15 applies penalties to the malicious interception, diversion, use or disclosure of correspondence sent, transmitted or received by means of telecommunication, or the setting up of a device designed to produce such interceptions.

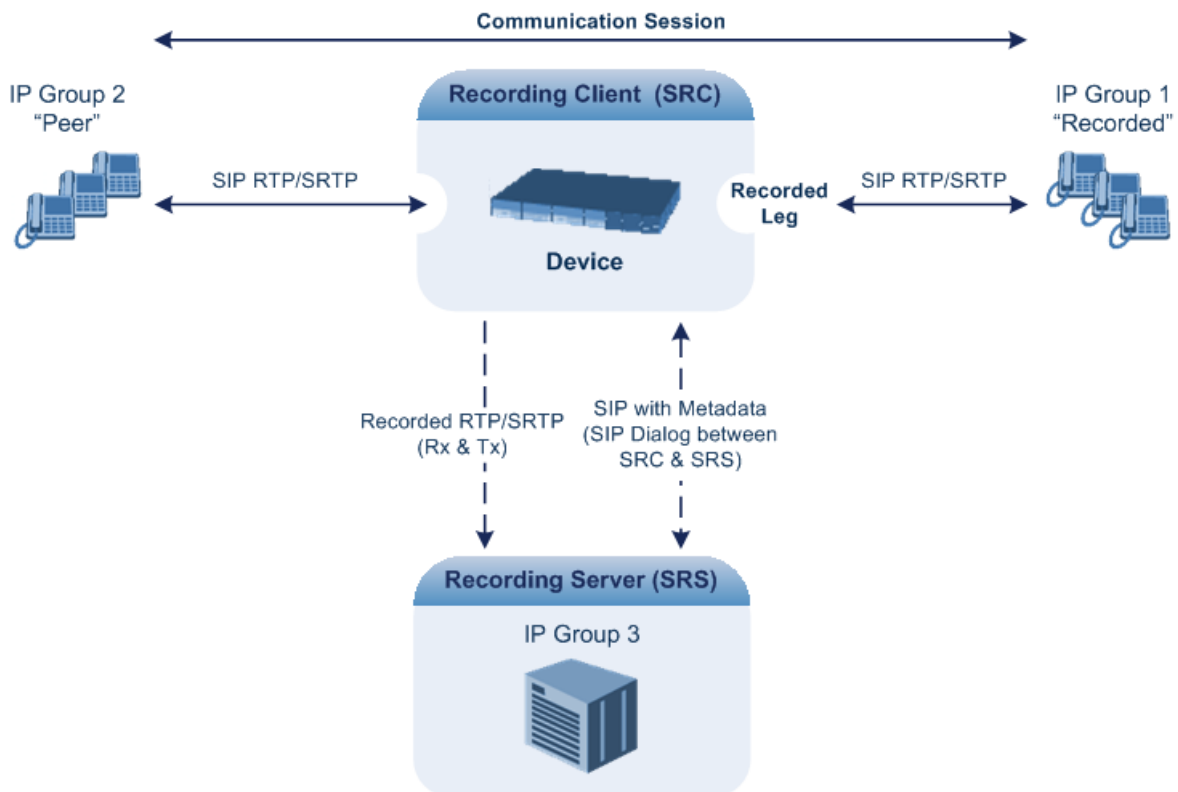


Note:

- The SIP-based Media Recording feature is available only if the device is installed with a License Key that includes this feature. For installing a License Key, see "License Key" on page 597. The License Key also specifies the maximum number of supported SIP recording sessions.
- For the maximum number of concurrent sessions that the device can record, contact your AudioCodes sales representative.

Session recording is a critical requirement in many business communications environments such as call centers and financial trading floors. In some of these environments, all calls must be recorded for regulatory and compliance reasons. In others, calls may be recorded for quality control or business analytics. Recording is typically performed by sending a copy of the session media to the recording devices.

The siprec protocol specifies the use of SIP, SDP, and RTP to establish a Recording Session (RS) from the Session Recording Client (SRC), which is on the path of the Communication Session (CS), to a Session Recording Server (SRS) at the recording equipment. The device functions as the SRC, sending recording sessions to a third-party SRS, as shown in the figure below.



The device can record calls between two IP Groups. The type of calls to record can be specified by source and/or destination prefix number or SIP Request-URI, as well as by call initiator. The side ("leg") on which the recording is done must be specified. Specifying the leg is important as it determines the various call media attributes of the recorded RTP (or SRTP) such as coder type.

The device can also record SRTP calls and send it to the SRS in SRTP. In such scenarios, the SRTP is used on one of the IP legs for SBC calls. For an SBC RTP-SRTP session, the recorded IP Group in the SIP Recording table must be set to the RTP leg if recording is required to be RTP, or set to the SRTP leg if recording is required to be SRTP.

For SBC calls, the device can also be located between an SRS and an SRC and act as an RTP-SRTP translator. In such a setup, the device receives SIP recording sessions (as a server) from the SRC and translates SRTP media to RTP, or vice versa, and then forwards the recording to the SRS in the translated media format.

The device initiates a recording session by sending an INVITE message to the SRS when the recorded call is connected. The SIP From header contains the identity of the SRC and the To header contains the identity of the SRS. The SDP in the INVITE contains:

- Two 'm=' lines that represent the two RTP/SRTP streams (Rx and Tx).
- Two 'a=label:' lines that identify the streams.
- XML body (also referred to as metadata) that provides information on the participants of the call session:
 - <group id>: Logging Session ID (displayed as [SID:nnnnn] in Syslog), converted from decimal to hex. This number remains the same even if the call is forwarded or transferred. This is important for recorded calls.
 - <session id>: Originally recorded Call-ID, converted from decimal to hex.
 - <group-ref>: same as <group id>.
 - <participant id>: SIP From / To user.
 - <nameID aor>: From/To user@host.
 - <send> and <recv>: ID's for the RTP/SRTP streams in hex - bits 0-31 are the same as group, bits 32-47 are the RTP port.
 - <stream id>: Same as <send> for each participant.
 - <label>: 1 and 2 (same as in the SDP's 'a=label:' line).

The SRS can respond with 'a=recvonly' for immediate recording or 'a=inactive' if recording is not yet needed, and send re-INVITE at any later time with the desired RTP/SRTP mode change. If a re-INVITE is received in the original call (e.g. when a call is on hold), the device sends another re-INVITE with two 'm=' lines to the SRS with the updated RTP/SRTP data. If the recorded leg uses SRTP, the device can send the media streams to the SRS as SRTP; otherwise, the media streams are sent as RTP to the SRS.

Below is an example of an INVITE sent by the device to an SRS:

```
INVITE sip:VSRP@1.9.64.253 SIP/2.0
Via: SIP/2.0/UDP 192.168.241.44:5060;branch=z9hG4bKac505782914
Max-Forwards: 10
From: <sip:192.168.241.44>;tag=1c505764207
To: <sip:VSRP@1.9.64.253>
Call-ID: 505763097241201011157@192.168.241.44
CSeq: 1 INVITE
Contact: <sip:192.168.241.44:5060>;src
Supported: replaces,resource-priority
Allow:
REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
Require: siprec
User-Agent: Mediant /v.7.20A.000.038
```

```

Content-Type: multipart/mixed;boundary=boundary_aclfffff85b
Content-Length: 1832

--boundary_aclfffff85b
Content-Type: application/sdp
v=0
o=AudiocodesGW 921244928 921244893 IN IP4 10.33.8.70
s=SBC-Call
c=IN IP4 10.33.8.70
t=0 0
m=audio 6020 RTP/AVP 8 96
c=IN IP4 10.33.8.70
a=ptime:20
a=sendonly
a=label:1
a=rtpmap:8 PCMA/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
m=audio 6030 RTP/AVP 8 96
c=IN IP4 10.33.8.70
a=ptime:20
a=sendonly
a=label:2
a=rtpmap:8 PCMA/8000
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
--boundary_aclfffff85b
Content-Type: application/rs-metadata
Content-Disposition: recording-session
<?xml version="1.0" encoding="UTF-8"?>
<recording xmlns='urn:ietf:params:xml:ns:recording'>
  <datamode>complete</datamode>
  <group id="00000000-0000-0000-0000-00003a36c4e3">
    <associate-time>2010-01-24T01:11:57Z</associate-time>
  </group>
  <session id="0000-0000-0000-0000-00000000d0d71a52">
    <group-ref>00000000-0000-0000-0000-00003a36c4e3</group-ref>
    <start-time>2010-01-24T01:11:57Z</start-time>
    <ac:AvayaUCID
xmlns="urn:ietf:params:xml:ns:Avaya">FA080030C4E34B5B9E59</ac:Avaya
aUCID>
  </session>
  <participant id="1056" session="0000-0000-0000-0000-
00000000d0d71a52">
    <nameID aor="1056@192.168.241.20"></nameID>
    <associate-time>2010-01-24T01:11:57Z</associate-time>
    <send>00000000-0000-0000-0000-1CF23A36C4E3</send>
    <recv>00000000-0000-0000-0000-BF583A36C4E3</recv>
  </participant>
  <participant id="182052092" session="0000-0000-0000-0000-
00000000d0d71a52">
    <nameID aor="182052092@voicelab.local"></nameID>
    <associate-time>2010-01-24T01:11:57Z</associate-time>
    <recv>00000000-0000-0000-0000-1CF23A36C4E3</recv>
    <send>00000000-0000-0000-0000-BF583A36C4E3</send>
  </participant>
  <stream id="00000000-0000-0000-0000-1CF23A36C4E3" session="0000-
0000-0000-0000-00000000d0d71a52">
    <label>1</label>

```

```

</stream>
<stream id="00000000-0000-0000-0000-BF583A36C4E3" session="0000-
0000-0000-00000000d0d71a52">
  <label>2</label>
</stream>
</recording>
--boundary_ac1ffffff85b-

```

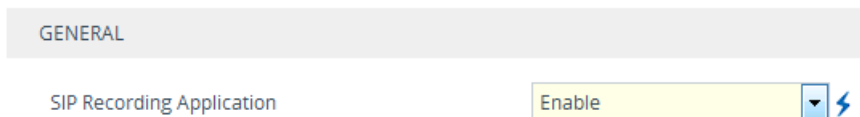
17.2.1 Enabling SIP-based Media Recording

The following procedure describes how to enable the SIP-based media Recording feature.

➤ **To enable SIP-based media recording:**

1. Open the SIP Recording Settings page (**Setup** menu > **Signaling & Media** tab > **SIP Recording** folder > **SIP Recording Settings**).

Figure 17-6: Enabling SIPRec



2. From the 'SIP Recording Application' drop-down list, select **Enable**.
3. Click **Apply**, and then reset the device with a save-to-flash for your settings to take effect.

17.2.2 Configuring SIP Recording Rules

The SIP Recording Rules table lets you configure up to 30 SIP-based media recording rules. A SIP Recording rule defines call routes that you want to record. For an overview of the feature, see "SIP-based Media Recording" on page 211.

The following procedure describes how to configure SIP Recording rules through the Web interface. You can also configure it through ini file (SIPRecRouting) or CLI (configure voip > sip-definition sip-recording sip-rec-routing).

➤ **To configure a SIP Recording Routing rule:**

1. Open the SIP Recording Rules table (**Setup** menu > **Signaling & Media** tab > **SIP Recording** folder > **SIP Recording Rules**).

- Click **New**; the following dialog box appears:

Figure 17-7: SIP Recording Rules Table - Add Dialog Box

The figure above shows a configuration example where the device records calls made by IP Group "ITSP" to IP Group "IP PBX" that have the destination number prefix, "1800". The device records the calls from the leg interfacing with IP Group "IP PBX" and sends the recorded media to IP Group "SRS".

- Configure a SIP recording rule according to the parameters described in the table below.
- Click **Apply**, and then save your settings to flash memory.

Table 17-6: SIP Recording Rules Table Parameter Descriptions

Parameter	Description
Index [SIPRecRouting_Index]	Defines an index number for the new table record.
Recorded IP Group recorded-ip-group-name [SIPRecRouting_RecordedIPGroupName]	Defines the IP Group participating in the call and the recording is done on the leg interfacing with this IP Group. To configure IP Groups, see "Configuring IP Groups" on page 329. By default, all IP Groups are defined (Any). Note: For an SBC RTP-SRTP session, the recorded IP Group must be set to the RTP leg if recording is required to be RTP, or set to the SRTP leg if recording is required to be SRTP.
Recorded Source Prefix recorded-src-prefix [SIPRecRouting_RecordedSourcePrefix]	Defines calls to record based on source number or URI. By default, all source numbers or URIs are defined (*).
Recorded Destination Prefix recorded-dst-prefix [SIPRecRouting_RecordedDestinationPrefix]	Defines calls to record based on destination number or URI. By default, all destination numbers or URIs are defined (*).
Peer IP Group peer-ip-group-name [SIPRecRouting_PeerIPGroupName]	Defines the peer IP Group that is participating in the call. By default, all IP Groups are defined (Any).

Parameter	Description
Caller caller [SIPRecRouting_Caller]	Defines which calls to record according to which party is the caller. <ul style="list-style-type: none"> ▪ [0] Both = (Default) Caller can be peer or recorded side ▪ [1] Recorded Party ▪ [2] Peer Party
Recording Server (SRS) IP Group srs-ip-group-name [SIPRecRouting_SRSIPGroupName]	Defines the IP Group of the recording server (SRS). By default, no value is defined.. Note: The SIP Interface used for communicating with the SRS is according to the SRD assigned to the SRS IP Group (in the IP Groups table).

17.2.3 Configuring SIP User Part for SRS

You can configure the SIP user part of the Request-URI for the recording server (SRS). The device inserts this user part in the SIP To header of the INVITE message sent to the SRS.

➤ **To configure the SIP user part for SRS:**

1. Open the SIP Recording Settings page (**Setup** menu > **Signaling & Media** tab > **SIP Recording** folder > **SIP Recording Settings**).

Figure 17-8: Configuring User Part of To Header for SRS

Recording Server (SRS) Destination Username

2. In the 'Recording Server (SRS) Destination Username' field, enter a user part value (string of up to 50 characters).
3. Click **Apply**.

17.2.4 Interworking SIP-based Media Recording with Third-Party Vendors

The device can interwork the SIP-based Media Recording feature with third-party vendors, as described in the following subsections.

17.2.4.1 Genesys

The device's SIP-based media recording can interwork with Genesys' equipment. Genesys sends its proprietary X-Genesys-CallUUID header (which identifies the session) in the first SIP message, typically in the INVITE and the first 18x response. If the device receives a SIP message with Genesys SIP header, it adds the header's information to AudioCodes' proprietary tag in the XML metadata of the SIP INVITE that it sends to the recording server, as shown below:

```
<ac:GenesysUUID
xmlns="urn:ietf:params:xml:ns:Genesys">4BOKLLA3VH66JF112M1CC9VHKS1
4F0KP</ac:GenesysUUID>
```

No configuration is required for this support.

17.2.4.2 Avaya UCID

The device's SIP-based media recording can interwork with Avaya equipment. The Universal Call Identifier (UCID) is Avaya's proprietary call identifier used to correlate call records between different systems and identifies sessions. Avaya generates this in outgoing calls. If the device receives a SIP INVITE from Avaya, it adds the UCID value, received in the User-to-User SIP header to AudioCodes' proprietary tag in the XML metadata of the SIP INVITE that it sends to the recording server. For example, if the received SIP header is:

```
User-to-User: 00FA080019001038F725B3;encoding=hex
```

the device includes the following in the XML metadata:

```
xml metadata:
<ac:AvayaUCID xmlns="urn:ietf:params:xml:ns:Avaya">
FA080019001038F725B3</ac:AvayaUCID>
```



Note: For calls sent from the device to Avaya equipment, the device can generate the Avaya UCID, if required. To configure this support, use the following parameters:

- 'UUI Format' in the IP Groups table - enables Avaya support.
- 'Network Node ID' - defines the Network Node Identifier of the device for Avaya UCID.

17.3 RADIUS-based Services

The device supports Remote Authentication Dial In User Service (RADIUS) by acting as a RADIUS client. You can use RADIUS for the following:

- Authentication and authorization of management users (login username and password) to gain access to the device's management interface.
- Accounting where the device sends accounting data of SIP calls as call detail records (CDR) to a RADIUS Accounting server (for third-party billing purposes).

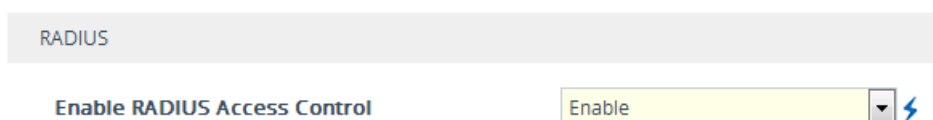
17.3.1 Enabling RADIUS Services

Before you can implement any RADIUS services, you must enable the RADIUS feature, as described in the procedure below.

➤ **To enable RADIUS:**

1. Open the Authentication Server page (**Setup** menu > **Administration** tab > **Web & CLI** folder > **Authentication Server**).

Figure 17-9: Enabling RADIUS



2. Under the RADIUS group, from the 'Enable RADIUS Access Control' drop-down list, select **Enable**.
3. Click **Apply**, and then reset the device with a save-to-flash for your settings to take effect.

17.3.2 Configuring RADIUS Servers

The RADIUS Servers table lets you configure up to three RADIUS servers. You can use RADIUS servers for RADIUS-based management-user login authentication and/or RADIUS-based accounting (sending of SIP CDRs to the RADIUS server).

When multiple RADIUS servers are configured, RADIUS server redundancy can be implemented. When the primary RADIUS server is down, the device sends a RADIUS request twice (one retransmission) and if both fail (i.e., no response), the device considers the server as down and attempts to send requests to the next server. The device continues sending RADIUS requests to the redundant RADIUS server even if the primary server returns to service later on. However, if a device reset occurs or a switchover occurs in a High-Availability (HA) system, the device sends RADIUS requests to the primary RADIUS server. By default, the device waits for up to two seconds (i.e., timeout) for a response from the RADIUS server for RADIUS requests and retransmission before it considers the server as down.

For each RADIUS server, the IP address, port, and shared secret can be configured. Each RADIUS server can be defined for RADIUS-based login authentication and/or RADIUS-based accounting. By setting the relevant port (authentication or accounting) to "0" disables the corresponding functionality. If both ports are configured, the RADIUS server is used for authentication and accounting. All servers configured with non-zero Authorization ports form an Authorization redundancy group and the device sends authorization requests to one of them, depending on their availability. All servers configured with non-zero Accounting ports form an Accounting redundancy group and the device sends accounting CDRs to one of them, depending on their availability. Below are example configurations:

- Only one RADIUS server is configured and used for authorization and accounting purposes (no redundancy). Therefore, both the Authorization and Accounting ports are defined.
- Three RADIUS servers are configured:
 - Two servers are used for authorization purposes only, providing redundancy. Therefore, only the Authorization ports are defined, while the Accounting ports are set to 0.
 - One server is used for accounting purposes only (i.e., no redundancy). Therefore, only the Accounting port is defined, while the Authorization port is set to 0.
- Two RADIUS servers are configured and used for authorization and accounting purposes, providing redundancy. Therefore, both the Authorization and Accounting ports are defined.

The status of the RADIUS servers can be viewed through CLI:

```
# show system radius servers status
```

The example below shows the status of two RADIUS servers in redundancy mode for authorization and accounting:

```
servers 0
 ip-address 10.4.4.203
 auth-port 1812
 auth-ha-state "ACTIVE"
 acc-port 1813
 acc-ha-state "ACTIVE"
servers 1
 ip-address 10.4.4.202
 auth-port 1812
 auth-ha-state "STANDBY"
 acc-port 1813
 acc-ha-state "STANDBY"
```

Where *auth-ha-state* and *acc-ha-state* display the authentication and accounting redundancy status respectively. "ACTIVE" means that the server was used for the last sent authentication or accounting request; "STANDBY" means that the server was not used in the last sent request.

The following procedure describes how to configure a RADIUS server through the Web interface. You can also configure it through ini file (RadiusServers) or CLI configure system (> radius servers).



Note:

- To enable and configure RADIUS-based accounting, see "Configuring RADIUS Accounting" on page 685.
- The device can send up to 201 concurrent RADIUS requests per RADIUS service type (Accounting or Authentication), per RADIUS server (up to three servers per service type), and per local port (up to 4 local ports). For example, 801 (201 * 4) concurrent RADIUS requests can be sent for Authentication and 801 (201 * 4) for Accounting.

➤ **To configure a RADIUS server:**

1. Open the RADIUS Servers table (**Setup** menu > **IP Network** tab > **RADIUS & LDAP** folder > **RADIUS Servers**).
2. Click **New**; the following dialog box appears:

Figure 17-10: RADIUS Servers Table - Add Dialog Box

3. Configure a RADIUS server according to the parameters described in the table below.
4. Click **Apply**.

Table 17-7: RADIUS Servers Table Parameter Descriptions

Parameter	Description
Index [RadiusServers_Index]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
IP Address ip-address [RadiusServers_IPAddress]	Defines the IP address of the RADIUS server (in dotted-decimal notation).
Authentication Port	Defines the port of the RADIUS Authentication server for

Parameter	Description
auth-port [RadiusServers_AuthenticationPort]	authenticating the device with the RADIUS server. When set to any value other than 0, the RADIUS server is used by the device for RADIUS-based management-user login authentication. When set to 0, RADIUS-based login authentication is not implemented. The valid value is 0 to any integer. The default is 1645.
Accounting Port acc-port [RadiusServers_AccountingPort]	Defines the port of the RADIUS Accounting server to where the device sends accounting data of SIP calls as call detail records (CDR). When set to any value other than 0, the RADIUS server is used by the device for RADIUS-based accounting (CDR). When set to 0, RADIUS-based accounting is not implemented. The valid value is 0 to any integer. The default is 1646.
Shared Secret shared-secret [RadiusServers_SharedSecret]	Defines the shared secret (password) for authenticating the device with the RADIUS server. This should be a cryptically strong password. The shared secret is also used by the RADIUS server to verify the authentication of the RADIUS messages sent by the device (i.e., message integrity). The valid value is up to 48 characters. By default, no value is defined.

17.3.3 Configuring Interface for RADIUS Communication

The device can communicate with the RADIUS server through its' OAMP (default) or SIP Control network interface. To change the interface for RADIUS traffic, use the RadiusTrafficType parameter.



Note: If you configure the parameter to Control, make sure that only one Control interface is configured in the IP Interfaces table (see "Configuring IP Network Interfaces" on page 130); otherwise, RADIUS communication fails.

17.3.4 Configuring RADIUS Packet Retransmission

You can configure the device to resend packets to the RADIUS server if no response is received from the server. This functionality is applicable to RADIUS-based user authentication and RADIUS-based accounting.

➤ **To configure RADIUS packet retransmission:**

1. Open the Authentication Server page (**Setup** menu > **Administration** tab > **Web & CLI** folder > **Authentication Server**).

Figure 17-11: Configuring RADIUS Packet Retransmission

RADIUS Response Timeout [sec]	<input type="text" value="2"/>
RADIUS Packets Retransmission	<input type="text" value="1"/>

2. Under the RADIUS group, do the following:

- a. In the 'RADIUS Packets Retransmission' field (RADIUSRetransmission), enter the maximum number of RADIUS retransmissions that the device performs if no response is received from the RADIUS server.
 - b. In the 'RADIUS Response Time Out' field (RadiusTO), enter the interval (in seconds) that the device waits for a response before sending a RADIUS retransmission.
3. Click **Apply**.

17.3.5 Configuring the RADIUS Vendor ID

The vendor-specific attribute (VSA) identifies the device to the RADIUS server using the Vendor ID (as registered with the Internet Assigned Numbers Authority or IANA). The device's default vendor ID is 5003 which can be changed, as described in the following procedure. For an example of using the Vendor ID, see "Setting Up a Third-Party RADIUS Server" on page 223. The procedure is applicable to both RADIUS-based user authentication and RADIUS-based accounting.



Note: The Vendor ID must be the same as the Vendor ID set on the third-party RADIUS server. See the example for setting up a third-party RADIUS server in "Setting Up a Third-Party RADIUS Server" on page 223.

- **To configure the RADIUS Vendor ID:**
1. Open the Authentication Server page (**Setup** menu > **Administration** tab > **Web & CLI** folder > **Authentication Server**).

Figure 17-12: Configuring RADIUS Vendor ID

RADIUS VSA Vendor ID

2. Under the RADIUS group, in the 'RADIUS VSA Vendor ID' field, enter the **same** vendor ID number as set on the third-party RADIUS server.
3. Click **Apply**.

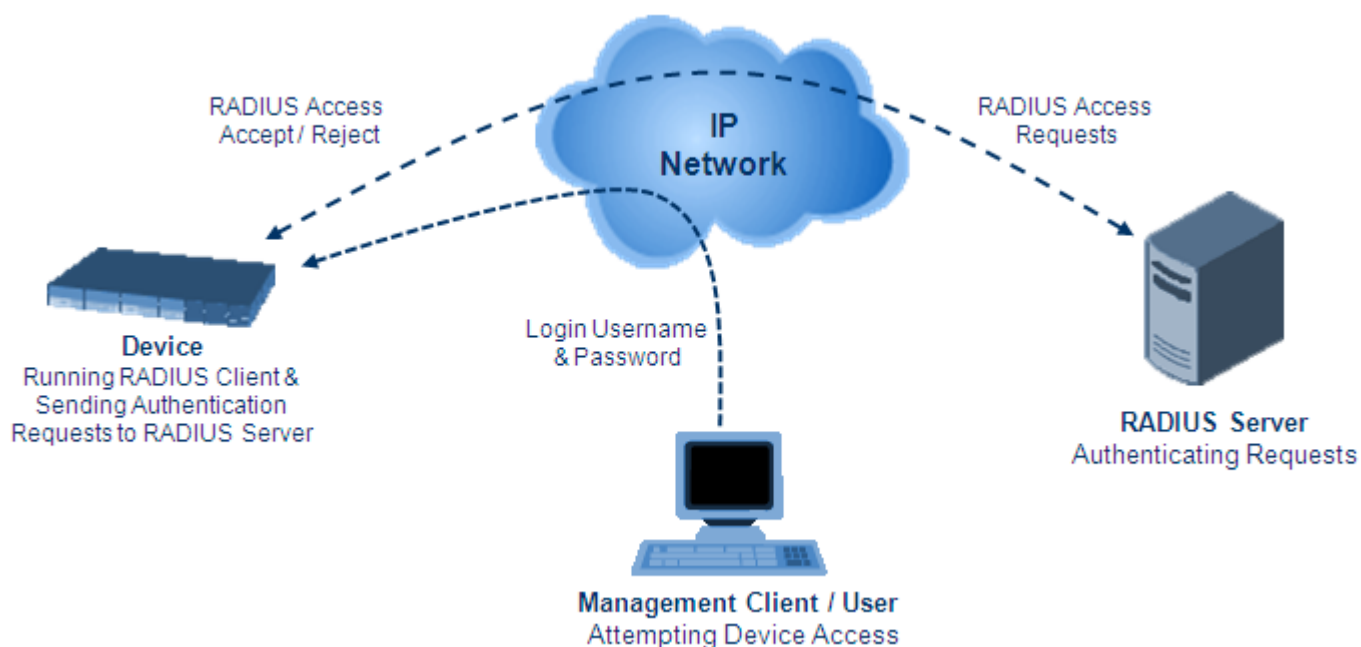
17.3.6 RADIUS-based Management User Authentication

You can enhance security for your device by implementing Remote Authentication Dial-In User Service (RADIUS - RFC 2865) for authenticating multiple management user accounts of the device's embedded Web and Telnet (CLI) servers. Thus, RADIUS also prevents unauthorized access to your device.

When RADIUS authentication is not used, the user's login username and password are locally authenticated by the device using the Local Users table (see "Configuring Management User Accounts" on page 60). However, you can configure the device to use the Local Users table as a fallback mechanism if the RADIUS server does not respond.

When RADIUS authentication is used, the RADIUS server stores the user accounts - usernames, passwords, and access levels (authorization). When a management user (client) tries to access the device, the device sends the RADIUS server the user's username and password for authentication. The RADIUS server replies with an acceptance or a rejection notification. During the RADIUS authentication process, the device's Web interface is blocked until an acceptance response is received from the RADIUS server. Communication between the device and the RADIUS server is done using a shared secret, which is not transmitted over the network.

Figure 17-13: RADIUS Login Authentication for Management



For using RADIUS, you need to do the following:

- Set up a RADIUS server (third-party) to communicate with the device - see "Setting Up a Third-Party RADIUS Server" on page 223
- Configure the device as a RADIUS client for communication with the RADIUS server - see "Configuring RADIUS Authentication" on page 224

17.3.6.1 Setting Up a Third-Party RADIUS Server

The following procedure provides an example for setting up a third-party RADIUS sever, *FreeRADIUS* which can be downloaded from www.freeradius.org. Follow the instructions on this Web site for installing and configuring the server. If you use a RADIUS server from a different vendor, refer to its appropriate documentation.

➤ To set up a third-party RADIUS server (e.g., *FreeRADIUS*):

1. Define the device as an authorized client of the RADIUS server, with the following:
 - Predefined *shared secret* (password used to secure communication between the device and the RADIUS server)
 - Vendor ID (configured on the device in "Configuring the RADIUS Vendor ID" on page 222)

Below is an example of the *clients.conf* file (FreeRADIUS client configuration):

```
#
# clients.conf - client configuration directives
```

```
#
client 10.31.4.47 {
    secret          = FutureRADIUS
    shortname       = audc_device
}
```

2. If access levels are required, set up a Vendor-Specific Attributes (VSA) dictionary for the RADIUS server and select an attribute ID that represents each user's access level. The example below shows a dictionary file for FreeRADIUS that defines the attribute "ACL-Auth-Level" with "ID=35". For the device's user access levels and their corresponding numeric representation in RADIUS servers, see "Configuring Management User Accounts" on page 60.

```
#
# AudioCodes VSA dictionary
#
VENDOR AudioCodes 5003
ATTRIBUTE ACL-Auth-Level 35 integer AudioCodes
VALUE ACL-Auth-Level ACL-Auth-UserLevel 50
VALUE ACL-Auth-Level ACL-Auth-AdminLevel 100
VALUE ACL-Auth-Level ACL-Auth-SecurityAdminLevel 200
```

3. Define the list of users authorized to use the device, using one of the password authentication methods supported by the server implementation. The example below shows a user configuration file for FreeRADIUS using a plain-text password:

```
# users - local user configuration database

john  Auth-Type := Local, User-Password == "qwerty"
      Service-Type = Login-User,
      ACL-Auth-Level = ACL-Auth-SecurityAdminLevel

sue   Auth-Type := Local, User-Password == "123456"
      Service-Type = Login-User,
      ACL-Auth-Level = ACL-Auth-UserLevel
```

4. Record and retain the IP address, port number, shared secret code, vendor ID, and VSA access level identifier (if access levels are implemented) used by the RADIUS server.

17.3.6.2 Configuring RADIUS-based User Authentication

The following procedure describes how to configure RADIUS-based login authentication. For a detailed description of the RADIUS parameters, see "RADIUS Parameters" on page 835.

➤ **To configure RADIUS-based login authentication:**

1. Open the Authentication Server page (**Setup** menu > **Administration** tab > **Web & CLI** folder > **Authentication Server**).
2. From the 'Use RADIUS for Web/Telnet Login' drop-down list, select **Enable** to enable RADIUS authentication for Web and Telnet login:

Figure 17-14: Enabling RADIUS-based Login Authentication

Use RADIUS for Web/Telnet Login

3. When implementing Web user access levels, do one of the following:

- **If the RADIUS server response includes the access level attribute:** In the 'RADIUS VSA Access Level Attribute' field, enter the code that indicates the access level attribute in the VSA section of the received RADIUS packet. For defining the RADIUS server with access levels, see "Setting Up a Third-Party RADIUS Server" on page 223.

Figure 17-15: Authentication Settings Page - RADIUS Configuration

RADIUS VSA Access Level Attribute

- **If the RADIUS server response does not include the access level attribute:** In the 'Default Access Level' field, enter the default access level that is applied to all users authenticated by the RADIUS server.

Figure 17-16: Configuring Default Access Level

Default Access Level

4. Configure RADIUS timeout handling:
 - a. From the 'Behavior upon Authentication Server Timeout' drop-down list, select the option if the RADIUS server does not respond within five seconds:
 - ◆ **Deny Access:** device denies user login access.
 - ◆ **Verify Access Locally:** device checks the username and password configured locally for the user in the Local Users table (see "Configuring Management User Accounts" on page 60), and if correct, allows access.
 - b. In the 'Password Local Cache Timeout' field, enter a time limit (in seconds) after which the username and password verified by the RADIUS server becomes invalid and a username and password needs to be re-validated with the RADIUS server.
 - c. From the 'Password Local Cache Mode' drop-down list, select the option for the local RADIUS password cache timer:
 - ◆ **Reset Timer Upon Access:** upon each access to a Web page, the timer resets (reverts to the initial value configured in the previous step).
 - ◆ **Absolute Expiry Timer:** when you access a Web page, the timer doesn't reset, but continues its count down.

Figure 17-17: Configuring RADIUS Timeout

Behavior upon Authentication Server Timeout ⚡

Password Local Cache Mode

Password Local Cache Timeout (sec)

5. Configure when the Local Users table must be used to authenticate login users. From the 'Use Local Users Database' drop-down list, select one of the following:
 - **When No Auth Server Defined (default):** When no RADIUS server is configured or if a server is configured but connectivity with the server is down (if the server is up, the device authenticates the user with the server).
 - **Always:** First attempts to authenticate the user using the Local Users table, but if not found, it authenticates the user with the RADIUS server.

Figure 17-18: Local Users Table for Login Authentication

Use Local Users Database ⚡

6. Click **Apply**, and then reset the device with a save-to-flash for your settings to take effect.

17.3.6.3 Securing RADIUS Communication

RADIUS authentication requires HTTP basic authentication (according to RFC 2617). However, this is insecure as the usernames and passwords are transmitted in clear text over plain HTTP. Thus, as digest authentication is not supported with RADIUS, it is recommended that you use HTTPS with RADIUS so that the usernames and passwords are encrypted. To enable the device to use HTTPS, configure the 'Secured Web Connection (HTTPS)' parameter to **HTTPS Only** (see "Configuring Secured (HTTPS) Web" on page 68).

17.3.6.4 RADIUS-based User Authentication in URL

RADIUS authentication of the management user is typically done after the user accesses the Web interface by entering only the device's IP address in the Web browser's URL field (for example, `http://10.13.4.12/`) and then entering the username and password credentials in the Web interface's login screen. However, authentication with the RADIUS server can also be done immediately after the user enters the URL, if the URL also contains the login credentials. For example:
`http://10.4.4.112/Forms/RadiusAuthentication?WSBackUserName=John&WSBackPassword=1234`



Note: This feature allows up to five simultaneous users only.

17.3.7 RADIUS-based CDR Accounting

Once you have configured a RADIUS server(s) for accounting in "Configuring RADIUS Servers" on page 219, you need to enable and configure RADIUS-based CDR accounting (see "Configuring RADIUS Accounting" on page 685).

17.4 LDAP-based Management and SIP Services

The device supports the Lightweight Directory Access Protocol (LDAP) application protocol and can operate with third-party, LDAP-compliant servers such as Microsoft Active Directory (AD).

You can use LDAP for the following LDAP services:

- **SIP-related (Control) LDAP Queries:** LDAP can be used for routing and manipulation (e.g., calling name and destination address).

The device connects and binds to the remote LDAP server (IP address or DNS/FQDN) during the service's initialization (at device start-up) or whenever you change the LDAP server's IP address and port. Binding to the LDAP server is based on username and password (Bind DN and Password). 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 the LDAP server's IP address or port is changed. If connection to the LDAP server later fails, the service attempts to reconnect.

For the device to run a search, the path to the directory's subtree, known as the distinguished name (DN), where the search is to be done must be configured (see "Configuring LDAP DN's (Base Paths) per LDAP Server" on page 234). The search key (filter), which defines the exact DN to search and one or more attributes whose values must be returned to the device must also be configured. For more information

on configuring these attributes and search filters, see "AD-based Routing for Microsoft Skype for Business" on page 248.

The device can store recent LDAP queries and responses in its local cache. The cache is used for subsequent queries and/or in case of LDAP server failure. For more information, see "Configuring the Device's LDAP Cache" on page 238.

If connection with the LDAP server disconnects (broken), the device sends the SNMP alarm, `acLDAPLostConnection`. Upon successful reconnection, the alarm clears. If connection with 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.

- **Management-related LDAP Queries:** LDAP can be used for authenticating and authorizing management users (Web and CLI) and is based on the user's login username and password (credentials) when attempting login to one of the device's management platforms. When configuring the login username (LDAP Bind DN) and password (LDAP Password) to send to the LDAP server, you can use templates based on the dollar (\$) sign, which the device replaces with the actual username and password entered by the user during the login attempt. You can also configure the device to send the username and password in clear-text format or encrypted using TLS (SSL).

The device connects to the LDAP server (i.e., an LDAP session is created) only when a login attempt occurs. The LDAP Bind operation establishes the authentication of the user based on the username-password combination. The server typically checks the password against the `userPassword` attribute in the named entry. A successful Bind operation indicates that the username-password combination is correct; a failed Bind operation indicates that the username-password combination is incorrect.

Once the user is successfully authenticated, the established LDAP session may be used for further LDAP queries to determine the user's management access level and privileges (Operator, Admin, or Security Admin). This is known as the user authorization stage. To determine the access level, the device searches the LDAP directory for groups of which the user is a member, for example:

```
CN=# Support Dept,OU=R&D
Groups,OU=Groups,OU=APC,OU=Japan,OU=ABC,DC=corp,DC=abc,DC=com
CN=#AllCellular,OU=Groups,OU=APC,OU=Japan,OU=ABC,DC=corp,DC=abc,DC=com
```

The device then assigns the user the access level configured for that group (in "Configuring Access Level per Management Groups Attributes" on page 236). The location in the directory where you want to search for the user's member group(s) is configured using the following:

- Search base object (distinguished name or DN, e.g., "ou=ABC,dc=corp,dc=abc,dc=com"), which defines the location in the directory from where the LDAP search begins and is configured in "Configuring LDAP DNS (Base Paths) per LDAP Server" on page 234.
- Search filter, for example, `(&(objectClass=person)(sAMAccountName=JohnD))`, which filters the search in the subtree to include only the specific username. The search filter can be configured with the dollar (\$) sign to represent the username, for example, `(sAMAccountName=)`. To configure the search filter, see "Configuring the LDAP Search Filter Attribute" on page 235.
- Management attribute (e.g., `memberOf`), from where objects that match the search filter criteria are returned. This shows the user's member groups. The attribute is configured in the LDAP Servers table (see "Configuring LDAP Servers" on page 231).

If the device finds a group, it assigns the user the corresponding access level and permits login; otherwise, login is denied. Once the LDAP response has been received (success or failure), the device ends the LDAP session.

For both of the previously discussed LDAP services, the following additional LDAP functionality is supported:

- Search method for searching DN object records between LDAP servers and within each LDAP server (see Configuring LDAP Search Methods).
- Default access level that is assigned to the user if the queried response does not contain an access level.
- Local Users table for authenticating users instead of the LDAP server (for example, when a communication problem occurs with the server). For more information, see "Configuring Local Database for Management User Authentication" on page 242.

17.4.1 Enabling the LDAP Service

Before you can configure LDAP support, you need to enable the LDAP service.

➤ To enable LDAP:

1. Open the LDAP Settings page (**Setup** menu > **IP Network** tab > **RADIUS & LDAP** folder > **LDAP Settings**).

Figure 17-19: Enabling LDAP



LDAP Service Enable ⚡

2. From the 'LDAP Service' drop-down list, select **Enable**.
3. Click **Apply**, and then reset the device with a save-to-flash for your settings to take effect.

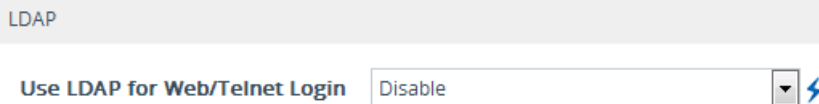
17.4.2 Enabling LDAP-based Web/CLI User Login Authentication and Authorization

The LDAP service can be used for authenticating and authorizing device management users (Web and CLI), based on the user's login username and password (credentials). At the same, it can also be used to determine users' management access levels (privileges). Before you can configure LDAP-based login authentication, you must enable this type of LDAP service, as described in the following procedure.

➤ To enable LDAP-based login authentication:

1. Open the Authentication Server page (**Setup** menu > **Administration** tab > **Web & CLI** folder > **Authentication Server**).

Figure 17-20: Enabling LDAP-based Login Authentication



LDAP

Use LDAP for Web/Telnet Login Disable ⚡

2. Under the LDAP group, from the 'Use LDAP for Web/Telnet Login' drop-down list, select **Enable**.
3. Click **Apply**, and then reset the device with a save-to-flash for your settings to take effect.

17.4.3 Configuring LDAP Server Groups

The LDAP Server Groups table lets you configure up to 600 LDAP Server Groups. An LDAP Server Group is a logical configuration entity that contains up to two LDAP servers.

LDAP servers are assigned to LDAP Server Groups in the LDAP Servers table (see "Configuring LDAP Servers" on page 231). To use a configured LDAP server, you must assign it to an LDAP Server Group.

To use an LDAP server for call routing, you must configure its' LDAP Server Group as "Control" type, and then assign the LDAP Server Group to a Routing Policy. The Routing Policy in turn, needs to be assigned to the relevant routing rule(s). A Routing Policy can be assigned only one LDAP Server Group. Therefore, for multi-tenant deployments where multiple Routing Policies are employed, each tenant can be assigned a specific LDAP Server Group through its unique Routing Policy.

To use an LDAP server for management user login authentication and authorization, you must configure its' LDAP Server Group as "Management" type. Additional LDAP-based management parameters need to be configured, as described in "Enabling LDAP-based Web/CLI User Login Authentication and Authorization" on page 228 and "Configuring LDAP Servers" on page 231.

The following procedure describes how to configure an LDAP Server Group through the Web interface. You can also configure it through ini file (LDAPServerGroups) or CLI (configure system > ldap ldap-server-groups).



Note: The device provides a preconfigured LDAP Server Group ("DefaultCTRLServersGroupin") in the LDAP Server Groups table, which can be modified or deleted.

➤ **To configure an LDAP Server Group:**

1. Open the LDAP Server Groups table (**Setup** menu > **IP Network** tab > **RADIUS & LDAP** folder > **LDAP Server Groups**).
2. Click **New**; the following dialog box appears:

Figure 17-21: LDAP Server Groups Table - Add Dialog Box

GENERAL		CACHE	
Index	0	Cache Entry Timeout [min]	1200
Name		Cache Entry Removal Timeout [hrs]	0
Type	Control		
Server Search Method	Parallel		
DN Search Method	Sequential		

3. Configure an LDAP Server Group according to the parameters described in the table below.
4. Click **Apply**.

Table 17-8: LDAP Server Groups Table Parameter Descriptions

Parameter	Description
General	
Index [LdapServerGroups_Index]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
Name name [LdapServerGroups_Name]	Defines an arbitrary name to easily identify the row. The valid value is a string of up to 20 characters. Note: Each row must be configured with a unique name.
Type server-type [LdapServerGroups_ServerType]	Defines whether the servers in the group are used for SIP-related LDAP queries (Control) or management login authentication-related LDAP queries (Management). <ul style="list-style-type: none"> ▪ [0] Control (Default) ▪ [1] Management Note: Only one LDAP Server Group can be defined for management.
Server Search Method server-search-method [LdapServerGroups_SearchMethod]	Defines the method for querying between the two LDAP servers in the group. <ul style="list-style-type: none"> ▪ [0] Parallel = (Default) The device queries the LDAP servers at the same time. ▪ [1] Sequential = The device first queries one of the LDAP servers and if the DN object is not found or the search fails, it queries the second LDAP server.
DN Search Method search-dn-method [LdapServerGroups_SearchDnsMethod]	Defines the method for querying the Distinguished Name (DN) objects within each LDAP server. <ul style="list-style-type: none"> ▪ [0] Sequential = (Default) The query is done in each DN object, one by one, until a result is returned. For example, a search for the DN object record "JohnD" is first run in DN object "Marketing" and if a result is not found, it searches in "Sales", and if not found, it searches in "Administration", and so on. ▪ [1] Parallel = The query is done in all DN objects at the same time. For example, a search for the DN object record "JohnD" is done at the same time in the "Marketing", "Sales" and "Administration" DN objects.
Cache	
Cache Entry Timeout cache-entry-timeout [LdapServersGroups_CacheEntryTimeout]	Defines the duration (in minutes) that an entry in the device's LDAP cache is valid. If the timeout expires, the cached entry is used only if there is no connectivity with the LDAP server. The valid range is 0 to 35791. The default is 1200. If set to 0, the LDAP entry is always valid.
Cache Entry Removal Timeout cache-entry-removal-timeout [LdapServerGroups_CacheEntryRemovalTimeout]	Defines the duration (in hours) after which the LDAP entry is deleted from the device's LDAP cache. The valid range is 0 to 596. The default is 0 (i.e., the entry is never deleted).

17.4.4 Configuring LDAP Servers

The LDAP Servers table lets you configure up to four LDAP servers. The table defines the address and connectivity settings of the LDAP server. The LDAP server can be configured for SIP-related queries (e.g., routing and manipulation) or LDAP-based management user login authentication and authorization (username-password).

The following procedure describes how to configure an LDAP server through the Web interface. You can also configure it through ini file (LdapConfiguration) or CLI (configure system > ldap ldap-configuration).



Note: When you configure an LDAP server, you need to assign it an LDAP Server Group. Therefore, before you can configure an LDAP server in the table, you must first configure at least one LDAP Server Group in the LDAP Server Groups table (see "Configuring LDAP Server Groups" on page 228).

➤ **To configure an LDAP server:**

1. Open the LDAP Servers table (**Setup** menu > **IP Network** tab > **RADIUS & LDAP** folder > **LDAP Servers**).
2. Click **New**; the following dialog box appears:

Figure 17-22: LDAP Servers Table - Add Dialog Box

3. Configure an LDAP server according to the parameters described in the table below.
4. Click **Apply**.

Table 17-9: LDAP Servers Table Parameter Descriptions

Parameter	Description
General	
Index	Defines an index number for the new table row.

Parameter	Description
[LdapConfiguration_Index]	Note: Each row must be configured with a unique index.
LDAP Servers Group server-group [LdapConfiguration_Group]	Assigns the LDAP server to an LDAP Server Group, configured in the LDAP Server Groups table (see "Configuring LDAP Server Groups" on page 228). Note: <ul style="list-style-type: none"> The parameter is mandatory and must be set before configuring the other parameters in the table. Up to two LDAP servers can be assigned to the same LDAP Server Group.
LDAP Network Interface interface-type [LdapConfiguration_Interface]	Assigns one of the device's IP network interfaces through which communication with the LDAP server is done. By default, no value is defined and the device uses the OAMP network interface, configured in the IP Interfaces table. To configure IP network interfaces, see "Configuring IP Network Interfaces" on page 130. Note: The parameter is mandatory.
Use TLS use-tls [LdapConfiguration_useTLS]	Enables the device to encrypt the username and password (for Control and Management related queries) using TLS when sending them to the LDAP server. <ul style="list-style-type: none"> [0] No = (Default) Username and password are sent in clear-text format. [1] Yes
TLS Context tls-context [LdapConfiguration_ContextName]	Assigns a TLS Context for the connection with the LDAP server. By default, no value is defined and the device uses the default TLS Context (ID 0). To configure TLS Contexts, see "Configuring TLS Certificate Contexts" on page 99. Note: The parameter is applicable only if the 'Use TLS' parameter is configured to Yes .
Connection	
LDAP Server IP server-ip [LdapConfiguration_LdapConfServerIp]	Defines the IP address of the LDAP server (in dotted-decimal notation, e.g., 192.10.1.255). By default, no IP address is defined. Note: <ul style="list-style-type: none"> The parameter is mandatory. If you want to use an FQDN for the LDAP server, leave the parameter undefined and configure the FQDN in the 'LDAP Server Domain Name' parameter (see below).
LDAP Server Port server-port [LdapConfiguration_LdapConfServerPort]	Defines the port number of the LDAP server. The valid value range is 0 to 65535. The default port number is 389.
LDAP Server Max Respond Time max-respond-time [LdapConfiguration_LdapConfServerMaxRespondTime]	Defines the duration (in msec) that the device waits for LDAP server responses. The valid value range is 0 to 86400. The default is 3000. Note: If the response time expires, you can configure the device to use the Local Users table for authenticating the user. For more

Parameter	Description
	information, see "Configuring Local Database for Management User Authentication" on page 242.
LDAP Server Domain Name domain-name [LdapConfiguration_LdapConfServerDomainName]	<p>Defines the domain name (FQDN) of the LDAP server. The device tries to connect to the LDAP server according to the IP address listed in the received 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>Note: If the 'LDAP Server IP' parameter is configured, the 'LDAP Server Domain Name' parameter is ignored. Thus, if you want to use an FQDN, leave the 'LDAP Server IP' parameter undefined.</p>
Verify Certificate verify-certificate [LdapConfiguration_VerifyCertificate]	<p>Enables certificate verification when the connection with the LDAP server uses TLS.</p> <ul style="list-style-type: none"> ▪ [0] No = (Default) No certificate verification is done. ▪ [1] Yes = The device verifies the authentication of the certificate received from the LDAP server. The device authenticates the certificate against the trusted root certificate store associated with the associated TLS Context (see 'TLS Context' parameter above) and if ok, allows communication with the LDAP server. If authentication fails, the device denies communication (i.e., handshake fails). The device can also authenticate the certificate by querying with an Online Certificate Status Protocol (OCSP) server whether the certificate has been revoked. This is also configured for the associated TLS Context. <p>Note: The parameter is applicable only if the 'Use TLS' parameter is configured to Yes.</p>
Connection Status connection-status [LdapConfiguration_ConnectionStatus]	<p>(Read-only) Displays the connection status with the LDAP server.</p> <ul style="list-style-type: none"> ▪ "Not Applicable" ▪ "LDAP Connection Broken" ▪ "Connecting" ▪ "Connected" <p>Note: For more information about a disconnected LDAP connection, see your Syslog messages generated by the device.</p>
Query	
LDAP Password password [LdapConfiguration_LdapConfPassword]	<p>Defines the user password for accessing the LDAP server during connection and binding operations.</p> <ul style="list-style-type: none"> ▪ LDAP-based SIP queries: The parameter is the password used by the device to authenticate itself, as a client, to obtain LDAP service from the LDAP server. ▪ LDAP-based user login authentication: The parameter represents the login password entered by the user during a login attempt. You can use the \$ (dollar) sign in this value to enable the device to automatically replace the \$ sign with the user's login password in the search filter, which it sends to the LDAP server for authenticating the user's username-password combination. For example, \$. <p>Note:</p>

Parameter	Description
LDAP Bind DN bind-dn [LdapConfiguration_LdapConfBindDn]	<ul style="list-style-type: none"> ▪ The parameter is mandatory. ▪ By default, the device sends the password in clear-text format. You can enable the device to encrypt the password using TLS (see the 'Use SSL' parameter below). <p>Defines the LDAP server's bind Distinguished Name (DN) or username.</p> <ul style="list-style-type: none"> ▪ LDAP-based SIP queries: The DN is used as the username during connection and binding to the LDAP server. The DN is used to uniquely name an AD object. Below are example parameter settings: <ul style="list-style-type: none"> ✓ cn=administrator,cn=Users,dc=domain,dc=com ✓ administrator@domain.com ✓ domain\administrator ▪ LDAP-based user login authentication: The parameter represents the login username entered by the user during a login attempt. You can use the \$ (dollar) sign in this value to enable the device to automatically replace the \$ sign with the user's login username in the search filter, which it sends to the LDAP server for authenticating the user's username-password combination. An example configuration for the parameter is \$@sales.local, where the device replaces the \$ with the entered username, for example, JohnD@sales.local. The username can also be configured with the domain name of the LDAP server. <p>Note: By default, the device sends the username in clear-text format. You can enable the device to encrypt the username using TLS (see the 'Use SSL' parameter below).</p>
Management Attribute mgmt-attr [LdapConfiguration_MngmAuthAttr]	<p>Defines the LDAP attribute name to query, which contains a list of groups to which the user is a member. For Active Directory, this attribute is typically "memberOf". The attribute's values (groups) are used to determine the user's management access level; the group's corresponding access level is configured in "Configuring Access Level per Management Groups Attributes" on page 236.</p> <p>Note:</p> <ul style="list-style-type: none"> ▪ The parameter is applicable only to LDAP-based login authentication and authorization (i.e., the 'Type' parameter is set to Management). ▪ If this functionality is not used, the device assigns the user the configured default access level. For more information, see "Configuring Access Level per Management Groups Attributes" on page 236.

17.4.5 Configuring LDAP DN's (Base Paths) per LDAP Server

The LDAP Search DN table lets you configure LDAP base paths. The table is a "child" of the LDAP Servers table (see "Configuring LDAP Servers" on page 231) and configuration is done per LDAP server. For the device to run a search using the LDAP service, the base path to the directory's subtree, referred to as the distinguished name object (or DN), where the search is to be done must be configured. For each LDAP server, you can configure up to three base paths.

The following procedure describes how to configure DN's per LDAP server through the Web interface. You can also configure it through ini file (LdapServersSearchDNs) or CLI (configure system > ldap ldap-servers-search-dns).

➤ **To configure an LDAP base path per LDAP server:**

1. Open the LDAP Servers table (**Setup** menu > **IP Network** tab > **RADIUS & LDAP** folder > **LDAP Servers**).
2. In the table, select the row of the LDAP server for which you want to configure DN base paths, and then click the **LDAP Servers Search Based DN's** link located below the table; the LDAP Server Search Base DN table opens.
3. Click **New**; the following dialog box appears:

Figure 17-23: LDAP Search Base DN Table - Add Dialog Box

The screenshot shows a dialog box titled "LDAP Server Search Base DN". It has a "GENERAL" tab selected. There are two input fields: "Index" with the value "1" and "Base DN" which is empty.

4. Configure an LDAP DN base path according to the parameters described in the table below.
5. Click **Apply**, and then save your settings to flash memory.

Table 17-10: LDAP Server Search Base DN Table Parameter Descriptions

Parameter	Description
Index set internal-index [LdapServersSearchDNs_Index]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
Base DN set base-path [LdapServersSearchDNs_Base_Path]	Defines the full path (DN) to the objects in the AD where the query is done. The valid value is a string of up to 256 characters. For example: OU=NY,DC=OCSR2,DC=local. In this example, the DN path is defined by the LDAP names, OU (organizational unit) and DC (domain component).

17.4.6 Configuring the LDAP Search Filter Attribute

When the LDAP-based login username-password authentication succeeds, the device searches the LDAP server for all groups of which the user is a member. The LDAP query is based on the following LDAP data structure:

- **Search base object (distinguished name or DN, e.g., "ou=ABC,dc=corp,dc=abc,dc=com"):** The DN defines the location in the directory from which the LDAP search begins and is configured in "Configuring LDAP DN's (Base Paths) per LDAP Server" on page 234.
- **Filter (e.g., "(&(objectClass=person)(sAMAccountName=johnd))"):** This filters the

search in the subtree to include only the login username (and excludes others). This is configured by the 'LDAP Authentication Filter' parameter, as described in the following procedure. You can use the dollar (\$) sign to represent the username. For example, the filter can be configured as "(sAMAccountName=*)", where if the user attempts to log in with the username "SueM", the LDAP search is done only for the attribute sAMAccountName that equals "SueM".

- **Attribute (e.g., "memberOf") to return from objects that match the filter criteria:**
The attribute is configured by the 'Management Attribute' parameter in the LDAP Servers table (see "Configuring LDAP Servers" on page 231).

Therefore, the LDAP response includes only the groups of which the specific user is a member.



Note:

- The search filter is applicable only to LDAP-based login authentication and authorization queries.
- The search filter is a global setting that applies to all LDAP-based login authentication and authorization queries, across all configured LDAP servers.

➤ **To configure the LDAP search filter for management users:**

1. Open the Authentication Server page (**Setup** menu > **Administration** tab > **Web & CLI** folder > **Authentication Server**).

Figure 17-24: Configuring LDAP Search Filter

LDAP Authentication Filter

2. In the 'LDAP Authentication Filter' parameter, enter the LDAP search filter attribute for searching the login username for user authentication.
3. Click **Apply**.

17.4.7 Configuring Access Level per Management Groups Attributes

The Management LDAP Groups table lets you configure LDAP group objects and their corresponding management user access level. The table is a "child" of the LDAP Servers table (see "Configuring LDAP Servers" on page 231) and configuration is done per LDAP server. For each LDAP server, you can configure up to three table row entries of LDAP group(s) and their corresponding access level.

**Note:**

- The Management LDAP Groups table is applicable only to LDAP-based login authentication and authorization queries.
- If the LDAP response received by the device includes multiple groups of which the user is a member and you have configured different access levels for some of these groups, the device assigns the user the highest access level. For example, if the user is a member of two groups where one has access level "Monitor" and the other "Administrator", the device assigns the user the "Administrator" access level.
- When the access level is unknown, the device assigns the default access level to the user, configured by the 'Default Access Level' parameter as used also for RADIUS (see "Configuring RADIUS-based User Authentication" on page 224). This can occur in the following scenarios:
 - ✓ The user is not a member of any group.
 - ✓ The group of which the user is a member is not configured on the device (as described in this section).
 - ✓ The device is not configured to query the LDAP server for a management attribute (see "Configuring LDAP Servers" on page 231).

Group objects represent groups in the LDAP server of which the user is a member. The access level represents the user account's permissions and rights in the device's management interface (e.g., Web and CLI). The access level can either be Monitor, Administrator, or Security Administrator. For an explanation on the privileges of each level, see "Configuring Management User Accounts" on page 60.

When the username-password authentication with the LDAP server succeeds, the device searches the LDAP server for all groups of which the user is a member. The LDAP query is based on the following LDAP data structure:

- Search base object (distinguished name or DN, e.g., "ou=ABC,dc=corp,dc=abc,dc=com"), which defines the location in the directory from which the LDAP search begins. This is configured in "Configuring LDAP DNs (Base Paths) per LDAP Server" on page 234.
- Filter (e.g., "(&(objectClass=person)(sAMAccountName=johnd))"), which filters the search in the subtree to include only the login username (and excludes others). For configuration, see "Configuring the LDAP Search Filter Attribute" on page 235.
- Attribute (e.g., "memberOf") to return from objects that match the filter criteria. This attribute is configured by the 'Management Attribute' parameter in the LDAP Servers table.

The LDAP response includes all the groups of which the specific user is a member, for example:

```
CN=# Support Dept,OU=R&D
Groups,OU=Groups,OU=APC,OU=Japan,OU=ABC,DC=corp,DC=abc,DC=com
CN=#AllCellular,OU=Groups,OU=APC,OU=Japan,OU=ABC,DC=corp,DC=abc,DC=com
```

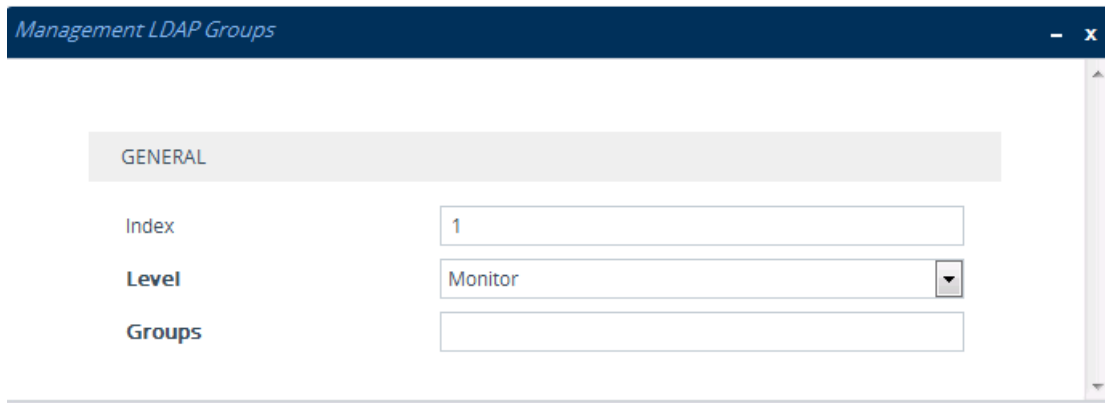
The device searches this LDAP response for the group names that you configured in the Management LDAP Groups table in order to determine the user's access level. If the device finds a group name, the user is assigned the corresponding access level and login is permitted; otherwise, login is denied. Once the LDAP response has been received (success or failure), the LDAP session terminates.

The following procedure describes how to configure an access level per management groups through the Web interface. You can also configure it through ini file (MgmtLDAPGroups) or CLI (configure system > ldap mgmt-ldap-groups).

- **To configure management groups and corresponding access level:**

 1. Open the LDAP Servers table (**Setup** menu > **IP Network** tab > **RADIUS & LDAP** folder > **LDAP Servers**).
 2. In the table, select the row of the LDAP server for which you want to configure management groups with a corresponding access level, and then click the **Management LDAP Groups** link located below the table; the Management LDAP Groups table opens.
 3. Click **New**; the following dialog box appears:

Figure 17-25: Management LDAP Groups Table - Add Dialog Box



4. Configure a group name(s) with a corresponding access level according to the parameters described in the table below.
5. Click **Apply**, and then save your settings to flash memory.

Table 17-11: Management LDAP Groups Table Parameter Descriptions

Parameter	Description
Index [MgmntLDAPGroups_GroupIndex]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
Level level [MgmntLDAPGroups_Level]	Defines the access level of the group(s). <ul style="list-style-type: none"> ▪ [0] Monitor (Default) ▪ [1] Admin ▪ [2] Security Admin
Groups groups [MgmntLDAPGroups_Group]	Defines the attribute names of the groups in the LDAP server. The valid value is a string of up to 256 characters. To define multiple groups, separate each group name with a semicolon (;).

17.4.8 Configuring the Device's LDAP Cache

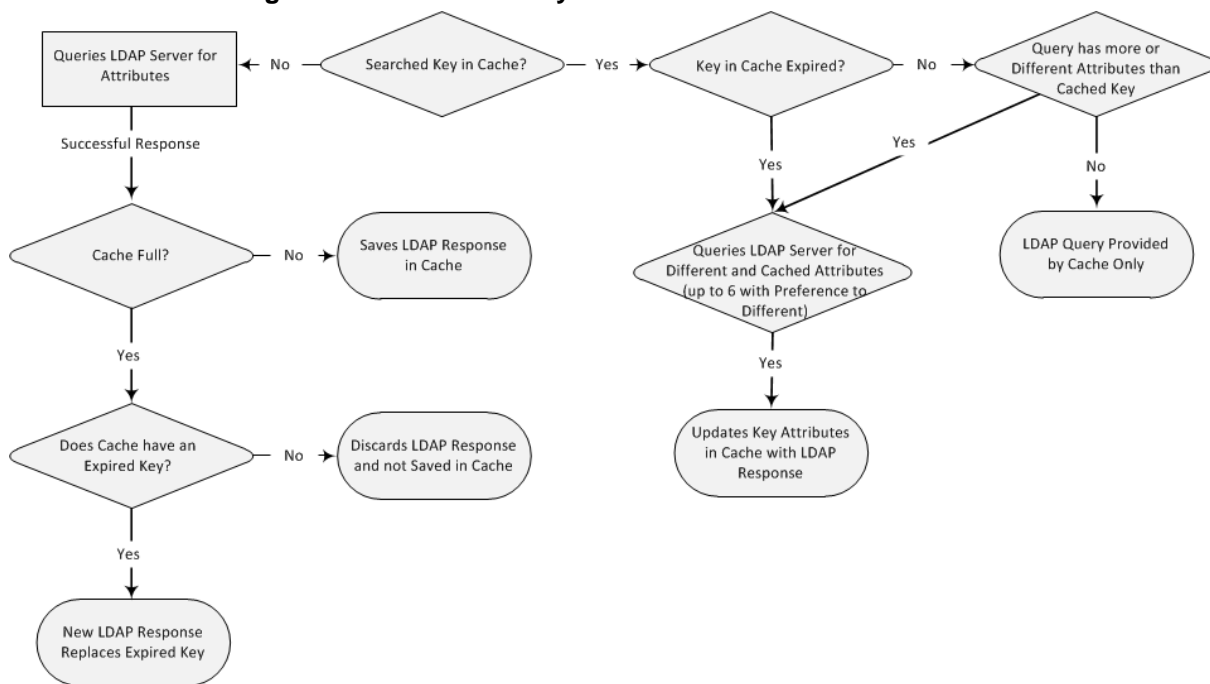
The device can optionally store LDAP queries of LDAP Attributes for a searched key with an LDAP server and the responses (results) in its local cache. The cache is used for subsequent queries and/or in case of LDAP server failure. The benefits of this feature include the following:

- 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 using the device's LDAP cache is shown in the flowchart below:

Figure 17-26: LDAP Query Process with Local LDAP Cache



If an LDAP query is required for an Attribute of a key that is already cached with that same Attribute, instead of sending a query to the LDAP server, the device uses the cache. However, if an LDAP query is required for an Attribute that does not appear for the cached key, the device queries the LDAP server and then saves the new Attribute (and response) in the cache for that key. When the device queries new Attributes for a cached key, the device also includes already cached Attributes of the key, while adhering to the maximum number of allowed saved Attributes (see note below), with preference to the new Attributes. In other words, if the cached key already contains the maximum Attributes and an LDAP query is required for a new Attribute, the device sends an LDAP query to the server for the new Attribute and for the five most recent Attributes already cached with the key. Upon the LDAP response, the new Attribute replaces the oldest cached Attribute while the values of the other Attributes are refreshed with the new response. The following table shows an example of different scenarios of LDAP queries of a cached key whose cached Attributes include a, b, c, and d, where a is the oldest and d the most recent Attribute:

Table 17-12: Example of LDAP Query for Cached Attributes

Attributes Requested in New LDAP Query for Cached Key	Attributes Sent in LDAP Query to LDAP Server	Attributes Saved in Cache after LDAP Response
e	e, a, b, c, d	e, a, b, c, d
e, f	e, f, a, b, c, d	e, f, a, b, c, d
e, f, g, h, i	e, f, g, h, i, a	e, f, g, h, i, a
e, f, g, h, i, j	e, f, g, h, i, j	e, f, g, h, i, j



Note:

- The LDAP Cache feature is applicable only to LDAP-based SIP queries (Control).
- The maximum LDAP cache size is 20,000 bytes.
- The device can save up to six LDAP Attributes in the cache per user (search LDAP key).
- The device also saves in the cache queried Attributes that do not have any values in the LDAP server.

The following procedure describes how to configure the device's LDAP cache through the Web interface. For a full description of the cache parameters, see "LDAP Parameters" on page 837.

➤ **To enable and configure the LDAP cache:**

1. Open the LDAP Settings page (**Setup** menu > **IP Network** tab > **RADIUS & LDAP** folder > **LDAP Settings**).

Figure 17-27: Enabling LDAP Cache

CACHE	
LDAP Cache Service	• Enable
LDAP Cache Entry Timeout	1200
LDAP Cache Entry Removal Timeout	0

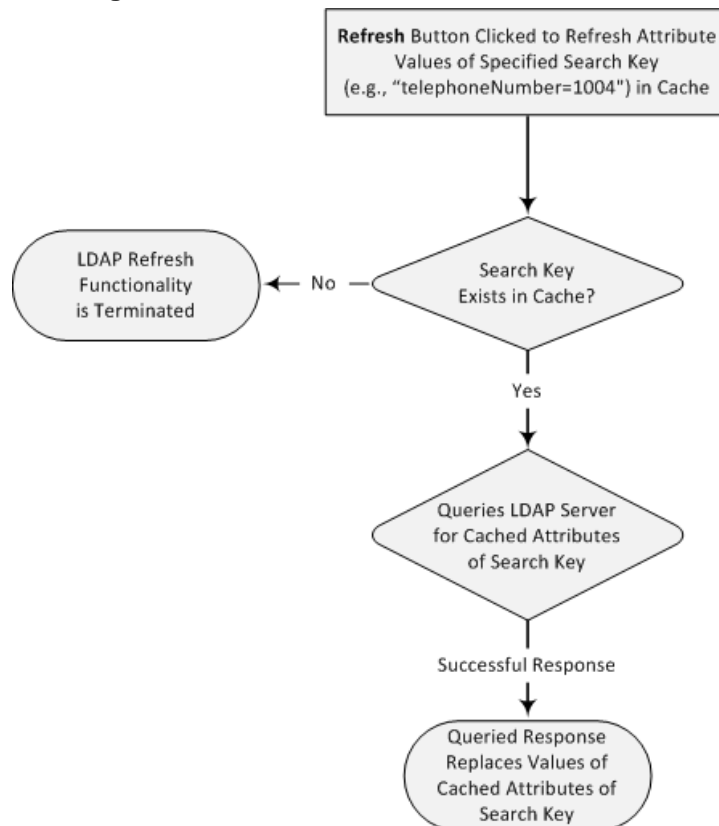
2. Under the Cache group, do the following:
 - a. From the 'LDAP Cache Service' drop-down list, select **Enable** to enable LDAP cache.
 - b. In the 'LDAP Cache Entry Timeout' field, enter the duration (in minutes) for which an entry in the LDAP cache is valid.
 - c. In the 'LDAP Cache Entry Removal Timeout' field, enter the duration (in hours) after which the device removes the LDAP entry from the cache.
3. Click **Apply**, and then reset the device with a save-to-flash for your settings to take effect.

17.4.8.1 Refreshing the LDAP Cache

You can refresh values of LDAP Attributes associated with a specified LDAP search key that are stored in the device's LDAP cache. The device sends an LDAP query to the LDAP server for the cached Attributes of the specified search key and replaces the old values in the cache with the new values received in the LDAP response.

For example, assume the cache contains a previously queried LDAP Attribute "telephoneNumber=1004" whose associated Attributes include "displayName", "mobile" and "ipPhone". If you perform a cache refresh based on the search key "telephoneNumber=1004", the device sends an LDAP query to the server requesting values for the "displayName", "mobile" and "ipPhone" Attributes of this search key. When the device receives the LDAP response, it replaces the old values in the cache with the new values received in the LDAP response.

Figure 17-28: LDAP Cache Refresh Flowchart



➤ **To refresh the LDAP cache per LDAP Server Group:**

1. Open the LDAP Settings page (**Setup** menu > **IP Network** tab > **RADIUS & LDAP** folder > **LDAP Settings**).

Figure 17-29: Refreshing LDAP Cache

CACHE ACTIONS	
LDAP Group Index	<input type="text" value="1"/>
LDAP Refresh Cache by Key	<input type="text" value="telephoneNumber="/> <input type="button" value="Refresh"/>

2. Under the Cache Actions group, do the following:
 - a. From the 'LDAP Group Index' drop-down list, select the required LDAP Server Group (see "Configuring LDAP Server Groups" on page 228).
 - b. In the 'LDAP Refresh Cache by Key' field, enter the LDAP search key that you want to refresh (e.g., telephoneNumber=1004).
 - c. Click **Refresh**; if a request with the specified key exists in the cache, a request is sent to the LDAP server for the Attributes associated in the cache with the search key.

17.4.8.2 Clearing the LDAP Cache

You can remove (clear) all LDAP entries in the device's LDAP cache for a specific LDAP Server Group, as described in the following procedure.

➤ **To clear the LDAP cache:**

1. Open the LDAP Settings page (**Setup** menu > **IP Network** tab > **RADIUS & LDAP** folder > **LDAP Settings**).
2. Under the Cache Actions group, do the following:
 - a. From the 'LDAP Group Index' drop-down list, select the required LDAP Server Group (see "Configuring LDAP Server Groups" on page 228).
 - b. Click **Clear Group**.

17.4.9 Configuring Local Database for Management User Authentication

You can configure the device to use the Local Users table (local database) to authenticate management users based on username-password combination. You can configure the device to use the Local Users table (see "Configuring Management User Accounts" on page 60) upon the following scenarios:

- LDAP or RADIUS server is not configured (or broken connection) or always use the Local Users table and only if the user is not found, to use the server.
- Connection with the LDAP or RADIUS server fails due to a timeout. In such a scenario, the device can deny access or verify the user's credentials (username-password) locally in the Local Users table.

If user authentication using the Local Users table succeeds, the device grants management access to the user; otherwise access is denied. The access level assigned to the user is also determined by the Local Users table.



Note:

- This feature is applicable to LDAP and RADIUS.
- This feature is applicable only to user management authentication.

➤ **To use the Local Users table for authenticating management users:**

1. Open the Authentication Server page (**Setup** menu > **Administration** tab > **Web & CLI** folder > **Authentication Server**).

Figure 17-30: Local Users Table for Login Authentication

Use Local Users Database	When No Auth Server Defined	⚡
Behavior upon Authentication Server Timeout	Verify Access Locally	⚡

2. Under the General group, do the following:
 - a. Configure when the Local Users table must be used to authenticate login users. From the 'Use Local Users Database' drop-down list, select one of the following:
 - ◆ **When No Auth Server Defined (default):** When no LDAP/RADIUS server is configured or if a server is configured but connectivity with the server is down (if the server is up, the device authenticates the user with the server).
 - ◆ **Always:** First attempts to authenticate the user using the Local Users table, but if not found, it authenticates the user with the LDAP/RADIUS server.

- **DN (base path):** OU=testMgmt,OU=QA,DC=testqa,DC=local. The DN path to search for the username in the directory is shown below:

Figure 17-31: Base Path (DN) in LDAP Server

Path: CN=John Doe,OU=testMgmt,OU=QA,DC=testqa,DC=local, 10.3.9.93 [testqa.testqa.local]

Active Directory Explorer

10.3.9.93 [testqa.testqa.local]

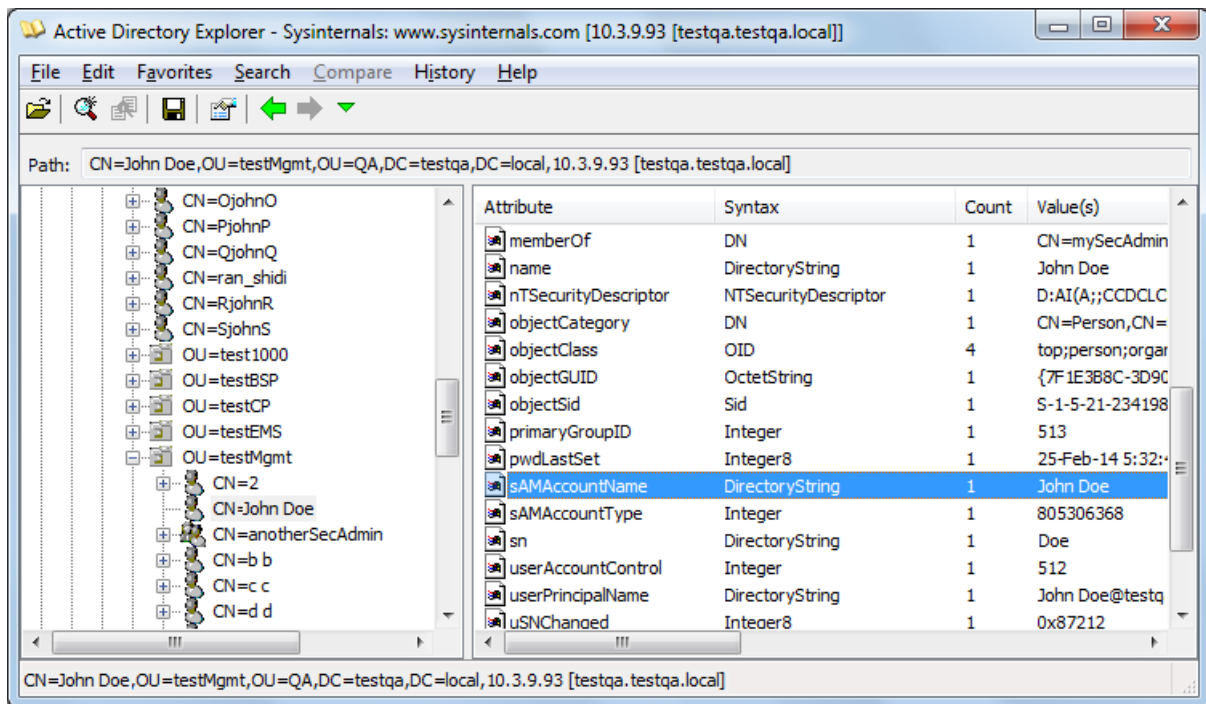
- DC=testqa,DC=local
 - CN=Builtin
 - CN=Computers
 - CN=Deleted Objects
 - OU=Domain Controllers
 - CN=ForeignSecurityPrincipals
 - CN=Infrastructure
 - CN=LostAndFound
 - CN=NTDS Quotas
 - CN=Program Data
 - OU=QA
 - CN=Aaapaul50digitsL
 - CN=Aaapaul51digitsL
 - CN=AjohnA
 - CN=BjohnB
 - CN=CjohnC
 - CN=DjohnD
 - CN=EjohnE
 - CN=Firstaaaa Lastbbbb
 - CN=FjohnF
 - CN=George Harrison
 - CN=GjohnG
 - CN=HjohnH
 - CN=IjohnI
 - CN=JjohnJ
 - CN=John Doe
 - CN=John Doe Bind
 - CN=KjohnK
 - CN=LjohnL
 - OU=Misc
 - CN=MjohnM
 - CN=NjohnN
 - CN=OjohnO
 - CN=PjohnP
 - CN=QjohnQ
 - CN=ran_shidi
 - CN=RjohnR
 - CN=SjohnS
 - OU=test1000
 - OU=testBSP
 - OU=testCP
 - OU=testEMS
 - OU=testMgmt
 - CN=2
 - CN=John Doe
 - CN=anotherSecAdmin
 - CN=b b
 - CN=c c
 - CN=d d

Attribute	Syntax	Count	Value(s)
accountExpires	Integer8	1	0x7FFFFFFFFFFFFFFF
badPasswordTime	Integer8	1	06-Mar-14 10:03:18 AM
badPwdCount	Integer	1	0
cn	DirectoryString	1	John Doe
codePage	Integer	1	0
countryCode	Integer	1	0
description	DirectoryString	1	10600
displayName	DirectoryString	1	John Doe
distinguishedName	DN	1	CN=John Doe,OU=testMgm
givenName	DirectoryString	1	John
instanceType	Integer	1	4
lastLogoff	Integer8	1	0x0
lastLogon	Integer8	1	06-Mar-14 10:03:41 AM
logonCount	Integer	1	0
memberOf	DN	1	CN=mySecAdmin,OU=testM
name	DirectoryString	1	John Doe
nTSecurityDescriptor	NTSecurityDescriptor	1	D:AI(A;;CCDCLCSWRPWPDP
objectCategory	DN	1	CN=Person,CN=Schema,CN
objectClass	OID	4	top;person;organizationalPe
objectGUID	OctetString	1	{7F1E3B8C-3D90-47BC-A9E
objectSid	Sid	1	S-1-5-21-2341986137-2970
primaryGroupID	Integer	1	513
pwdLastSet	Integer8	1	25-Feb-14 5:32:45 PM
sAMAccountName	DirectoryString	1	John Doe
sAMAccountType	Integer	1	805306368
sn	DirectoryString	1	Doe
userAccountControl	Integer	1	512
userPrincipalName	DirectoryString	1	John.Doe@testqa.local
uSNChanged	Integer8	1	0x87212
uSNCreated	Integer8	1	0x8311F
whenChanged	GeneralizedTime	1	25-Feb-14 5:32:45 PM
whenCreated	GeneralizedTime	1	06-Oct-02 5:27:51 AM

CN=John Doe,OU=testMgmt,OU=QA,DC=testqa,DC=local, 10.3.9.93 [testqa.testqa.local]

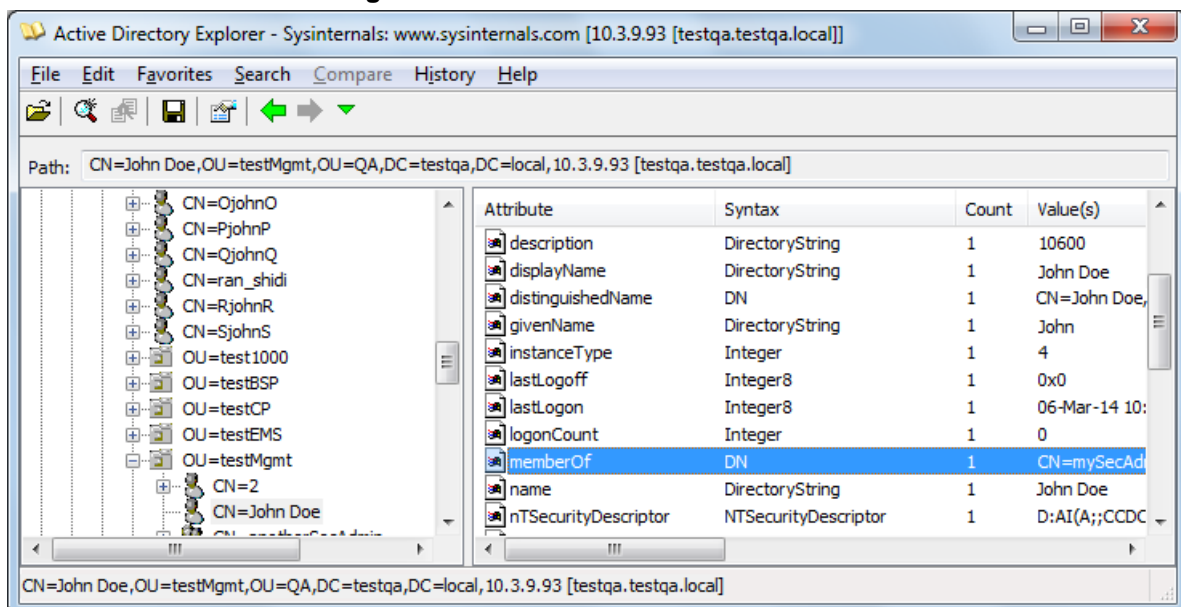
- **Search Attribute Filter:** (sAMAccountName=\$). The login username is found based on this attribute (where the attribute's value equals the username):

Figure 17-32: Username Found using sAMAccount Attribute Search Filter



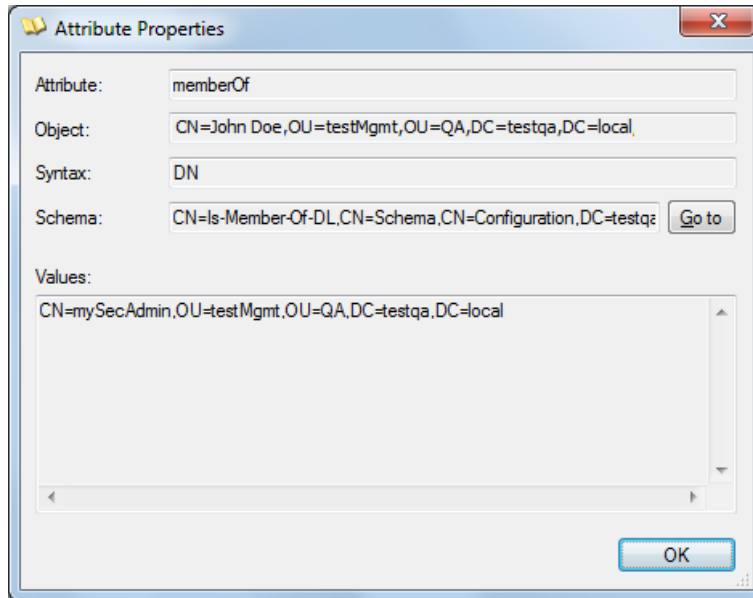
- **Management Attribute:** memberOf. The attribute contains the member groups of the user:

Figure 17-33: User's memberOf Attribute



- **Management Group:** mySecAdmin. The group to which the user belongs, as listed under the memberOf attribute:

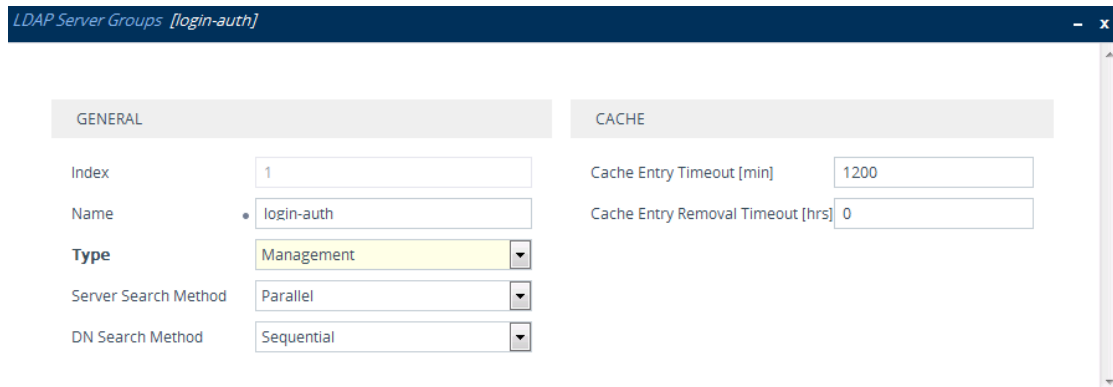
Figure 17-34: User's mySecAdmin Group in memberOf Management Attribute



The configuration to match the above LDAP data structure schema is as follows:

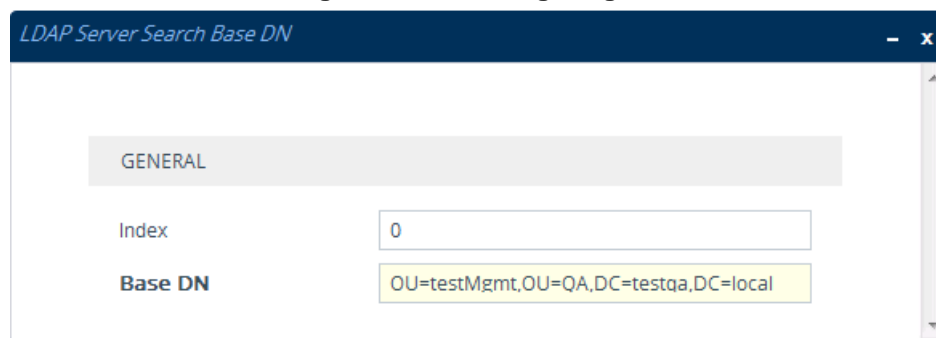
- LDAP-based login authentication (management) is enabled in the LDAP Server Groups table (see "Configuring LDAP Server Groups" on page 228):

Figure 17-35: Configuring LDAP Server Group for Management



- The DN is configured in the LDAP Server Search Base DN table (see "Configuring LDAP DN's (Base Paths) per LDAP Server" on page 234):

Figure 17-36: Configuring DN



- The search attribute filter based on username is configured by the 'LDAP

Authentication Filter' parameter (see "Configuring the LDAP Search Filter Attribute" on page 235):

Figure 17-37: Configuring Search Attribute Filter

GENERAL

LDAP Service: Enable

LDAP Authentication Filter: (\$AMAccountName=\$)

- The group management attribute is configured by the 'Management Attribute' parameter in the LDAP Servers table:

Figure 17-38: Configuring Management Attribute

LDAP Servers

LDAP Servers Group: #1 [login-auth]

GENERAL

Index: 0

LDAP Network Interface: #0 [O+M+C] View

Use TLS: No

TLS Context: -- View

QUERY

LDAP Password:

LDAP Bind DN: \$@testqa.local

Management Attribute: memberOf

CONNECTION

LDAP Server IP: 10.3.9.93

LDAP Server Port: 389

LDAP Server Max Respond Time [msec]: 3000

LDAP Server Domain Name:

Connection Status:

Verify Certificate: No

- The management group and its corresponding access level is configured in the Management LDAP Groups table (see "Configuring Access Level per Management Groups Attributes" on page 236):

Figure 17-39: Configuring Management Group Attributes for Determining Access Level

Management LDAP Groups

GENERAL

Index: 0

Level: Security Admin

Groups: mySecAdmin

17.4.11 Enabling LDAP Searches for Numbers with Characters

Typically, the device performs LDAP searches in the AD for complete numbers where the digits are adjacent to one another (e.g., 5038234567). However, if the number is defined in the AD with characters (such as spaces, hyphens and periods) separating the digits (e.g., 503-823 4567), the LDAP query returns a failed result.

To enable the device to search the AD for numbers that may contain characters between its digits, you need to specify the Attribute (up to five) for which you want to apply this functionality, using the `LDAPNumericAttributes` parameter. For example, the `telephoneNumber` Attribute could be defined in AD with the telephone number "503-823-4567" (i.e., hyphens), "503.823.4567" (i.e., periods) or "503 823 4567" (i.e., spaces). If the device performs an LDAP search on this Attribute for the number 5038234567, the LDAP query will return results only if you configure the `LDAPNumericAttributes` parameter with the `telephoneNumber` Attribute. To search for the number with characters, the device inserts the asterisk (*) wildcard between all digits in the LDAP query (e.g., `telephoneNumber = 5*0*3*8*2*3*4*5*6*7`). As the AD server recognizes the * wildcard as representing any character, it returns all possible results to the device. Note that the wildcard represents only a character; a query result containing a digit in place of a wildcard is discarded and the device performs another query for the same Attribute. For example, it may return the numbers 533-823-4567 (second digit "3" and hyphens) and 503-823-4567. As the device discards query results where the wildcard results in a digit, it selects 503-823-4567 as the result. The correct query result is cached by the device for subsequent queries and/or in case of LDAP server failure.

17.4.12 AD-based Routing for Microsoft Skype for Business

Typically, enterprises wishing to deploy the Microsoft® Skype for Business (formerly known as Lync) are faced with a complex, call routing dial plan when migrating users from their existing PBX or IP PBX to the Skype for Business 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 outbound IP call routing decisions based on information stored on the AD. Based on queries sent to the AD, the device can route the call to one of the following IP domains:

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

17.4.12.1 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, Skype for Business 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 17-13: Parameters for Configuring Query Attribute Key

Parameter	Queried User Domain (Attribute) in AD	Query or Query Result Example
MSLDAPPBXNumAttributeName	PBX or IP PBX number (e.g., "telephoneNumber" - default)	telephoneNumber= +3233554447
MSLDAPOCSNumAttributeName	Mediation Server / Skype for Business client number (e.g., "msRTCSIP-Line")	msRTCSIP-Line=john.smith@company.com
MSLDAPMobileNumAttributeName	Mobile number (e.g., "mobile")	mobile=+3247647156
MSLDAPPrivateNumAttributeName	Any attribute (e.g., "msRTCSIP-PrivateLine") Note: Used only if set to same value as Primary or Secondary key.	msRTCSIP-PrivateLine= +3233554480
MSLDAPPrimaryKey	Primary Key query search instead of PBX key - can be any AD attribute	msRTCSIP-PrivateLine= +3233554480
MSLDAPSecondaryKey	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 queries the following attributes (if configured):
 - 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 - Skype for Business, 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 Tel-to-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:<Skype for Business_number>): used to match a routing rule based on query results of the Skype for Business 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

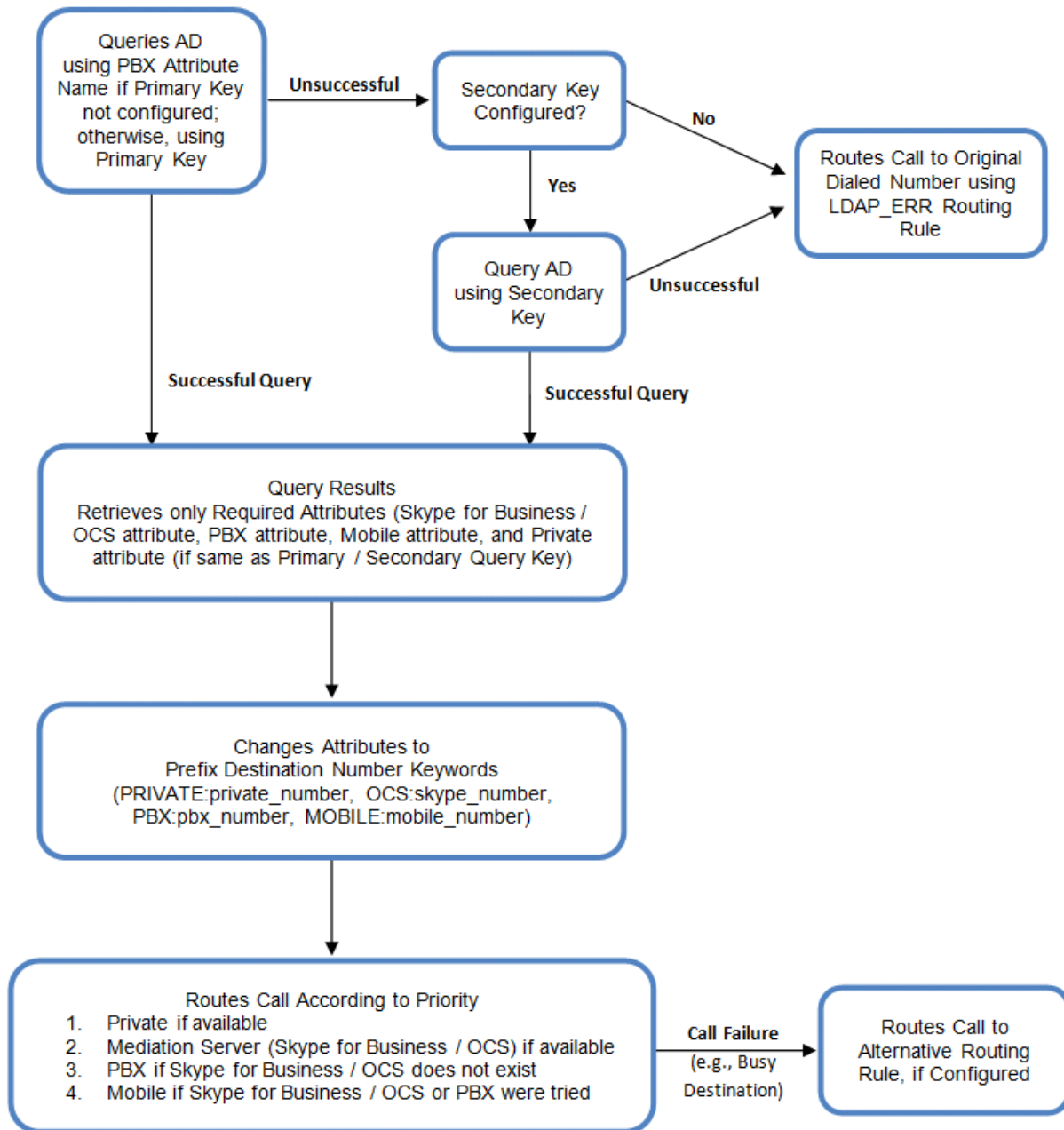


Note: These prefixes are involved only in the routing and manipulation processes; they are not used as the final destination number.

7. The device uses the Tel-to-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, the device routes the call according to this attribute.
 2. **Mediation Server SIP address (Skype for Business):** If the private attribute does not exist or is not queried, the device routes the call to the Mediation Server (which then routes the call to the Skype for Business client).
 3. **PBX / IP PBX:** If the Skype for Business client is not found in the AD, it routes the call to the PBX / IP PBX.
 4. **Mobile number:** If the Skype for Business client (or Mediation Server) is unavailable (e.g., SIP response 404 "Not Found" upon INVITE sent to Skype for Business client), and the PBX / IP PBX is also unavailable, 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.

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

Figure 17-40: Querying AD in Skype for Business Environment



Note: If you are using the device's local LDAP cache, see "Configuring the Device's LDAP Cache" on page 238 for the LDAP query process.

17.4.12.2 Configuring AD-Based Routing Rules

The following procedure describes how to configure outbound IP routing based on LDAP queries.

➤ **To configure LDAP-based IP routing for Skype for Business:**

1. Configure the LDAP server parameters, as described in "Configuring LDAP Servers" on page 231.
2. Configure the AD attribute names used in the LDAP query:
 - a. Open the SIP Definitions General Settings page (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **SIP Definitions General Settings**).

Figure 17-41: LDAP Parameters for Microsoft Skype for Business

ACTIVE DIRECTORY	
LDAP Numeric Attributes	<input type="text"/>
LDAP OCS Number Attribute Name	<input type="text" value="msRTCSIP-Line"/>
MS LDAP PBX Number Attribute Name	<input type="text" value="telephoneNumber"/>
LDAP MOBILE Number Attribute Name	<input type="text" value="mobile"/>
LDAP DISPLAY Name Attribute Name	<input type="text" value="displayName"/>
LDAP PRIVATE Number Attribute Name	<input type="text" value="msRTCSIP-PrivateLine"/>
LDAP Primary Key	• <input type="text" value="telephoneNumber"/>
LDAP Secondary Key	<input type="text"/>

- b. Configure the LDAP attribute names as desired.
3. Configure query-result routing rules for each IP domain (private, PBX / IP PBX, Skype for Business clients, and mobile), using the LDAP keywords (case-sensitive) for the prefix destination number:
4. Configure AD-based IP-to-IP routing rules:
 - a. Open the IP-to-IP Routing table (see Configuring SBC IP-to-IP Routing Rules on page 470).
 - b. Configure query-result routing rules for each IP domain (private, PBX / IP PBX, Skype for Business clients, and mobile), using the LDAP keywords (case-sensitive) in the Destination Username Prefix field:
 - ◆ PRIVATE: Private number
 - ◆ OCS: Skype for Business 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 17-14: 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 Skype for Business client (i.e., Mediation Server at 10.33.45.68) upon successful AD query result for the Skype for Business 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, Skype for Business, PBX, and mobile), and a relevant SBC Alternative Routing Reason (see Configuring SIP Response Codes for Alternative Routing Reasons on page 482) 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.

17.5 Least Cost Routing

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

17.5.1 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 IP-to-IP Routing table. The device searches the routing table for matching routing rules and then selects the rule with the lowest call cost. If two routing rules have identical costs, the rule appearing higher up in the table is used (i.e., first-matched rule). If the selected route is unavailable, the device selects the next least-cost routing rule.

Even if a matched routing rule is not assigned a Cost Group, the device can select it as the preferred route over other matched rules that are assigned Cost Groups. This is determined according to the settings of the 'Default Call Cost' parameter configured for the Routing Policy (associated with the routing rule). To configure the Routing Policy, see [Configuring SBC Routing Policy Rules on page 484](#).

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:

$$\text{Total Call Cost} = \text{Connection Cost} + (\text{Minute Cost} * \text{Average Call Duration})$$

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 17-15: 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 rule.

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:

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 Tel-to-IP Routing table:

The 'Default Call Cost' parameter in the Routing Policy rule is configured to **Lowest Cost**, meaning that if the device locates other matching 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:

Routing Index	Dest Phone Prefix	Destination IP	Cost Group
1	201	x.x.x.x	"A"
2	201	x.x.x.x	"B"
3	201	x.x.x.x	0
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 Call Cost' parameter is configured to **Lowest Cost**, 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

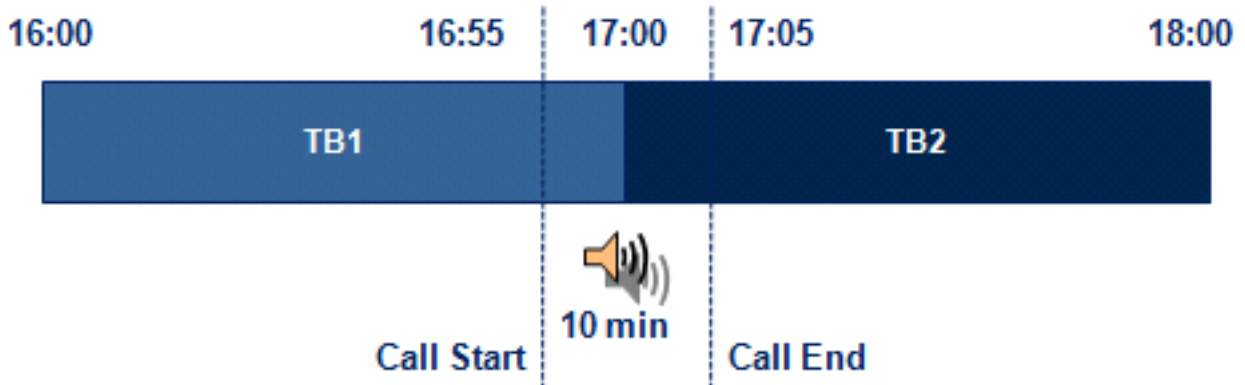
over multiple time bands:

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 17-42: 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:

$$\text{Total call cost} = \text{"TB1" Connection Cost} + (\text{"TB1" Minute Cost} \times \text{call duration}) = 2 + 1 \times 10 \text{ min} = 12$$

17.5.2 Configuring LCR

To configure LCR, perform the following main steps:

1. Enable LCR - see Configuring SBC Routing Policy Rules on page 484.
2. Configure Cost Groups - see "Configuring Cost Groups" on page 256.
3. Configure Time Bands for a Cost Group - see "Configuring Time Bands for Cost Groups" on page 257.
4. Assign Cost Groups to outbound IP routing rules - see "Assigning Cost Groups to Routing Rules" on page 259.

17.5.2.1 Configuring Cost Groups

The Cost Groups table lets you configure up to 10 Cost Groups. A Cost Group defines a fixed call connection cost and a call rate (charge per minute). Once configured, you can configure Time Bands per Cost Group.

The following procedure describes how to configure Cost Groups through the Web interface. You can also configure it through ini file (CostGroupTable) or CLI (configure voip > sip-definition least-cost-routing cost-group).

➤ **To configure a Cost Group:**

1. Open the Cost Groups table (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Least Cost Routing** > **Cost Groups**).

- Click **New**; the following dialog box appears:

- Configure a Cost Group according to the parameters described in the table below.
- Click **Apply**, and then save your settings to flash memory.

Table 17-16: Cost Groups Table Parameter Descriptions

Parameter	Description
Index [CostGroupTable_Index]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
Name cost-group-name [CostGroupTable_CostGroupName]	Defines an arbitrary name to easily identify the row. The valid value is a string of up to 40 characters. Note: Each Cost Group must have a unique name.
Default Connection Cost default-connection-cost [CostGroupTable_DefaultConnectionCost]	Defines the call connection cost (added as a fixed charge to the call) for a call outside the time bands. The valid value range is 0-65533. The default is 0. Note: 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 Minute Cost default-minute-cost [CostGroupTable_DefaultMinuteCost]	Defines the call charge per minute for a call outside the time bands. The valid value range is 0-65533. The default is 0. Note: 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.

17.5.2.1 Configuring Time Bands for Cost Groups

The Time Band table lets you configure Time Bands per Cost Group. A Time Band defines a day and time range (e.g., from Saturday 05:00 to Sunday 24:00) and a fixed call connection charge and call rate per minute for this interval. You can configure up to 70 Time Bands, where up to 21 Time Bands can be assigned to each Cost Group.



Note:

- You cannot configure overlapping Time Bands.
- If a Time Band is not configured for a specific day and time range, the default connection cost and default minute cost configured for the Cost Group in the Cost Groups table is applied.

The following procedure describes how to configure Time Bands per Cost Group through the Web interface. You can also configure it through ini file (CostGroupTimebands) or CLI (configure voip > sip-definition least-cost-routing cost-group-time-bands).

➤ **To configure a Time Band per Cost Group:**

1. Open the Cost Groups table (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Least Cost Routing** > **Cost Groups**).
2. 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.
3. Click **New**; the following dialog box appears:

4. Configure a Time Band according to the parameters described in the table below.
5. Click **Apply**, and then save your settings to flash memory.

Table 17-17: Time Band Table Description

Parameter	Description
Index timeband-index [CostGroupTimebands_TimebandIndex]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
Start Time start-time [CostGroupTimebands_StartTime]	Defines the day and time of day from when this time band is applicable. The format is DDD:hh:mm, where: <ul style="list-style-type: none"> ▪ <i>DDD</i> is the day of the week, represented by the first three letters of the day in upper case (i.e., SUN, MON, TUE, WED, THU, FRI, or SAT). ▪ <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) For example, SAT:22:00 denotes Saturday at 10 pm.

Parameter	Description
End Time end-time [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 connection-cost [CostGroupTimebands_ConnectionCost]	Defines the call connection cost during the time band. This is added as a fixed charge to the call. The valid value range is 0-65533. The default is 0. Note: The entered value must be a whole number (i.e., not a decimal).
Minute Cost minute-cost [CostGroupTimebands_MinuteCost]	Defines the call cost per minute charge during the time band. The valid value range is 0-65533. The default is 0. Note: The entered value must be a whole number (i.e., not a decimal).

17.5.2.2 Assigning Cost Groups to Routing Rules

To use your configured Cost Groups, you need to assign them to routing rules:

- IP-to-IP Routing table - see Configuring SBC IP-to-IP Routing Rules on page 470

17.6 Remote Web Services

This section describes configuration for remote Web services.

17.6.1 Configuring Remote Web Services

The Remote Web Services table lets you configure up to seven Web-based (HTTP/S) services provided by third-party, remote HTTP/S hosts. The following types of services can be offered by the remote host:

- **Routing:** Call routing service, whereby the remote host (e.g., routing server) determines the next hop of an incoming call on the path to the final destination. For more information on employing a third-party, remote routing server, see "Centralized Third-Party Routing Server" on page 266.
- **Call Status:** Call status of calls processed by the device. The call status is provided to the remote host through CDRs sent by the device.
- **Topology Status:** Status of device configuration (add, edit and delete). The device sends topology status to the HTTP host, using the REST TopologyStatus API command. To enable the functionality, see "Enabling Topology Status Services" on page 265.

Topology status includes the following:

- IP Group Connectivity: Status is reported when the keep-alive mechanism, enabled for the associated Proxy Set, detects that the IP Group is unavailable, or when CAC thresholds (configured in the Admission Control table) associated with the IP Group are crossed.

- Configuration Status: Status is reported when IP Groups or SIP Interfaces that are configured to be used by remote Web-based services (i.e., the UsedByRoutingServer parameter is set to 1 - Used) are created or deleted. If you subsequently change the settings of the UsedByRoutingServer parameter or the 'Name' parameter, the device reports the change as a creation or deletion of the corresponding configuration entity.
- **Capture:** Recording of signaling and RTP packets, and Syslog. The remote host can be, for example, a Syslog server or AudioCodes SEM.



Note:

- You can configure only **one** Remote Web Service for Routing, for Call Status, and for Topology. However, you can configure up to four Remote Web Services for Capture.
- The Routing service also includes the Call Status and Topology Status services.
- Currently, the Capture service is not supported.
- The device supports HTTP redirect responses (3xx) only during connection establishment with the host. Upon receipt of a redirect response, the device attempts to open a new socket with the host and if this is successful, closes the current connection.

The following procedure describes how to configure Remote Web Services through the Web interface. You can also configure it through ini file (HTTPRemoteServices) or CLI (configure system > http-services > http-remote-services).

➤ **To configure a remote Web service:**

1. Open the Remote Web Services table (**Setup** menu > **IP Network** tab > **Web Services** folder > **Remote Web Services**).
2. Click **New**; the following dialog box appears:

Figure 17-43: Remote Web Services Table - Add Dialog Box

GENERAL		LOGIN	
Index	0	Login Needed	Enable
Name		Username	user
Type	Routing	Password	
Path	api	SECURITY	
Status		TLS Context	--
CONNECTION		Verify Certificate	Disable
Policy	Round Robin	TIMEOUTS	
Persistent Connection	Enable	Response Timeout [sec]	5
Number of Sockets	1	Keep-Alive Timeout [sec]	0

3. Configure a remote Web service according to the parameters described in the table below.

4. Click **Apply**, and then save your settings to flash memory.

Table 17-18: Remote Web Services Table Parameter Descriptions

Parameter	Description
General	
Index [HTTPRemoteServices_Index]	Defines an index number for the new table row. Note: <ul style="list-style-type: none"> ▪ Each row must be configured with a unique index. ▪ The parameter is mandatory.
Name rest-name [HTTPRemoteServices_Name]	Defines an arbitrary name to easily identify the row. The valid value is a string of up to 40 characters. Note: <ul style="list-style-type: none"> ▪ Each row must be configured with a unique name. ▪ The parameter is mandatory.
Type rest-message-type [HTTPRemoteServices_HTTPType]	Defines the type of service provided by the HTTP remote host: <ul style="list-style-type: none"> ▪ [0] Routing (default) = Routing service (also includes Call Status and Topology Status). ▪ [1] Call Status = Call status service. ▪ [2] Topology Status = Topology status service (e.g., change in configuration). ▪ [3] Capture = Recording of signaling and RTP packets, which can be sent to a remote host, for example, to a Syslog server or AudioCodes SEM. Note: <ul style="list-style-type: none"> ▪ You can configure only one remote Web service for each of the following service types: Routing, Call Status, and Topology Status. ▪ For the Topology Status option to be functional, you must enable the functionality (see "Enabling Topology Status Services" on page 265). ▪ The Routing option also includes the Call Status and Topology Status services. ▪ Currently, the Capture option is not supported.
Path rest-path [HTTPRemoteServices_Path]	Defines the path (prefix) to the REST APIs. The valid value is a string of up to 80 characters. The default is "api".
Status http-service-state [HTTPRemoteServices_ServiceStatus]	(Read-only) Displays the status of the host associated with the Web service. <ul style="list-style-type: none"> ▪ "Connected": At least one of the hosts is connected. ▪ "Disconnected": All hosts are disconnected. ▪ "Not In Service": Configuration of the service is invalid.
Connection	
Policy http-policy [HTTPRemoteServices_Policy]	Defines the mode of operation when you have configured multiple remote hosts (in the HTTP Remote Hosts table) for a specific remote Web service. <ul style="list-style-type: none"> ▪ [0] Round Robin = (Default) Load balancing of traffic across all configured hosts. Every consecutive message is sent to

Parameter	Description
	<p>the next available host.</p> <ul style="list-style-type: none"> [1] Sticky Primary = Device always attempts to send traffic to the first (primary) host. If the host does not respond, the device sends the traffic to the next available host. If the primary host becomes available again, the device sends the traffic to the primary host. [2] Sticky Next = Similar to Sticky Primary, but if the primary host does not respond, the device sends the traffic to the next available host and continues sending traffic to this host even if the primary host becomes available again.
Persistent Connection <code>http-persistent-connection</code> [HTTPRemoteServices_PersistentConnection]	Defines whether the HTTP connection with the host remains open or is only opened per request. <ul style="list-style-type: none"> [0] Disable = Connection is not persistent and closes when the device detects inactivity. The device uses HTTP keep-alive messages to detect inactivity. [1] Enable = (Default) Connection remains open (persistent) even during inactivity. The device uses HTTP keep-alive / HTTP persistent connection messages to keep the connection open.
Number of Sockets <code>http-num-sockets</code> [HTTPRemoteServices_NumOfSockets]	Defines how many sockets (connection) are established per remote host. The valid value is 1 to 10. The default is 1.
Login	
Login Needed <code>http-login-needed</code> [HTTPRemoteServices_LoginNeeded]	Enables the use of proprietary REST API Login and Logout commands for connecting to the remote host. The commands verify specific information (e.g., software version) before allowing connectivity with the device. <ul style="list-style-type: none"> [0] Disable = Commands are not used. [1] Enable (default)
Username <code>rest-user-name</code> [HTTPRemoteServices_AuthUsername]	Defines the username for HTTP authentication. The valid value is a string of up to 80 characters. The default is "user".
Password <code>rest-password</code> [HTTPRemoteServices_AuthPassword]	Defines the password for HTTP authentication. The valid value is a string of up to 80 characters. The default is "password".
Security	
TLS Context <code>rest-tls-context</code> [HTTPRemoteServices_TLSContext]	Assigns a TLS Context for connection with the remote host. By default, no value is defined. To configure TLS Contexts, see "Configuring TLS Certificate Contexts" on page 99. Note: The parameter is applicable only if the connection is HTTPS.
Verify Certificate <code>rest-verify-certificates</code>	Enables certificate verification when connection with the host is based on HTTPS.

Parameter	Description
[HTTPRemoteServices_VerifyCertificate]	<ul style="list-style-type: none"> ▪ [0] Disable = (Default) No certificate verification is done. ▪ [1] Enable = The device verifies the authentication of the certificate received from the HTTPS peer. The device authenticates the certificate against the trusted root certificate store associated with the associated TLS Context (see 'TLS Context' parameter above) and if ok, allows communication with the HTTPS peer. If authentication fails, the device denies communication (i.e., handshake fails). The device can also authenticate the certificate by querying with an Online Certificate Status Protocol (OCSP) server whether the certificate has been revoked. This is also configured for the associated TLS Context. <p>Note: The parameter is applicable only if the connection is HTTPS.</p>
Timeouts	
Response Timeout rest-timeout [HTTPRemoteServices_TimeOut]	<p>Defines the TCP response timeout (in seconds) from the remote host. If one of the remote hosts does not respond to a request within the specified timeout, the device closes the corresponding socket and attempts to connect to the next remote host.</p> <p>The valid value is 1 to 65535. The default is 5.</p>
Keep-Alive Timeout rest-ka-timeout [HTTPRemoteServices_KeepAliveTimeOut]	<p>Defines the duration/timeout (in seconds) in which HTTP-REST keep-alive messages are sent by the device if no other messages are sent. Keep-alive messages may be required for HTTP services that expire upon inactive sessions.</p> <p>The valid value is 0 to 65535. The default is 0 (i.e., no keep-alive messages are sent).</p> <p>Note: The parameter is applicable only if the 'Persistent Connection' parameter (in the table) is configured to Enable.</p>

17.6.1.1 Configuring Remote HTTP Hosts

The HTTP Remote Hosts table lets you configure up to 10 remote HTTP hosts per Remote Web Service. The HTTP Remote Hosts table is a "child" of the Remote Web Services table (configured in "Configuring Remote Web Services" on page 259).

The following procedure describes how to configure HTTP Remote hosts through the Web interface. You can also configure it through ini file (HTTPRemoteServices) or CLI (configure system > http-services > http-remote-hosts).

➤ **To configure a remote HTTP host:**

1. Open the Remote Web Services table (**Setup** menu > **IP Network** tab > **Web Services** folder > **Remote Web Services**).
2. In the table, select the required remote Web service index row, and then click the **HTTP Remote Hosts** link located below the table; the HTTP Remote Hosts table appears.

- Click **New**; the following dialog box appears:

Figure 17-44: HTTP Remote Hosts Table - Add Dialog Box

- Configure an HTTP remote host according to the parameters described in the table below.
- Click **Apply**, and then save your settings to flash memory.

Table 17-19: HTTP Remote Hosts Table Parameter Descriptions

Parameter	Description
Index rest-servers [HTTPRemoteHosts_RemoteHostindex]	Defines an index number for the new table row. Note: <ul style="list-style-type: none"> Each row must be configured with a unique index. The parameter is mandatory.
Name [HTTPRemoteHosts_Name]	Defines an arbitrary name to easily identify the row. The valid value is a string of up to 40 characters. By default, no value is defined. Note: <ul style="list-style-type: none"> Each row must be configured with a unique name. The parameter is mandatory.
Address rest-address [HTTPRemoteHosts_Address]	Defines the address (IP address or FQDN) of the remote host. The valid value is a string of up to 80 characters. Note: <ul style="list-style-type: none"> An IPv6 address can only be configured if the interface is a CONTROL type. If the address is an FQDN and the DNS resolution results in multiple IP addresses, the device device attempts to establish multiple connections (sessions) for each IP address. Only the first 10 resolved IP addresses are used regardless of the number of hosts. FQDN resolution is also performed (immediately)

Parameter	Description
	<p>when connection is subsequently "closed" (by timeout or by the remote host) and connections are updated accordingly. In addition, the device periodically (every 15 minutes) performs DNS name resolution to ensure that the list of resolved IP addresses has not changed. If a change is detected, the device updates its' list of IP addresses and re-establishes connections accordingly.</p> <ul style="list-style-type: none"> In addition to multiple HTTP sessions, the device establishes multiple (TCP) connections per session, thereby enhancing data exchange capabilities with the host.
Port <code>rest-port</code> [HTTPRemoteHosts_Port]	Defines the port of the host. The valid value is 0 to 65535. The default is 80.
Interface <code>rest-interface</code> [HTTPRemoteHosts_Interface]	Assigns one of the device's IP network interfaces through which communication with the remote host is done. By default, no value is defined and the OAMP interface is used.
Transport Type <code>rest-transport-type</code> [HTTPRemoteHosts_HTTPTransportType]	Defines the protocol for communicating with the remote host: <ul style="list-style-type: none"> [0] HTTP (default) [1] HTTPS
Status <code>http-host-state</code>	(Read-only) Displays the status of the connection with the remote host. <ul style="list-style-type: none"> "Connected": The hosts is connected. "Disconnected": The host is disconnected. "Not In Service": Configuration of the host is invalid.

17.6.2 Enabling Topology Status Services

The following procedure describes how to enable Topology Status for Web-based services. For more information on Topology Status services, see "Configuring Remote Web Services" on page 259.

➤ To enable Topology Status services:

- Open the Web Service Settings page (**Setup** menu > **IP Network** tab > **Web Services** folder > **Web Service Settings**).
- From the 'Topology Status' drop-down list (RoutingServerGroupStatus), select **Enable**:

Figure 17-45: Enabling Topology Status Web-based Service



- Click **Apply**.

17.6.3 Centralized Third-Party Routing Server

You can employ a remote, third-party Routing server to handle call routing decisions in deployments consisting of multiple AudioCodes devices. Employing a Routing server replaces the need for the device's routing tables (IP-to-IP Routing table) to determine call destination.

When the device receives an incoming call (SIP INVITE, NOTIFY or MESSAGE), it searches the IP-to-IP Routing table for a matching routing rule that is also configured to use a Routing server. If found, the device requests the Routing server for an appropriate destination. The request is sent to the Routing server using an HTTP Get Route message. The request contains information about the call (SIP message).

The Routing server uses its own algorithms and logic in determining the best route path. The Routing server manages the call route between devices in "hops", which may be spread over different geographical locations. The destination to each hop (device) can be by IP address (with port) or IP Group. If the destination is an IP address, even though the destination type (in the IP-to-IP Routing table) is an IP Group, the device only uses the IP Group for profiling (i.e., associated IP Profile etc.). If multiple devices exist in the call routing path, the Routing server sends the IP address only to the last device ("node") in the path.

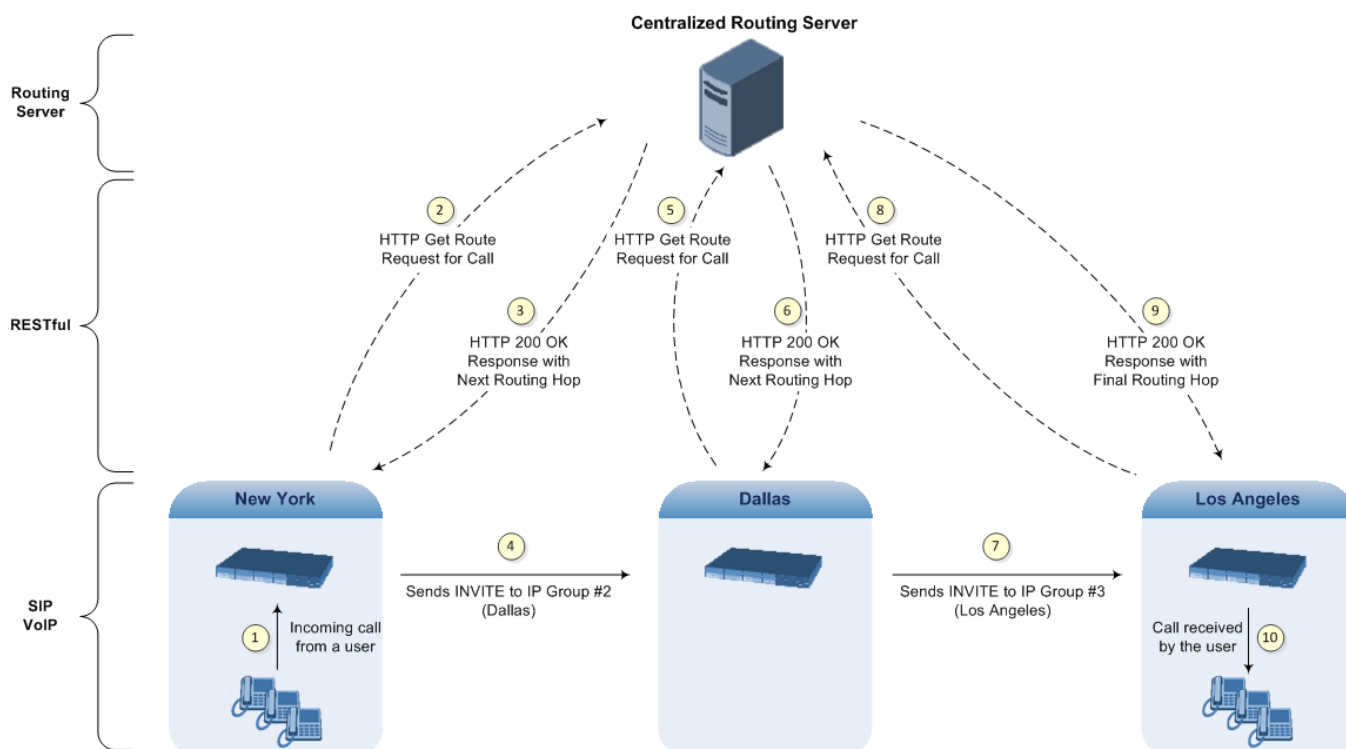
Once the device receives the resultant destination hop from the Routing server, it sends the call to that destination. The Routing server can provide the device with an appropriate route or reject the call. However, if for the **initial** request (first sent Get Route request for the call) the Routing server cannot find an appropriate route for the call or it does not respond, for example, due to connectivity loss (i.e., the Routing server sends an HTTP 404 "Not Found" message), the device routes the call using its routing tables. If the Get Route request is not the first one sent for the call (e.g., in call forwarding or alternative routing) and the Routing server responds with an HTTP 404 "Not Found" message, the device rejects the call.

This HTTP request-response transaction for the routing path occurs between Routing server and each device in the route path (hops) as the call traverses the devices to its final destination. Each device in the call path connects to the Routing server, which responds with the next hop in the route path. Each device considers the call as an incoming call from an IP Group. The session ID (SID) is generated by the first device in the path and then passed unchanged down the route path, enabling the Routing server to uniquely identify requests belonging to the same call session.

Communication between the device and the Routing server is through the device's embedded Representational State Transfer (RESTful) API. The RESTful API is used to manage the routing-related information exchanged between the Routing server (RESTful server) and the device (RESTful client). When you have configured the device with connection settings of the Routing sever and the device starts-up, it connects to the Routing server and activates the RESTful API, which triggers the routing-related API commands.

The following figure provides an example of information exchange between devices and a Routing server for routing calls:

Figure 17-46: Example of Call Routing Information Exchange between Devices and Routing Server



The Routing server can also manipulate call data such as calling name, if required. It can also create new IP Groups and associated configuration entities, if necessary for routing. Multiple Routing servers can also be employed, whereby each device in the chain path can use a specific Routing server. Alternatively, a single Routing server can be employed and used for all devices ("stateful" Routing server).

The device automatically updates (sends) the Routing server with its' configuration topology regarding SIP routing-related entities (SRDs, SIP Interfaces, and IP Groups) that have been configured for use by the Routing server. For example, if you add a new IP Group and enable it for use by the Routing server, the device sends this information to the Routing server. Routing of calls associated with routing-related entities that are disabled for use by the Routing server (default) are handled only by the device (not the Routing server).

In addition to regular routing, the Routing server also supports the following:

- Alternative Routing:** If a call fails to be established, the device "closest" to the failure and configured to send "additional" routing requests (through REST API - "additionalRoute" attribute in HTTP Get Route request) to the Routing server, sends a new routing request to the Routing server. The Routing server may respond with a new route destination, thereby implementing alternative routing. Alternatively, it may enable the device to return a failure response to the previous device in the route path chain and respond with an alternative route to this device. Therefore, alternative routing can be implemented at any point in the route path. If the Routing server sends an HTTP 404 "Not Found" message for an alternative route request, the device rejects the call. If the Routing server is configured to handle alternative routing, the device does not make any alternative routing decisions based on its alternative routing tables.
- Call Status:** The device can report call status to the Routing server to indicate whether a call has successfully been established and/or failed (disconnected). The device can also report when an IP Group (Proxy Set) is unavailable, detected by the keep-alive mechanism, or when the CAC thresholds permitted per IP Group have

been crossed.

- **Credentials for Authentication:** The Routing Server can provide user (e.g., IP Phone caller) credentials (username-password) in the Get Route response, which can be used by the device to authenticate outbound SIP requests if challenged by the outbound peer, for example, Microsoft Skype for Business (per RFC 2617 and RFC 3261). If multiple devices exist in the call routing path, the Routing server sends the credentials only to the last device ("node") in the path.

➤ **To configure routing based on Routing server:**

1. For each configuration entity (e.g., IP Group) that you want routing done by the Routing server, configure the entity's 'Used By Routing Server' parameter to **Used**:

Figure 17-47: Configuring Entity to Use Routing Server

Used By Routing Server

2. Configure an additional Security Administrator user account in the Local Users table (see "Configuring Management User Accounts" on page 60), which is used by the Routing server (REST client) to log in to the device's management interface.
3. Configure the address and connection settings of the Routing server, referred to as a Remote Web Service and HTTP remote host (see "Configuring Remote Web Services" on page 259). You must configure the 'Type' parameter of the Remote Web Service to **Routing**, as shown in the following example:

Figure 17-48: Configuring Remote Web Service for Routing Server

Remote Web Services

GENERAL

Index

Name

Type

4. In the IP-to-IP Routing table, configure the 'Destination Type' parameter of the routing rule to Routing Server (see Configuring SBC IP-to-IP Routing Rules on page 470), as shown below:

Figure 17-49: Configuring Routing Rule to use Routing Server

ACTION

Destination Type

17.7 HTTP-based Proxy Services

The device supports the following HTTP-based proxy services:

- **HTTP Reverse Proxy for Managing Equipment behind NAT:**

You can configure the device to function as a reverse HTTP proxy server. This functionality is required to enable administrators to manage communication equipment (such as IP Phones) over HTTP when the equipment is located behind NAT (e.g., in the LAN) and the administrator is located in a public domain (e.g., in the WAN). Thus,

this functionality resolves NAT issues, enabling the administrator to access the IP Phone's management interface (e.g., embedded Web server).

To support the functionality, the following configuration is required:

1. Enable the HTTP Proxy application (see "Enabling the HTTP Proxy Application" on page 269).
2. Define a local, listening HTTP interface for the leg interfacing with the administrator (see "Configuring HTTP Interfaces" on page 270).



Note: It is recommended **not** to use port 80 as this is the default port used by IP Phones for their Web-based management interface.

3. Define each HTTP-based managed equipment:
 - a. Define the URL prefix for accessing the equipment's management interface (see "Configuring HTTP Proxy Services" on page 272). To access the equipment's management interface, the administrator needs to enter the following URL in a Web browser:
`http://<device's WAN IP address:port>/url prefix/`
 - b. Define the IP address of the managed equipment (see "Configuring HTTP Proxy Hosts" on page 273).



Note: For this feature, no special configuration is required on the managed equipment.

■ HTTP-based EMS Services for AudioCodes Equipment behind NAT:

You can configure the device to act as an HTTP Proxy that enables AudioCodes EMS to manage AudioCodes equipment (such as IP Phones) over HTTP when the equipment is located behind NAT (e.g., in the LAN) and EMS is located in a public domain (e.g., in the WAN). Thus, the feature resolves NAT traversal issues. The IP Phones register with the device in order to allow communication between the IP Phones and the EMS.

To support the functionality, the following configuration is required:

1. Enable the HTTP Proxy application (see "Enabling the HTTP Proxy Application" on page 269).
2. Configure two local, listening HTTP interfaces - one for the EMS and one for the IP Phones (see "Configuring HTTP Interfaces" on page 270).
3. Configure the address of the EMS server (see "Configuring an HTTP-based EMS Service" on page 275).

17.7.1 Enabling the HTTP Proxy Application

Before you can configure HTTP-based proxy services, you must enable the HTTP Proxy application, as described in the following procedure. Once enabled, the Web interface displays menus in the Navigation pane that are relevant to the HTTP Proxy application.

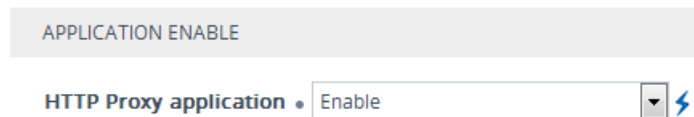


Note: The HTTP Proxy application is a license-dependent feature and is available only if it is included in the License Key installed on the device. For ordering the feature, please contact your AudioCodes sales representative. For installing a new License Key, see License Key on page 597.

➤ **To enable the HTTP Proxy application:**

1. Open the General Settings page (**Setup** menu > **IP Network** tab > **HTTP Proxy** folder > **General Settings**).

Figure 17-50: Enabling HTTP Proxy Application



2. From the 'HTTP Proxy Application' drop-down list, select **Enable**.
3. Click **Apply**, and then reset the device with a save-to-flash for your settings to take effect.

17.7.2 Configuring HTTP Interfaces

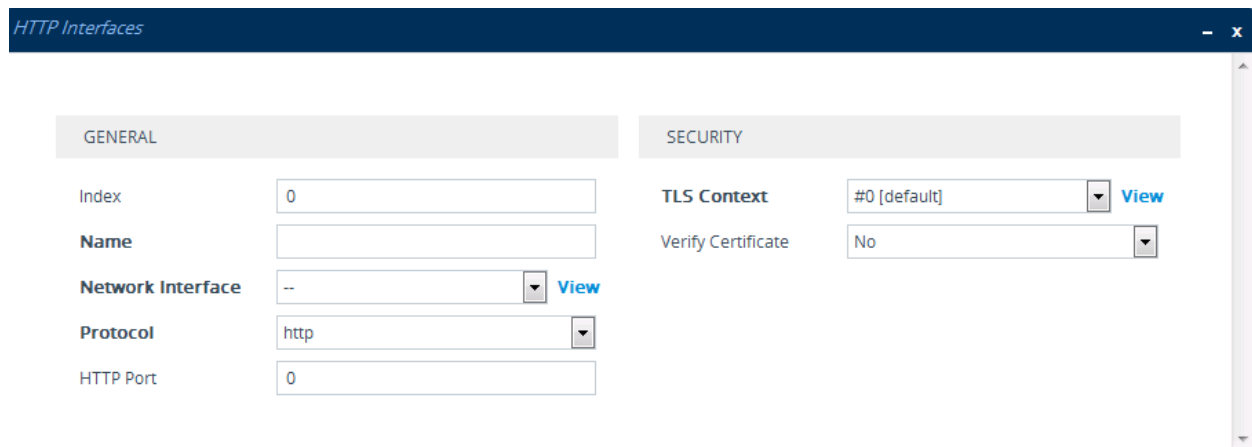
The HTTP Interfaces table lets you configure up to 10 HTTP Interfaces. An HTTP Interface represents a local, listening interface for receiving HTTP/S requests from HTTP-based (Web) clients such as managed equipment (e.g., IP Phones) and/or AudioCodes EMS management tool for HTTP/S-based services.

The following procedure describes how to configure HTTP Interfaces through the Web interface. You can also configure it through ini file (HTTPInterface) or CLI (configure network > http-proxy http-interface).

➤ **To configure an HTTP Interface:**

1. Open the HTTP Interfaces table (**Setup** menu > **IP Network** tab > **HTTP Proxy** folder > **HTTP Interfaces**).
2. Click **New**; the following dialog box appears:

Figure 17-51: HTTP Interfaces Table - Add Dialog Box



3. Configure an HTTP Interface according to the parameters described in the table below.

4. Click **Apply**, and then save your settings to flash memory.

Table 17-20: HTTP Interfaces Table Parameter Descriptions

Parameter	Description
General	
Index [HTTPInterface_Index]	Defines an index number for the new table row. Note: <ul style="list-style-type: none"> ▪ Each row must be configured with a unique index. ▪ The parameter is mandatory.
Name interface-name [HTTPInterface_InterfaceName]	Defines an arbitrary name to easily identify the row. The valid value is a string of up to 40 characters. By default, no value is defined. Note: <ul style="list-style-type: none"> ▪ Each row must be configured with a unique name. ▪ The parameter is mandatory.
Network Interface network-interface [HTTPInterface_NetworkInterface]	Assigns a local, network interface to the HTTP interface. By default, no value is defined. To configure network interfaces, see "Configuring IP Network Interfaces" on page 130. Note: The parameter is mandatory.
Protocol protocol [HTTPInterface_Protocol]	Defines the protocol type. <ul style="list-style-type: none"> ▪ [0] HTTP (default) ▪ [1] HTTPS
HTTP Port http-port [HTTPInterface_Port]	Defines the local, listening HTTP port. The valid value is 0 to 65534. The default is 0. Note: The parameter is mandatory.
Security	
TLS Context tls-context [HTTPInterface_TLSContext]	Assigns a TLS Context for the connection with the HTTP Proxy service. By default, the default TLS Context (Index 0) is assigned. To configure TLS Contexts, see "Configuring TLS Certificate Contexts" on page 99. Note: The parameter is applicable only if the connection protocol is HTTPS (defined using the 'Protocol' parameter, above).
Verify Certificate verify-cert [HTTPInterface_VerifyCert]	Enables TLS certificate verification when the connection with the proxy service is based on HTTPS. <ul style="list-style-type: none"> ▪ [0] No = (Default) No certificate verification is done. ▪ [1] Yes = The device verifies the authentication of the certificate received from the HTTPS peer. The device authenticates the certificate against the trusted root certificate store associated with the associated TLS Context (see 'TLS Context' parameter above) and if ok, allows communication with the HTTPS peer. If authentication fails, the device denies communication (i.e., handshake fails). The device can also authenticate the certificate by querying with an Online Certificate Status Protocol (OCSP) server whether the certificate has been revoked. This is also configured for the

Parameter	Description
	associated TLS Context. Note: The parameter is applicable only if the connection protocol is HTTPS (defined using the 'Protocol' parameter, above).

17.7.3 Configuring HTTP Proxy Services

The HTTP Proxy Services table lets you configure up to 10 HTTP Proxy Services.

The following procedure describes how to configure HTTP Proxy Services through the Web interface. You can also configure it through ini file (HTTPProxyService) or CLI (configure network > http-proxy http-proxy-serv).

➤ **To configure an HTTP Proxy Service:**

1. Open the HTTP Proxy Services table (**Setup** menu > **IP Network** tab > **HTTP Proxy** folder > **HTTP Proxy Services**).
2. Click **New**; the following dialog box appears:

Figure 17-52: HTTP Proxy Services Table - Add Dialog Box

3. Configure an HTTP Proxy service according to the parameters described in the table below.
4. Click **Apply**, and then save your settings to flash memory.

Table 17-21: HTTP Proxy Services Table Parameter Descriptions

Parameter	Description
Index [HTTPProxyService_Index]	Defines an index number for the new table row. Note: <ul style="list-style-type: none"> ▪ Each row must be configured with a unique index. ▪ The parameter is mandatory.
Name service-name [HTTPProxyService_ServiceName]	Defines an arbitrary name to easily identify the row. The valid value is a string of up to 40 characters. By default, no value is defined. Note: <ul style="list-style-type: none"> ▪ Each row must be configured with a unique name. ▪ The parameter is mandatory.

Parameter	Description
Listening Interface listening-int [HTTPProxyService_ListeningInterface]	Assigns an HTTP Interface to the HTTP Proxy service. To configure HTTP Interfaces, see "Configuring HTTP Interfaces" on page 270. Note: The parameter is mandatory.
URL Prefix url-prefix [HTTPProxyService_URLPrefix]	Defines the URL prefix that is used to access the managed equipment's embedded Web server. The URL prefix is matched against the target of the HTTP requests sent by the client (such as GET and POST). If a match is located in the table, the device removes the prefix from the request and then forwards the HTTP request to the managed equipment without the prefix. For example, for the URL of GET /home/index.html HTTP/1.1 (which is part of the URL http://10.20.30.40/home/index.html), a URL prefix of "/home" can be configured. To match all URLs, configure the parameter to "/" (default).
Keep-Alive Mode keep-alive-mode [HTTPProxyService_KeepAliveMode]	Enables a keep-alive mechanism with the managed equipment: <ul style="list-style-type: none"> ▪ [0] Disable ▪ [1] Options = (Default) Enables keep-alive by sending HTTP OPTIONS messages. If no response is received from the HTTP host, the device stops forwarding HTTP requests to the host and raises an SNMP alarm (acHTTPProxyServiceAlarm). If you configured the address of the host as an FQDN (see "Configuring HTTP Proxy Hosts" on page 273) and the DNS resolution results in multiple IP addresses, when no response is received from the keep-alive, the device checks connectivity with the next resolved IP address and so on, until a response is received.

17.7.3.1 Configuring HTTP Proxy Hosts

The HTTP Proxy Hosts table lets you configure HTTP Proxy hosts for HTTP Proxy services. An HTTP Proxy Host represents the HTTP-based managed equipment (e.g., IP Phone). The table is a "child" of the HTTP Proxy Services table (see "Configuring HTTP Proxy Services" on page 272). You can configure up to 50 HTTP Proxy hosts; up to 5 HTTP Proxy hosts per HTTP Proxy Service.

The following procedure describes how to configure HTTP Remote hosts through the Web interface. You can also configure it through ini file (HTTPProxyHost) or CLI (configure network > http-proxy http-proxy-host).

➤ **To configure an HTTP Proxy Host:**

1. Open the HTTP Proxy Services table (**Setup** menu > **IP Network** tab > **HTTP Proxy** folder > **HTTP Proxy Services**).
2. In the table, select the required HTTP Proxy Service index row, and then click the **HTTP Proxy Hosts** link located below the table; the HTTP Proxy Hosts table appears.

- Click **New**; the following dialog box appears:

Figure 17-53: HTTP Proxy Hosts Table - Add Dialog Box

- Configure an HTTP Proxy Host according to the parameters described in the table below.
- Click **Apply**, and then save your settings to flash memory.

Table 17-22: HTTP Proxy Hosts Table Parameter Descriptions

Parameter	Description
General	
Index	Defines an index number for the new table row. Note: <ul style="list-style-type: none"> Each row must be configured with a unique index. The parameter is mandatory.
Network Interface <code>network-interface</code> [HTTPProxyHost_NetworkInterface]	Assigns a local, network interface to the HTTP Proxy Host. By default, no value is defined. To configure network interfaces, see "Configuring IP Network Interfaces" on page 130. Note: The parameter is mandatory.
Proxy Address <code>proxy-address</code> [HTTPProxyHost_IpAddress]	Defines the address of the managed equipment (host). The valid value is an IP address in dotted-decimal notation or an FQDN (up to 100 characters). If the address is an FQDN, the device uses DNS to resolve it into an IP address. If the DNS resolution results in multiple IP addresses, the device uses the first available address (i.e., that responds to the keep-alive).
Protocol <code>protocol</code> [HTTPProxyHost_Protocol]	Defines the protocol type. <ul style="list-style-type: none"> [0] HTTP (default) [1] HTTPS
HTTP Port <code>http-port</code> [HTTPProxyHost_Port]	Defines the port of the managed equipment. The default is 0. Note: The parameter is mandatory.
Security	
TLS Context	Assigns a TLS Context for the TLS connection with the HTTP

Parameter	Description
tls-context [HTTPProxyHost_TLSContext]	Proxy host. By default, the default TLS Context (Index 0) is assigned. To configure TLS Contexts, see "Configuring TLS Certificate Contexts" on page 99. Note: The parameter is applicable only if the connection protocol is HTTPS (defined using the 'Protocol' parameter, above).
Verify Certificate verify-cert [HTTPProxyHost_VerifyCert]	Enables TLS certificate verification when the connection with the host is based on HTTPS. <ul style="list-style-type: none"> ▪ [0] No = No certificate verification is done. ▪ [1] Yes = (Default) The device verifies the authentication of the certificate received from the HTTPS peer. The device authenticates the certificate against the trusted root certificate store associated with the associated TLS Context (see 'TLS Context' parameter above) and if ok, allows communication with the HTTPS peer. If authentication fails, the device denies communication (i.e., handshake fails). The device can also authenticate the certificate by querying with an Online Certificate Status Protocol (OCSP) server whether the certificate has been revoked. This is also configured for the associated TLS Context. Note: The parameter is applicable only if the connection protocol is HTTPS (defined using the 'Protocol' parameter, above).

17.7.4 Configuring an HTTP-based EMS Service

The EMS Services table lets you configure a single HTTP-based EMS service. For more information on the EMS service, see "HTTP-based Proxy Services" on page 268.

The following procedure describes how to configure an EMS Service through the Web interface. You can also configure it through ini file (EMSService) or CLI (configure network > http-proxy ems-serv).

➤ **To configure an EMS Service:**

1. Open the EMS Services table (**Setup** menu > **IP Network** tab > **HTTP Proxy** folder > **EMS Services**).

- Click **New**; the following dialog box appears:

Figure 17-54: EMS Services Table - Add Dialog Box

- Configure an EMS Service according to the parameters described in the table below.
- Click **Apply**, and then save your settings to flash memory.

Table 17-23: EMS Services Table Parameter Descriptions

Parameter	Description
Index [EMSService_Index]	Defines an index number for the new table row. Note: <ul style="list-style-type: none"> Each row must be configured with a unique index. The parameter is mandatory.
Name service-name [EMSService_ServiceName]	Defines an arbitrary name to easily identify the row. The valid value is a string of up to 40 characters. By default, no value is defined. Note: <ul style="list-style-type: none"> Each row must be configured with a unique name. The parameter is mandatory.
EMS Primary Server primary-server [EMSService_PrimaryServer]	Defines the address of the primary EMS server. Note: The parameter is mandatory.
EMS Secondary Server secondary-server [EMSService_SecondaryServer]	Defines the address of the secondary EMS server.
Listening Interface to devices dev-login-int [EMSService_DeviceLoginInterface]	Assigns an HTTP Interface (local, listening HTTP interface:port) for communication with the client. To configure HTTP Interfaces, see "Configuring HTTP Interfaces" on page 270. By default, no value is defined. Note: The parameter is mandatory.
Listening to EMS Interface ems-int [EMSService_EMSServiceInterface]	Assigns an HTTP Interface (local, listening HTTP interface:port) for communication with the EMS. To configure HTTP Interfaces, see "Configuring HTTP Interfaces" on page 270. By default, no value is defined.

Parameter	Description
	Note: The parameter is mandatory.

17.8 E9-1-1 Support for Microsoft Skype for Business

The Enhanced 9-1-1 (E9-1-1) service is becoming the mandatory emergency service required in many countries around the world. The E9-1-1 service, based on its predecessor 911, enables emergency operators to pinpoint the location (granular location) of callers who dial the 9-1-1 emergency telephone number.

Today, most enterprises implement an IP-based infrastructure providing a VoIP network with fixed and nomadic users, allowing connectivity anywhere with any device. This, together with an often deployed multi-line telephone system (MLTS) poses a challenge for E9-1-1 due to the difficulty in accurately locating the E9-1-1 caller.

This section describes the E9-1-1 solution provided by Microsoft Skype for Business and AudioCodes' device's ELIN interworking capabilities, which provides the SIP Trunk to the E9-1-1 emergency service provider. This section also describes the configuration of the device for interoperating between the Skype for Business environment and the E9-1-1 emergency provider.

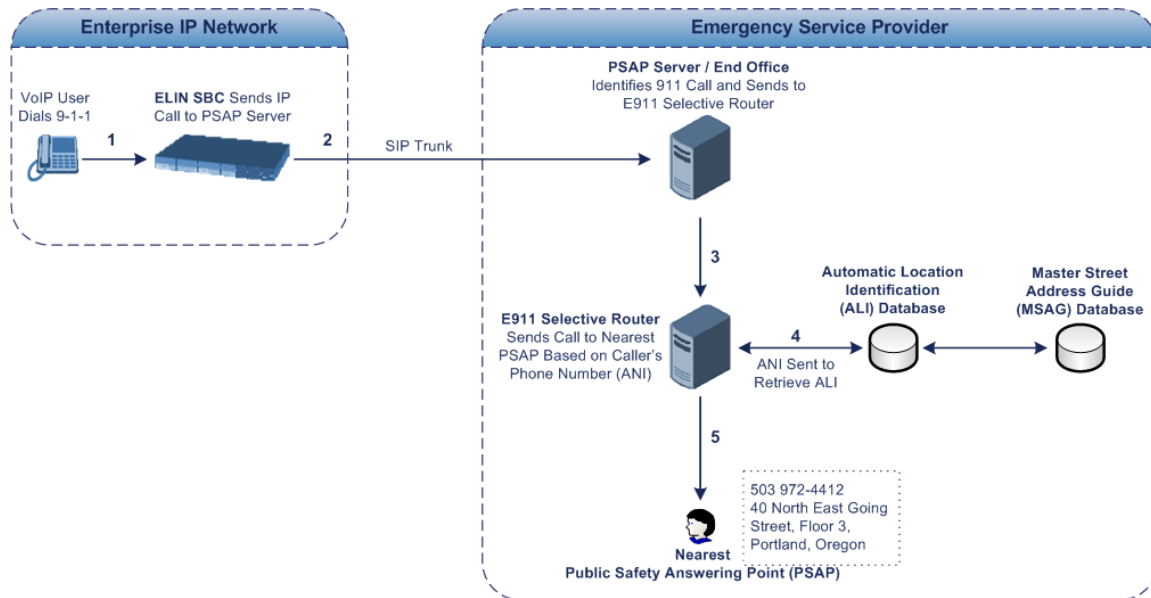


Note: The ELIN feature for E9-1-1 is a license-dependent feature and is available only if it is included in the License Key installed on the device. For ordering the feature, please contact your AudioCodes sales representative. For installing a new License Key, see "License Key" on page 597.

17.8.1 About E9-1-1 Services

E9-1-1 is a national emergency service for many countries, enabling E9-1-1 operators to automatically identify the geographical location and phone number of a 911 caller. In E9-1-1, the 911 caller is routed to the nearest E9-1-1 operator, termed *public safety answering point* (PSAP) based on the location of the caller. Automatic identification of the caller's location and phone number reduces the time spent on requesting this information from the 911 caller. Therefore, the E9-1-1 service enables the PSAP to quickly dispatch the relevant emergency services (for example, fire department or police) to the caller's location. Even if the call prematurely disconnects, the operator has sufficient information to call back the 911 caller.

The figure below illustrates the routing of an E9-1-1 call to the PSAP:



1. The VoIP user dials 9-1-1.
2. AudioCodes' ELIN device eventually sends the call to the emergency service provider over the SIP Trunk (PSAP server).
3. The emergency service provider identifies the call is an emergency call and sends it to an E9-1-1 Selective Router in the Emergency Services provider's network.
4. The E9-1-1 Selective Router determines the geographical location of the caller by requesting this information from an Automatic Location Identification (ALI) database based on the phone number or Automatic Number Identifier (ANI) of the 911 caller. Exact location information is also supplied by the Master Street Address Guide (MSAG) database, which is a companion database to the ALI database. Phone companies and public safety agencies collaborate beforehand to create master maps that match phone numbers, addresses and cross streets to their corresponding PSAP. This MSAG is the official record of valid streets (with exact spelling), street number ranges, and other address elements with which the service providers are required to update their ALI databases.
5. The E9-1-1 Selective Router sends the call to the appropriate PSAP based on the retrieved location information from the ALI.
6. The PSAP operator dispatches the relevant emergency services to the E9-1-1 caller.

17.8.2 Microsoft Skype for Business and E9-1-1

Microsoft Skype for Business enables Enterprise voice users to access its unified communications platform from virtually anywhere and through many different devices. This, together with a deployed MLTS, poses a challenge for E9-1-1 due to the difficulty in accurately locating the E9-1-1 caller. However, Skype for Business offers an innovative solution to solving Enterprises E9-1-1 location problems.

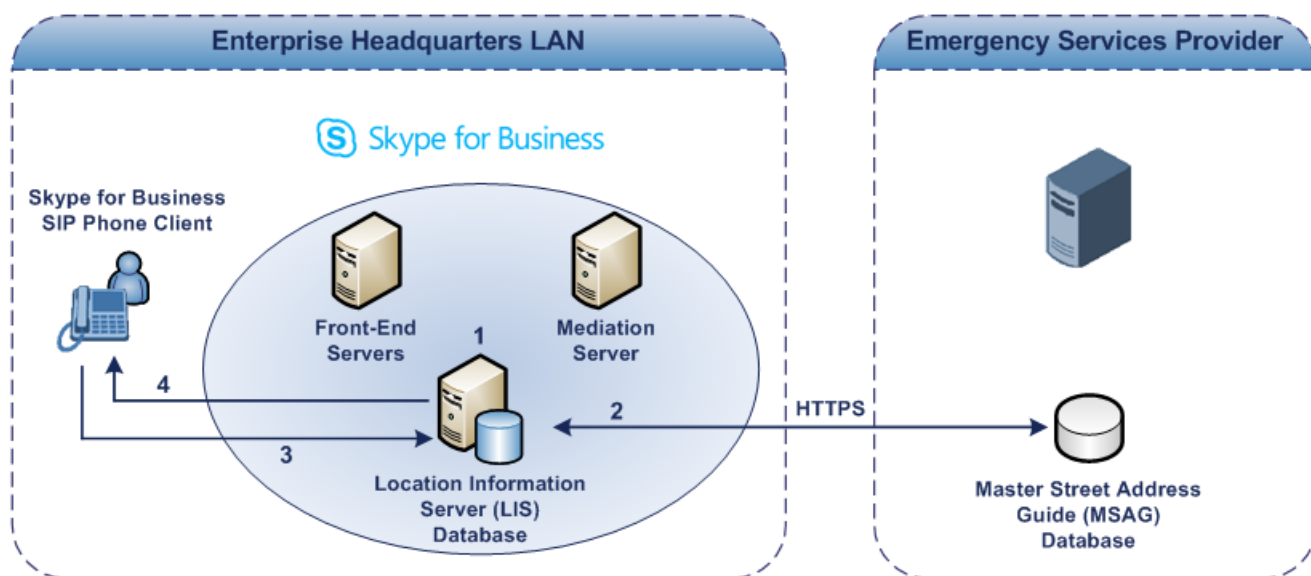
17.8.2.1 Gathering Location Information of Skype for Business Clients for 911 Calls

When a Microsoft® Skype for Business client is enabled for E9-1-1, the location data that is stored on the client is sent during an emergency call. This stored location information is acquired automatically from the Microsoft Location Information Server (LIS). The LIS stores the location of each network element in the enterprise. Immediately after the Skype for Business client registration process or when the operating system detects a network

connection change, each Skype for Business client submits a request to the LIS for a location. If the LIS is able to resolve a location address for the client request, it returns the address in a location response. Each client then caches this information. When the Skype for Business client dials 9-1-1, this location information is then included as part of the emergency call and used by the emergency service provider to route the call to the correct PSAP.

The gathering of location information in the Skype for Business network is illustrated in the figure below:

Figure 17-55: Microsoft Skype for Business Client Acquiring Location Information



1. The Administrator provisions the LIS database with the location of each network element in the Enterprise. The location is a civic address, which can include contextual in-building and company information. In other words, it associates a specific network entity (for example, a WAP) with a physical location in the Enterprise (for example, Floor 2, Wing A, and the Enterprise's street address). For more information on populating the LIS database, see "Adding ELINs to the Location Information Server" on page 280.
2. The Administrator validates addresses with the emergency service provider's MSAG – a companion database to the ALI database. This ensures that the civic address is valid as an official address (e.g., correct address spelling).
3. The Skype for Business client initiates a location request to the LIS under the following circumstances:
 - Immediately after startup and registering the user with Skype for Business
 - Approximately every four hours after initial registration
 - Whenever a network connection change is detected (such as roaming to a new WAP)

The Skype for Business client includes in its location request the following known network connectivity information:

- Always included:
 - ◆ IPv4 subnet
 - ◆ Media Access Control (MAC) address
- Depends on network connectivity:
 - ◆ Wireless access point (WAP) Basic Service Set Identifier (BSSID)
 - ◆ Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED)

chassis ID and port ID

For a Skype for Business client that moves inside the corporate network such as a soft phone on a laptop that connects wirelessly to the corporate network, Skype for Business can determine which subnet the phone belongs to or which WAP / SSID is currently serving the soft-client.

4. The LIS queries the published locations for a location and if a match is found, returns the location information to the client. The matching order is as follows:
 - WAP BSSID
 - LLDP switch / port
 - LLDP switch
 - Subnet
 - MAC address

This logic ensures that for any client that is connected by a wireless connection, a match is first attempted based on the hardware address of its connected access point. The logic is for the match to be based on the most detailed location. The subnet generally provides the least detail. If no match is found in the LIS for WAP BSSID, LLDP switch / port, LLDP switch, or subnet, the LIS proxies the MAC address to an integrated Simple Network Management Protocol (SNMP) scanning application. Using SNMP may benefit some organizations for the following reasons:

- LLDP is not supported by Skype for Business so this provides a mechanism for soft phones to acquire detailed location information.
- Installed Layer-2 switches may not support LLDP.

If there is no match and the LIS cannot determine the location, the user may be prompted to manually enter the location. For example, the client may be located in an undefined subnet, at home, in a coffee shop or anywhere else outside the network. When a user manually provides a location, the location is mapped based on the MAC address of the default gateway of the client's network and stored on the client. When the client returns to any previously stored location, the client is automatically set to that location. A user can also manually select any location stored in the local users table and manage existing entries.

17.8.2.2 Adding ELINs to the Location Information Server

As mentioned in the previous section, the administrator needs to populate the Location Information Server (LIS) database with a network wire map, which maps the Enterprise's network elements to civic addresses. Once done, it can automatically locate clients within a network. You can add addresses individually to the LIS or in a batch using a comma-separated value (CSV) file containing the column formats listed in the table below.

Table 17-24: Columns in the LIS Database

Network Element	Columns
Wireless access point	<BSSID>,<Description>,<Location>,<CompanyName>,<HouseNumber>,<HouseNumberSuffix>,<PreDirectional>,...<StreetName>,<StreetSuffix>,<PostDirectional>,<City>,<State>,<PostalCode>,<Country>
Subnet	<Subnet>,<Description>,<Location>,<CompanyName>,<HouseNumber>,<HouseNumberSuffix>,<PreDirectional>,...<StreetName>,<StreetSuffix>,<PostDirectional>,<City>,<State>,<PostalCode>,<Country>
Port	<ChassisID>,<PortIDSubType>,<PortID>,<Description>,<Location>,<CompanyName>,<HouseNumber>,<HouseNumberSuffix>,...<PreDirectional>,<StreetName>,<StreetSuffix>,<PostDirectional>,<City>,<State>,<PostalCode>,<Country>

Network Element	Columns
Switch	<ChassisID>,<Description>,<Location>,<CompanyName>,<HouseNumber>,<House NumberSuffix>,<PreDirectional>,...<StreetName>,<StreetSuffix>,<PostDirectional>,<City>,<State>,<PostalCode>,<Country>

For the ELIN number to be included in the SIP INVITE (XML-based PIDF-LO message) sent by the Mediation Server to the ELIN device, the administrator must add the ELIN number to the <CompanyName> column (shown in the table above in **bold** typeface). As the ELIN device supports up to five ELINs per PIDF-LO, the <CompanyName> column can be populated with up to this number of ELINs, each separated by a semicolon. The digits of each ELIN can be separated by hyphens (xxx-xxx-xxx) or they can be adjacent (xxxxxxxx).

When the ELIN device receives the SIP INVITE, it extracts the ELINs from the NAM field in the PIDF-LO (e.g., <ca:NAM>1111-222-333; 1234567890 </ca:NAM>), which corresponds to the <CompanyName> column of the LIS.

If you do not populate the location database, and the Skype for Business location policy, Location Required is set to **Yes** or **Disclaimer**, the user will be prompted to enter a location manually.

17.8.2.3 Passing Location Information to the PSTN Emergency Provider

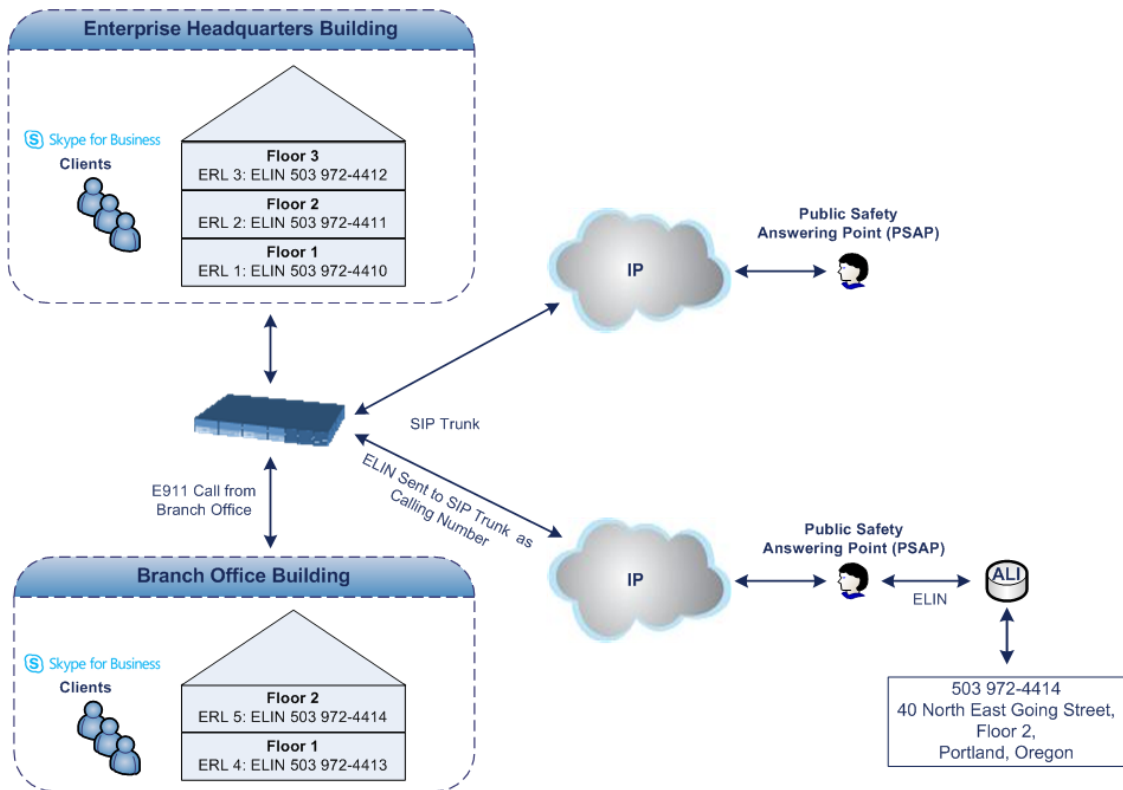
When a Skype for Business client, enabled for E9-1-1 emergency services, dials 9-1-1, the location data and callback information stored on the client is sent with the call through the Mediation Server to a SIP Trunk-based emergency service provider. The emergency service provider then routes the call to the nearest and most appropriate PSAP based on the location information contained within the call.

Skype for Business passes the location information of the Skype for Business client in an IETF-standard format - Presence Information Data Format - Location Object (PIDF-LO)—in a SIP INVITE message. However, this content cannot be sent on the SIP Trunks since they do not support such a content. To overcome this, Enterprises deploying the device can divide their office space into Emergency Response Locations (ERLs) and assign a dedicated Emergency Location Identification Number (ELIN) to each ERL (or zone). When Skype for Business sends a SIP INVITE message with the PIDF-LO to the device, it can parse the content and translate the calling number to an appropriate ELIN. The device then sends the call to the SIP Trunk with the ELIN number as the calling number. The ELIN number is sent to the emergency service provider, which sends it on to the appropriate PSAP according to the ELIN address match in the ALI database lookup.

The ERL defines a specific location at a street address, for example, the floor number of the building at that address. The geographical size of an ERL is according to local or national regulations (for example, less than 7000 square feet per ERL). Typically, you would have an ERL for each floor of the building. The ELIN is used as the phone number for 911 callers within this ERL.

The figure below illustrates the use of ERLs and ELINs, with an E9-1-1 call from floor 2 at the branch office:

Figure 17-56: ERLs and ELINs for E9-1-1 in Skype for Business



The table below shows an example of designating ERLs to physical areas (floors) in a building and associating each ERL with a unique ELIN.

Table 17-25: Designating ERLs and Assigning to ELINs

ERL Number	Physical Area	IP Address	ELIN
1	Floor 1	10.13.124.xxx	503 972-4410
2	Floor 2	10.15.xxx.xxx	503 972-4411
3	Floor 3	10.18.xxx.xxx	503 972-4412

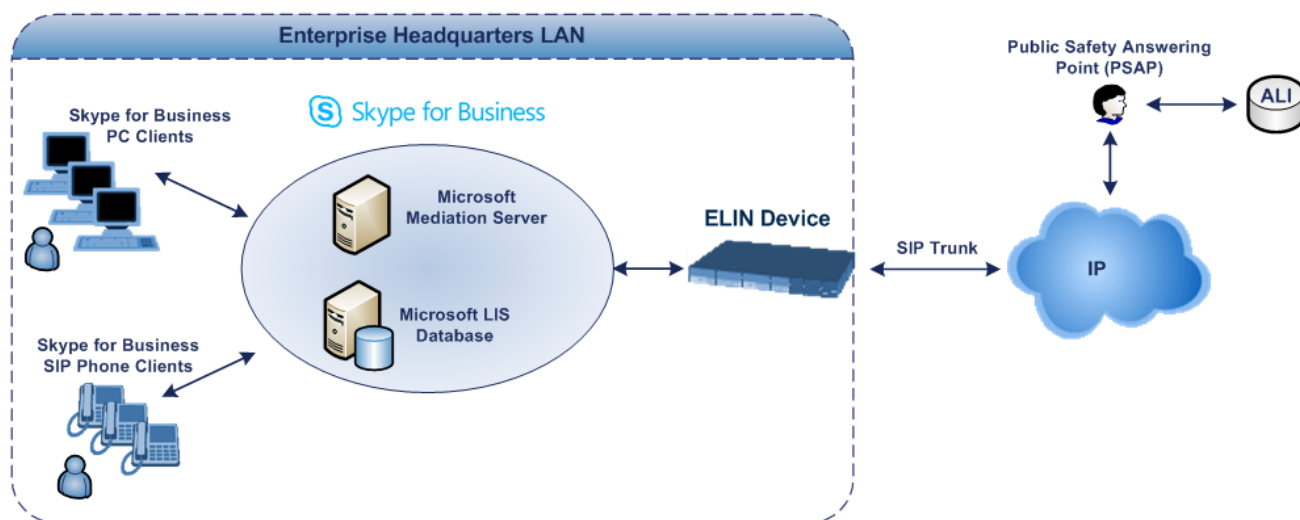
In the table above, a unique IP subnet is associated per ERL. This is useful if you implement different subnets between floors. Therefore, IP phones, for example, on a specific floor are in the same subnet and therefore, use the same ELIN when dialing 9-1-1.

17.8.3 AudioCodes ELIN Device for Skype for Business E9-1-1 Calls to PSTN

Microsoft Mediation Server sends the location information of the E9-1-1 caller in the XML-based PIDF-LO body contained in the SIP INVITE message. However, this content cannot be sent on the SIP Trunk since they do not support such content. To solve this issue, Skype for Business requires a device (*ELIN SBC*) to send the E9-1-1 call to the SIP Trunk. When Skype for Business sends the PIDF-LO to the device, it parses the content and translates the calling number to an appropriate ELIN. This ensures that the call is routed to an appropriate PSAP, based on ELIN-address match lookup in the emergency service provider's ALI database.

The figure below illustrates an AudioCodes ELIN device deployed in the Skype for Business environment for handling E9-1-1 calls between the Enterprise and the emergency service provider.

Figure 17-57: ELIN SBC for E9-1-1 in Skype for Business Environment



17.8.3.1 Detecting and Handling E9-1-1 Calls

The ELIN device identifies E9-1-1 calls and translates their incoming E9-1-1 calling numbers into ELIN numbers, sent toward the PSAP. The device handles the received E9-1-1 calls as follows:

1. The device identifies E9-1-1 calls if the incoming SIP INVITE message contains a PIDF-LO XML message body. This is indicated in the SIP *Content-Type* header, as shown below:

```
Content-Type: application/pdf+xml
```

2. The device extracts the ELIN number(s) from the "NAM" field in the XML message. The "NAM" field corresponds to the <CompanyName> column in the Location Information Server (LIS). The device supports up to five ELIN numbers per XML message. The ELINs are separated by a semicolon. The digits of the ELIN number can be separated by hyphens (xxx-xxx-xxx) or they can be adjacent (xxxxxxxxx), as shown below:

```
<ca:NAM>1111-222-333; 1234567890 </ca:NAM>
```

3. The device saves the *From* header value of the SIP INVITE message in its ELIN database table (**Call From** column). The ELIN table is used for PSAP callback, as discussed later in "PSAP Callback to Skype for Business Clients for Dropped E9-1-1 Calls" on page 285. The ELIN table also stores the following information:
 - **ELIN:** ELIN number
 - **Time:** Time at which the original E9-1-1 call was terminated with the PSAP
 - **Count:** Number of E9-1-1 calls currently using the ELIN

An example of the ELIN database table is shown below:

ELIN	Time	Count	Index	Call From
4257275678	22:11:52	0	2	4258359333
4257275999	22:11:57	0	3	4258359444

ELIN	Time	Count	Index	Call From
4257275615	22:12:03	0	0	4258359555
4257275616	22:11:45	0	1	4258359777

The ELIN table stores this information for a user-defined period (see "Configuring the E9-1-1 Callback Timeout" on page 287), starting from when the E9-1-1 call, established with the PSAP, terminates. After this time expires, the table entry with its ELIN is disregarded and no longer used (for PSAP callback). Therefore, table entries of only the most recently terminated E9-1-1 callers are considered in the ELIN table. The maximum entries in the ELIN table is 300.

- The device uses the ELIN number as the E9-1-1 calling number and sends it in the SIP INVITE message (as an ANI / Calling Party Number) to the SIP Trunk.

An example of a SIP INVITE message received from an E9-1-1 caller is shown below. The SIP *Content-Type* header indicating the PIDF-LO, and the NAM field listing the ELINs are shown in **bold** typeface.

```
INVITE sip:911;phone-context=Redmond@192.168.1.12;user=phone
SIP/2.0
From:
"voip_911_user1"<sip:voip_911_user1@contoso.com>;epid=1D19090AED;t
ag=d04d65d924
To: <sip:911;phone-context=Redmond@192.168.1.12;user=phone>
CSeq: 8 INVITE
Call-ID: e6828be1-1cdd-4fb0-bdda-cda7faf46df4
VIA: SIP/2.0/TLS 192.168.0.244:57918;branch=z9hG4bK528b7ad7
CONTACT:
<sip:voip_911_user1@contoso.com;opaque=user:epid:R4bCDaUj51a06PUbk
raS0QAA;gruu>;text;audio;video;image
PRIORITY: emergency
CONTENT-TYPE: multipart/mixed; boundary= -----
=_NextPart_000_4A6D_01CAB3D6.7519F890
geolocation: <cid:voip_911_user1@contoso.com>;inserted-
by="sip:voip_911_user1@contoso .com"
Message-Body:
-----=_NextPart_000_4A6D_01CAB3D6.7519F890
Content-Type: application/sdp ; charset=utf-8
v=0
o=- 0 0 IN IP4 Client
s=session
c=IN IP4 Client
t=0 0
m=audio 30684 RTP/AVP 114 111 112 115 116 4 3 8 0 106 97
c=IN IP4 172.29.105.23
a=rtcp:60423
a=label:Audio
a=rtpmap:3 GSM/8000/1
a=rtpmap:101 telephone-event/8000
a=fmtp:101 0-16
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=ptime:20
-----=_NextPart_000_4A6D_01CAB3D6.7519F890
Content-Type: application/pidf+xml
Content-ID: <voip_911_user1@contoso.com>
<?xml version="1.0" encoding="utf-8"?>
```

```

<presence xmlns="urn:ietf:params:xml:ns:pidf"
xmlns:gp="urn:ietf:params:xml:ns:pidf:geopriv10"
xmlns:bp="urn:ietf:params:xml:ns:pidf:geopriv10:basicPolicy"
xmlns:ca="urn:ietf:params:xml:ns:pidf:geopriv10:civicAddr"
xmlns:ms="urn:schema:Rtc.LIS.msftE911PidfExtn.2008"
entity="sip:voip_911_user1@contoso.com"><tuple
id="0"><status><gp:geopriv><gp:location-
info><ca:civicAddress><ca:country>US</ca:country><ca:A1>WA</ca:A1>
<ca:A3>Redmond</ca:A3><ca:RD>163rd</ca:RD><ca:STS>Ave</ca:STS><ca:
POD>NE</ca:POD><ca:HNO>3910</ca:HNO><ca:LOC>40/4451</ca:LOC>
<ca:NAM>1111-222-333; 1234567890 </ca:NAM>
<ca:PC>98052</ca:PC></ca:civicAddress></gp:location-
info><gp:usage-rules><bp:retransmission-
allowed>true</bp:retransmission-allowed></gp:usage-
rules></gp:geopriv><ms:msftE911PidfExtn><ms:ConferenceUri>sip:+142
55550199@contoso.com;user=phone</ms:ConferenceUri><ms:ConferenceMo
de>twoway</ms:ConferenceMode><LocationPolicyTagID
xmlns="urn:schema:Rtc.Lis.LocationPolicyTagID.2008">user-
tagid</LocationPolicyTagID
></ms:msftE911PidfExtn></status><timestamp>1991-09-
22T13:37:31.03</timestamp></tuple></presence>
-----_NextPart_000_4A6D_01CAB3D6.7519F890--

```

17.8.3.2 Pre-empting Existing Calls for E9-1-1 Calls

If the ELIN device receives an E9-1-1 call from the IP network and there are unavailable channels (for example, all busy), the device immediately terminates one of the non-E9-1-1 calls (arbitrary) and accepts the E9-1-1 call on the freed channel:

- The preemption is done only on a call pertaining to the same source IP Group from which the E9-1-1 call is received, or the same destination IP Group (i.e., PSAP Server).

This feature is initiated only if the received SIP INVITE message contains a *Priority* header set to "emergency", as shown below:

```
PRIORITY: emergency
```

17.8.3.3 PSAP Callback to Skype for Business Clients for Dropped E9-1-1 Calls

As the E9-1-1 service automatically provides all the contact information of the E9-1-1 caller to the PSAP, the PSAP operator can call back the E9-1-1 caller. This is especially useful in cases where the caller disconnects prematurely. However, as the Enterprise sends ELINs to the PSAP for E9-1-1 calls, a callback can only reach the original E9-1-1 caller using the device to translate the ELIN number back into the E9-1-1 caller's extension number.

In the ELIN table of the device, the temporarily stored *From* header value of the SIP INVITE message originally received from the E9-1-1 caller is used for PSAP callback. When the PSAP makes a callback to the E9-1-1 caller, the device translates the called number (i.e., ELIN) received from the PSAP to the corresponding E9-1-1 caller's extension number as matched in the ELIN table.

The handling of PSAP callbacks by the device is as follows:

1. When the device receives a call from the emergency service provider, it searches the ELIN table for an ELIN that corresponds to the received called party number in the incoming message.
2. If a match is found in the ELIN table, it routes the call to the Mediation Sever by sending a SIP INVITE, where the values of the *To* and *Request-URI* are taken from the value of the original *From* header that is stored in the ELIN table (in the **Call From** column).

3. The device updates the Time in the ELIN table. (The Count is not affected).

The PSAP callback can be done only within a user-defined period (see "Configuring the E9-1-1 Callback Timeout" on page 287), started from after the original E9-1-1 call established with the PSAP is terminated. After this time expires, the table entry with its ELIN is disregarded and no longer used (for PSAP callback). Therefore, table entries of only the most recently terminated E9-1-1 callers are considered in the ELIN table. If the PSAP callback is done after this timeout expires, the device is unable to route the call to the E9-1-1 caller and instead, either sends it as a regular call or most likely, rejects it if there are no matching routing rules. However, if another E9-1-1 caller has subsequently been processed with the same ELIN number, the PSAP callback is routed to this new E9-1-1 caller.

In scenarios where the same ELIN number is used by multiple E9-1-1 callers, upon receipt of a PSAP callback, the device sends the call to the most recent E9-1-1 caller. For example, if the ELIN number "4257275678" is being used by three E9-1-1 callers, as shown in the table below, then when a PSAP callback is received, the device sends it to the E9-1-1 caller with phone number "4258359555".

Table 17-26: Choosing Caller of ELIN

ELIN	Time	Call From
4257275678	11:00	4258359333
4257275678	11:01	4258359444
4257275678	11:03	4258359555

17.8.3.4 Selecting ELIN for Multiple Calls within Same ERL

The device supports the receipt of up to five ELIN numbers in the XML message of each incoming SIP INVITE message. As discussed in the preceding sections, the device sends the ELIN number as the E9-1-1 calling number to the emergency service provider. If the XML message contains more than one ELIN number, the device chooses the ELIN according to the following logic:

- If the first ELIN in the list is not being used by other active calls, it chooses this ELIN.
- If the first ELIN in the list is being used by another active call, the device skips to the next ELIN in the list, and so on until it finds an ELIN that is not being used and sends this ELIN.
- If all the ELINs in the list are in use by active calls, the device selects the ELIN number as follows:
 1. The ELIN with the lowest count (i.e., lowest number of active calls currently using this ELIN).
 2. If the count between ELINs is identical, the device selects the ELIN with the greatest amount of time passed since the original E9-1-1 call using this ELIN was terminated with the PSAP. For example, if E9-1-1 caller using ELIN 4257275678 was terminated at **11:01** and E9-1-1 caller using ELIN 4257275670 was terminated at **11:03**, then the device selects ELIN 4257275678.

In this scenario, multiple E9-1-1 calls are sent with the same ELIN.

17.8.4 Configuring AudioCodes ELIN Device

This section describes E9-1-1 configuration of the AudioCodes ELIN Gateway deployed in the Skype for Business environment.

17.8.4.1 Enabling the E9-1-1 Feature

By default, the ELIN device feature for E9-1-1 emergency call handling in a Skype for Business environment is disabled.

➤ **To enable ELIN feature:**

- For the IP Group through which you want to communicate with the public-safety answering point (PSAP), configure the 'SBC PSAP Mode' parameter to Enable. For more information, see Configuring IP Groups on page 329.

17.8.4.2 Configuring the E9-1-1 Callback Timeout

The PSAP can use the ELIN to call back the E9-1-1 caller within a user-defined time interval (in minutes) from when the initial call established with the PSAP has been terminated. By default, an ELIN can be used for PSAP callback within 30 minutes after the call is terminated. You can change this to any value between 0 and 60:

➤ **To configure the E9-1-1 callback timeout**

1. Open the Priority & Emergency page (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Priority and Emergency**).
2. In the 'E911 Callback Timeout' field (E911CallbackTimeout), enter the required callback timeout.

Figure 17-58: Configuring E9-1-1 Callback Timeout

E911 Callback Timeout	30
-----------------------	----

3. Click **Apply**.

17.8.4.3 Configuring SBC IP-to-IP Routing Rule for E9-1-1

To route incoming E9-1-1 calls to the emergency service provider's PSAP server, you need to configure routing rules in the IP-to-IP Routing table for routing between the emergency callers' IP Group and the PSAP server's IP Group. The only special configuration is to define the emergency number (e.g., 911) in the 'Destination Username Prefix' parameter of the IP Group belonging to the E9-1-1 callers. The following example shows IP-to-IP routing rules for E9-1-1 in a Skype for Business environment:

Figure 17-59: Example of IP-to-IP Routing Rules for Skype for Business E9-1-1

INDEX ↕	NAME	ROUTING POLICY	ALTERNATIVE ROUTE OPTIONS	SOURCE IP GROUP	REQUEST TYPE	SOURCE USERNAME PREFIX	DESTINATION USERNAME PREFIX	DESTINATION TYPE	DESTINATION IP GROUP
0	E911 > PSAP	Default_SBCRou	Route Row	LAN IP PBX	All	*	911	IP Group	PSAP Server
1	PSAP > E911	Default_SBCRou	Route Row	PSAP Server	All	*	*	IP Group	LAN IP PBX

17.8.4.4 Viewing the ELIN Table

To view the ELIN table:

- CLI

```
# show voip e911
ELIN          Time    Count Index Call From
-----
4257275678    22:11:52  0    2    4258359333
4257275999    22:11:57  0    3    4258359444
4257275615    22:12:03  0    0    4258359555
4257275616    22:11:45  0    1    4258359777
----- Current Time: 22:12:40
```

- Using Syslog, by invoking the following Web command shell:

```
SIP / GateWay / E911Dump
```


18 Quality of Experience

This chapter describes how to configure the Quality of Experience feature.

18.1 Reporting Voice Quality of Experience to SEM

The device can be configured to report voice (media) Quality of Experience (QoE) 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, which are then processed by the SEM.

SEM is a VoIP-quality monitoring and analysis tool. SEM provides comprehensive details on voice traffic quality, allowing system administrators to quickly identify, fix and prevent issues that could affect the voice calling experience in enterprise and service provider VoIP networks. IT managers and administrators can employ SEM in their VoIP networks to guarantee effective utilization, smooth performance, reliable QoS levels, and SLA fulfillment.



Note: For information on the SEM server, refer to the *SEM User's Manual*.

18.1.1 Configuring the SEM Server

The device can report QoE voice metrics to a single SEM server or to two SEM servers deployed in a Geographic Redundancy, High-Availability (HA) mode. Geographic Redundancy is when each SEM/EMS server is located in a different network subnet and has its own IP address. For the device to report QoE to both servers, you need to configure the IP address of each server. For normal HA mode, when both SEM/EMS servers are located in the same subnet, a single SEM/EMS server (global, virtual) IP address is used for all network components (EMS clients and managed devices). Thus, in such a setup, you need to configure only this IP address.

You can also configure the device to use a TLS connection with the SEM server. Before you can do this, configure a TLS Context (certificates) in the TLS Contexts table (see "Configuring TLS Certificate Contexts" on page 99). If no TLS Context is specified, the device uses the default TLS Context (ID 0).

You can also configure at what stage of the call the device must send the report to the SEM server. The report can be sent during the call or only at the end of the call. Reporting at the end of the call may be beneficial when network congestion occurs, as this reduces bandwidth usage over time.



Note: If a QoE traffic overflow is experienced between SEM and the device, the device sends the QoE data only at the end of the call, regardless of your settings.

For a detailed description of the SEM parameters, see "Quality of Experience Parameters" on page 775.

➤ **To configure the SEM server address and other related features:**

1. Open the Session Experience Manager page (**Setup** menu > **Signaling & Media** tab > **Media** folder > **Quality of Experience** > **Session Experience Manager**).

Figure 18-1: Configuring Session Experience Manager

GENERAL		TLS	
Server IP	<input type="text" value="0.0.0.0"/>	QoE Connection by TLS	<input type="text" value="Disable"/>
Redundant Server IP	<input type="text" value="0.0.0.0"/>	QoE TLS Context Name	<input type="text" value="default"/>
Interface Name	<input type="text" value="OAMP"/>		
REPORT MODE			
QoE Report Mode			<input type="text" value="Report QoE During C"/>

2. Configure the address of the SEM server:
 - a. In the 'Server IP' field, enter the primary SEM server's IP address.
 - b. If Geographical-Redundancy HA mode exists, in the 'Redundant Server IP' field, enter the secondary SEM server's IP address.
 - c. In the 'Interface Name' field, enter the device's IP network interface from which the device sends the reports to the SEM server.
3. From the 'QoE Report Mode' drop-down list, select when you want the device to send reports of a call to the SEM (during or at the end of the call).
4. (Optional) Configure a TLS connection with the SEM server:
 - a. From the 'QoE Connection by TLS' drop-down list, select **Enable**.
 - b. From the 'QoE TLS Context Name' drop-down list, select the TLS Context which defines the TLS settings (e.g., certificates).
5. Click **Apply**.

18.1.2 Configuring Clock Synchronization between Device and SEM

To ensure accurate call quality statistics and analysis by the SEM server, you must configure the device and the SEM server with the same clock source for clock synchronization. In other words, you need to configure them with the same NTP server.

The NTP server can be one of the following:

- AudioCodes EMS server (also acting as an NTP server)
- Third-party, external NTP server

Once you have determined the NTP server, all the elements--device, SEM, and EMS--must be configured with the same NTP server address.

To configure, the NTP server's address on the device, see "Configuring Automatic Date and Time using SNTP" on page 115.

18.1.3 Enabling RTCP XR Reporting to SEM

In order for the device to be able to send voice metric reports to the SEM, you need to enable the RTP Control Protocol Extended Reports (RTCP XR) VoIP management protocol. RTCP XR defines a set of voice metrics that contain information for assessing VoIP call quality and diagnosing problems. Enabling RTCP XR means that the device can send RTCP XR messages, containing the call-quality metrics, to the SEM server.

For enabling RTCP XR reporting, see "Configuring RTCP XR" on page 665. To configure what to report to the SEM, see "Configuring Quality of Experience Profiles" on page 291.

18.2 Configuring Quality of Experience Profiles

Quality of Experience Profiles enable you to effectively monitor the quality of voice calls traversing the device in your network. Quality of Experience Profiles define severity thresholds for voice metrics monitored by the device, which if crossed can result in various actions (discussed later in the section).

Quality of Experience is configured using two tables with parent-child type relationship. The Quality of Experience Profile table is the parent, which defines the name of the Quality of Experience Profile. The Quality of Experience Color Rules table is the child, which defines severity thresholds per voice metric for the specific Quality of Experience Profile. You can configure up to 256 Quality of Experience Profiles and up to 256 Quality of Experience Color Rules.

Once configured, you can apply the Quality of Experience Profiles to specific calls (network links), by assigning them to any of the following configuration entities:

- IP Groups (see "Configuring IP Groups" on page 329)
- Media Realms (see "Configuring Media Realms" on page 303)
- Remote Media Subnets (see "Configuring Remote Media Subnets" on page 306)

The Quality of Experience Profile allows you to configure thresholds for the following monitored voice metrics:

- **Mean Opinion Score (MOS):** MOS is the average grade on a quality scale, expressed as a single number in the range of 1 to 5, where 1 is the lowest audio quality and 5 the highest audio quality.
- **Delay (or latency):** Time it takes for information to travel from source to destination (round-trip time).
- **Packet Loss:** Lost packets are RTP packets that are not received by the voice endpoint. Packet loss can result in choppy voice transmission.
- **Jitter:** Jitter can result from uneven delays between received voice packets. To space evenly, the device's jitter buffer adds delay. The higher the measurement, the greater the impact of the jitter buffer's delay on audio quality.
- **Residual Echo Return Loss (RERL):** An echo is a reflection of sound arriving at the listener at some time after the sound was initiated (often by the listener). Echo is typically caused by delay.

At any given time during a call, a voice metric can be in one of the following color-coded quality states (as displayed by SEM):

- **Green:** Indicates good call quality
- **Yellow:** Indicates fair call quality
- **Red:** Indicates poor call quality

When the threshold of a voice metric is crossed, the device changes the alarm severity and corresponding color-coded quality state of the call:

- **Minor Threshold (Yellow):** Lower threshold that indicates changes from Green or Red to Yellow.
- **Major Threshold (Red):** Higher threshold that indicates changes from Green or Yellow to Red.

The device also uses hysteresis to determine whether the threshold has indeed being crossed. Hysteresis defines the amount of fluctuation from the threshold in order for the threshold to be considered as crossed (i.e., change in color state). Hysteresis is used to avoid false reports being sent by the device. Hysteresis is used only for threshold crossings toward a lesser severity (i.e., from Red to Yellow, Red to Green, or Yellow to Green).

The following example is used to explain how the device considers threshold crossings. The example is based on the MOS of a call, where the Major threshold is configured to 2, the Minor threshold to 4 and the hysteresis for both thresholds to 0.1:

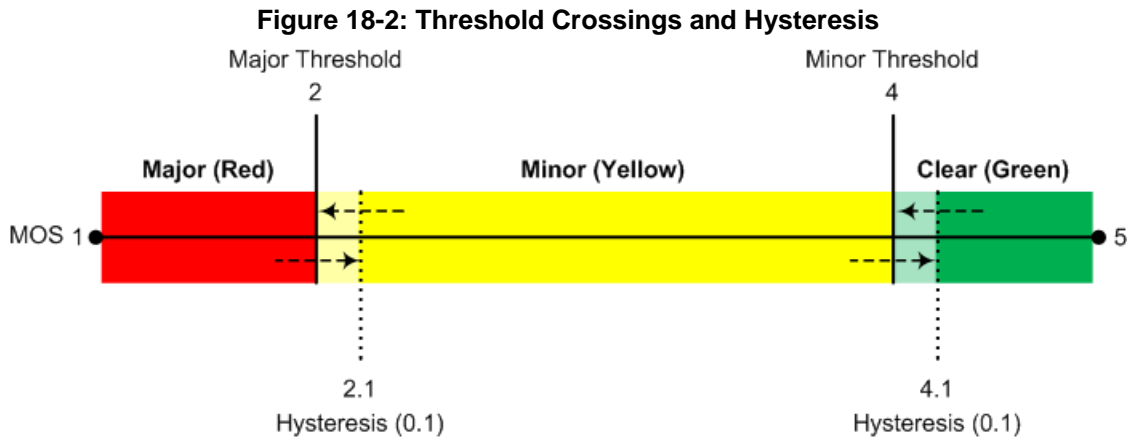


Table 18-1: Threshold Crossings based on Threshold and Hysteresis

Threshold Crossing	Calculation	Threshold based on Example
Green to Yellow (Minor alarm)	The change occurs if the measured metric crosses the configured Minor threshold only (i.e., hysteresis is not used).	4
Green to Red (Major alarm)	The change occurs if the measured metric crosses the configured Major threshold only (i.e., hysteresis is not used).	2
Yellow to Red (Major alarm)	The change occurs if the measured metric crosses the configured Major threshold only (i.e., hysteresis is not used).	2
Red to Yellow (Minor alarm)	The change occurs if the measured metric crosses the configured Major threshold with hysteresis configured for the Major threshold.	2.1 (i.e., 2 + 0.1)
Red to Green (alarm cleared)	The change occurs if the measured metric crosses the configured Minor threshold with hysteresis configured for the Minor threshold.	4.1 (i.e., 4 + 0.1)
Yellow to Green (alarm cleared)	The change occurs if the measured metric crosses the configured Minor threshold with hysteresis configured for the Minor threshold.	4.1 (i.e., 4 + 0.1)

Each time a voice metric threshold is crossed (i.e., color changes), the device can do the following depending on configuration:

- Report the change in the measured metrics to AudioCodes' Session Experience Manager (SEM) server. The SEM displays this call quality status for the associated SEM link (IP Group, Media Realm, or Remote Media Subnet). To configure the SEM server's address, see "Configuring the SEM Server" on page 289.
- Depending on the crossed threshold type, you can configure the device to reject calls to the destination IP Group or use an alternative IP Profile for the IP Group. For more information, see "Configuring Quality of Service Rules" on page 300.

- Alternative routing based on measured metrics. If a call is rejected because of a crossed threshold, the device generates a SIP 806 response. You can configure this SIP response code as a reason for alternative routing (see "Configuring SIP Response Codes for Alternative Routing Reasons" on page 482).



Note: For your convenience, the device provides pre-configured Quality of Experience Profiles. One of these pre-configured profiles is the default Quality of Experience Profile, which is used if you do not configure a Quality of Experience Profile.

The following procedure describes how to configure Quality of Experience Profiles through the Web interface. You can also configure it through other management platforms:

- Quality of Experience Profile table:** *ini* file (QoEProfile) or CLI (configure voip > qoe qoe-profile)
- Quality of Experience Color Rules table:** *ini* file (QOECColorRules) or CLI (configure voip > qoe qoe-profile qoe-color-rules)

➤ **To configure a QoE Profile:**

- Open the Quality of Experience Profile table (**Setup** menu > **Signaling & Media** tab > **Media** folder > **Quality of Experience** > **Quality of Experience Profile**).
- Click **New**; the following dialog box appears:

Figure 18-3: Quality of Experience Profile Table - Dialog Box

- Configure a QoE Profile according to the parameters described in the table below.
- Click **Apply**.

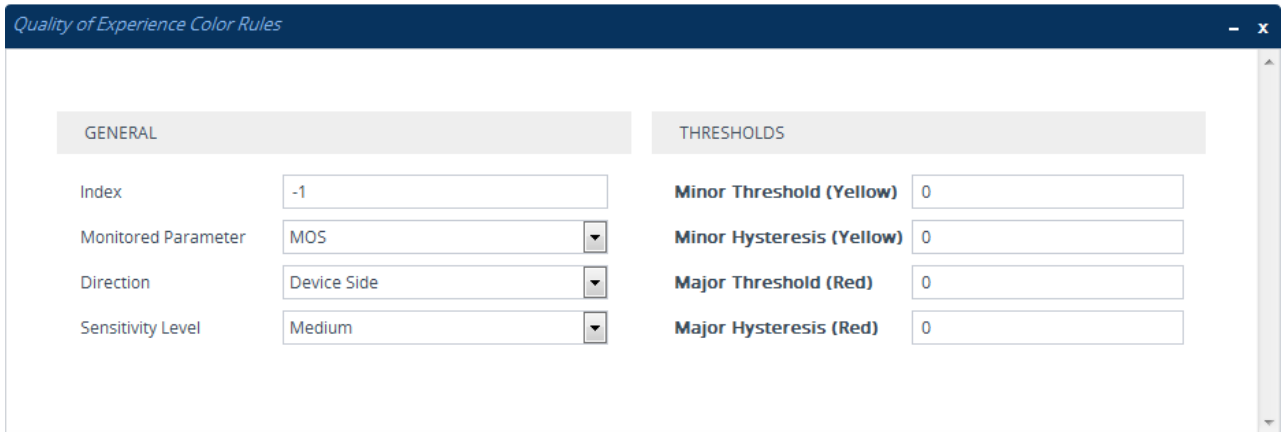
Table 18-2: Quality of Experience Profile Table Parameter Descriptions

Parameter	Description
Index [QoEProfile_Index]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
Profile Name name [QoEProfile_Name]	Defines an arbitrary name to easily identify the row. The valid value is a string of up to 20 characters.
Sensitivity Level sensitivity-level	Defines the pre-configured threshold profile to use. <ul style="list-style-type: none"> [0] User Defined = Need to define thresholds per monitored parameter in the Quality of Experience Color Rules table.

Parameter	Description
[QOEProfile_SensitivityLevel]	<ul style="list-style-type: none"> [1] Low = Pre-configured low sensitivity thresholds. [2] Medium = (Default) Pre-configured medium sensitivity thresholds. [3] High = Pre-configured high sensitivity thresholds. Reporting is done for small fluctuations in parameter values.

- In the Quality of Experience Profile table, select the row for which you want to configure QoE thresholds, and then click the **Quality of Experience Color Rules** link located below the table; the Quality of Experience Color Rules table appears.
- Click **New**; the following dialog box appears:

Figure 18-4: Quality of Experience Color Rules Table - Dialog Box



- Configure a rule according to the parameters described in the table below.
- Click **New**, and then save your settings to flash memory.

Table 18-3: Quality of Experience Color Rules Table Parameter Descriptions

Parameter	Description
General	
Index index [QOECOLORRules_ColorRuleIndex]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
Monitored Parameter monitored-parameter [QOECOLORRules_monitoredParam]	Defines the parameter to monitor and report. <ul style="list-style-type: none"> [0] MOS (default) [1] Delay [2] Packet Loss [3] Jitter [4] RERL [Echo]
Direction direction [QOECOLORRules_direction]	Defines the monitoring direction. <ul style="list-style-type: none"> [0] Device Side (default) [1] Remote Side
Sensitivity Level sensitivity-level [QOECOLORRules_profile]	Defines the sensitivity level of the thresholds. <ul style="list-style-type: none"> [0] User Defined = Need to define the thresholds in the parameters described below. [1] Low = Pre-configured low sensitivity threshold values.

Parameter	Description
	<p>Thus, reporting is done only if changes in parameters' values are significant.</p> <ul style="list-style-type: none"> ▪ [2] Medium = (Default) Pre-configured medium sensitivity threshold values. ▪ [3] High = Pre-configured high sensitivity threshold values. Thus, reporting is done for small fluctuations in parameter values.
Thresholds	
Minor Threshold (Yellow) minor-threshold-yellow [QOECColorRules_MinorThreshold]	<p>Defines the Minor threshold value, which is the lower threshold located between the Yellow and Green states. To consider a threshold crossing:</p> <ul style="list-style-type: none"> ▪ Increase in severity (i.e., Green to Yellow): Only this value is used. ▪ Decrease in severity (Red to Green, or Yellow to Green): This value is used with the hysteresis, configured by the 'Minor Hysteresis (Yellow)' parameter (see below). <p>The valid threshold values are as follows:</p> <ul style="list-style-type: none"> ▪ MOS values are in multiples of 10. For example, to denote a MOS of 3.2, the value 32 (i.e., 3.2×10) must be entered. ▪ Delay values are in msec. ▪ Packet Loss values are in percentage (%). ▪ Jitter is in msec. ▪ Echo measures the Residual Echo Return Loss (RERL) in dB.
Minor Hysteresis (Yellow) minor-hysteresis-yellow [QOECColorRules_MinorHysteresis]	<p>Defines the amount of fluctuation (hysteresis) from the Minor threshold, configured by the 'Minor Threshold (Yellow)' parameter in order for the threshold to be considered as crossed. The hysteresis is used only to determine threshold crossings to Green (i.e., from Yellow to Green, or Red to Green). In other words, the device considers a threshold crossing to Green only if the measured voice metric crosses the Minor threshold and the hysteresis.</p> <p>For example, if you configure the 'Minor Threshold (Yellow)' parameter to 4 and the 'Minor Hysteresis (Yellow)' parameter to 0.1 (for MOS), the device considers a threshold crossing to Green only if the MOS crosses 4.1 (i.e., $4 + 0.1$).</p>
Major Threshold (Red) major-threshold-red [QOECColorRules_MajorThreshold]	<p>Defines the Major threshold value, which is the upper threshold located between the Yellow and Red states. To consider a threshold crossing:</p> <ul style="list-style-type: none"> ▪ Increase in severity (i.e., Yellow to Red): Only this value is used. ▪ Decrease in severity (Red to Yellow): This value is used with the hysteresis, configured by the 'Major Hysteresis (Red)' parameter (see below). <p>The valid threshold values are as follows:</p> <ul style="list-style-type: none"> ▪ MOS values are in multiples of 10. For example, to denote a MOS of 3.2, the value 32 (i.e., 3.2×10) must be entered. ▪ Delay values are in msec. ▪ Packet Loss values are in percentage (%).

Parameter	Description
	<ul style="list-style-type: none"> ■ Jitter is in msec. ■ Echo measures the Residual Echo Return Loss (RERL) in dB.
Major Hysteresis (Red) major-hysteresis-red [QOECOLORRules_MajorHysteresis]	Defines the amount of fluctuation (hysteresis) from the Major threshold, configured by the 'Major Threshold (Red)' parameter in order for the threshold to be considered as crossed. The hysteresis is used only to determine threshold crossings from Red to Yellow. In other words, the device considers a threshold crossing to Yellow only if the measured voice metric crosses the Major threshold and the hysteresis. For example, if you configure the 'Major Threshold (Red)' parameter to 2 and the 'Major Hysteresis (Red)' parameter to 0.1 (for MOS), the device considers a threshold crossing to Yellow only if the MOS crosses 2.1 (i.e., 2 + 0.1).

18.3 Configuring Bandwidth Profiles

The Bandwidth Profile table lets you configure up to 1,884 Bandwidth Profiles. A Bandwidth Profile defines bandwidth utilization thresholds for audio and/or video traffic (incoming and outgoing), which if crossed can result in various actions (discussed later in the section). Bandwidth Profiles enhance the device's monitoring of bandwidth utilization.

Once configured, you can apply Bandwidth Profiles to specific calls, by assigning them to any of the following configuration entities:

- IP Groups (see "Configuring IP Groups" on page 329)
- Media Realms (see "Configuring Media Realms" on page 303)
- Remote Media Subnets (see "Configuring Remote Media Subnets" on page 306)

Each time a configured bandwidth threshold is crossed, the device can do the following, depending on configuration:

- Reject calls destined to the IP Group or use an alternative IP Profile for the IP Group. For more information, see "Configuring Quality of Service Rules" on page 300.
- Use an alternative routing rule for alternative routing. If a call is rejected due to a crossed threshold, the device generates a SIP 806 response. You can configure the SIP response code as a reason for alternative routing (see "Configuring SIP Response Codes for Alternative Routing Reasons" on page 482).
- Send an SNMP alarm (acMediaRealmBWThresholdAlarm). The device clears the alarm when bandwidth utilization returns to normal (Green).

The SEM displays bandwidth utilization using color-coded states:

- **Green:** Indicates bandwidth utilization is within normal range.
- **Yellow:** Indicates bandwidth utilization is encroaching on "total" bandwidth, serving as a warning (or it could also mean that bandwidth utilization has dropped below the red state).
- **Red:** Indicates that bandwidth utilization has exceeded total bandwidth.

Bandwidth Profiles let you configure bandwidth thresholds, which when crossed changes the color-coded state for bandwidth utilization:

- **Green-Yellow (Minor) Threshold:** Lower threshold configured as a percentage of the configured major (total) bandwidth threshold. When bandwidth goes over the threshold, the device considers it a Yellow state (Minor alarm severity); when it goes below the threshold, it considers it a Green state (cleared alarm).

- Yellow-Red (Major) Threshold:** Upper threshold configured by the major (total) bandwidth threshold. When bandwidth goes over the threshold, the device considers it a Red state (Major alarm severity); when it goes below the threshold, it considers it a Yellow state (Minor alarm severity).

The device also uses hysteresis to determine whether the threshold has indeed being crossed. Hysteresis defines the amount of fluctuation from the threshold in order for the threshold to be considered as crossed (i.e., change in color state). Hysteresis is used to avoid false reports being sent by the device. Hysteresis is used only for threshold crossings toward a lesser severity (i.e., from Red to Yellow, Red to Green, or Yellow to Green). Hysteresis is configured as a percentage of the configured major (total) bandwidth threshold.

The following example is used to explain how the device considers threshold crossings. The example is based on a setup where the Major (total) bandwidth threshold is configured to 64,000 Kbps, the Minor threshold to 50% (of the total) and the hysteresis to 10% (of the total):

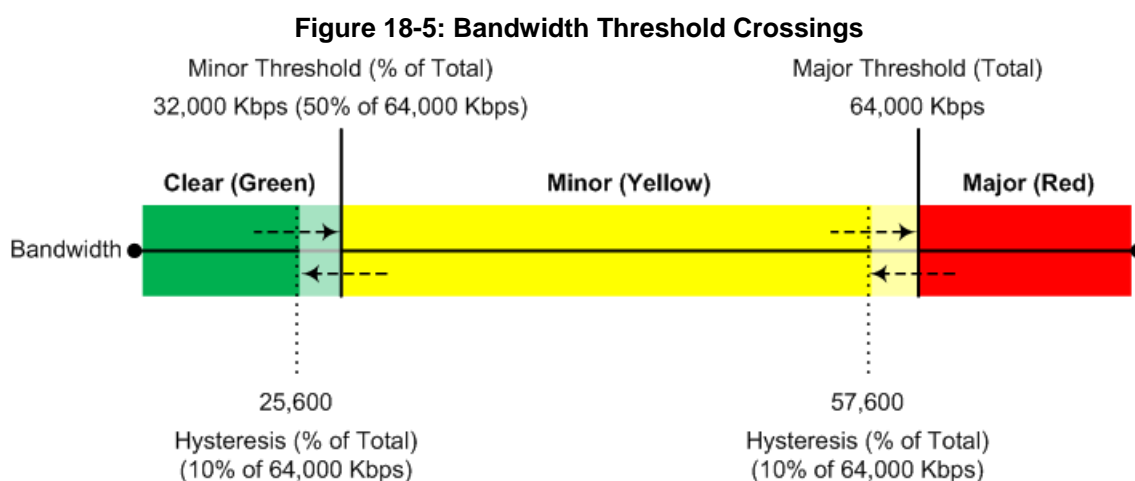


Table 18-4: Threshold Crossings based on Threshold and Hysteresis

Threshold Crossing	Calculation	Threshold based on Example
Green to Yellow (Minor alarm)	The change occurs if the current bandwidth crosses the configured Minor threshold only (i.e., hysteresis is not used).	32,000 Kbps
Green to Red (Major alarm)	The change occurs if the current bandwidth crosses the configured Major threshold only (i.e., hysteresis is not used).	64,000 Kbps
Yellow to Red (Major alarm)	The change occurs if the current bandwidth crosses the configured Major threshold only (i.e., hysteresis is not used).	64,000 Kbps
Red to Yellow (Minor alarm)	The change occurs if the current bandwidth crosses the configured Major threshold with hysteresis.	57,600 Kbps [64,000 - (10% x 64,000)]
Yellow to Green (alarm cleared)	The change occurs if the current bandwidth crosses the configured Minor threshold with hysteresis.	25,600 Kbps [32,000 - (10% x 64,000)]
Red to Green (alarm cleared)	The change occurs if the current bandwidth crosses the configured Minor threshold with	25,600 Kbps [32,000 - (10% x

Threshold Crossing	Calculation	Threshold based on Example
	hysteresis.	64,000)]

The following procedure describes how to configure Bandwidth Profiles through the Web interface. You can also configure it through ini file (BWProfile) or CLI (configure voip > que bw-profile).

➤ **To configure a Bandwidth Profile:**

1. Open the Bandwidth Profile table (**Setup** menu > **Signaling & Media** tab > **Media** folder > **Quality of Experience** > **Bandwidth Profile**).
2. Click **New**; the following dialog box appears:

Figure 18-6: Bandwidth Profile Table - Dialog Box

3. Configure a rule according to the parameters described in the table below.
4. Click **Apply**, and then reset the device with a save to flash memory.

Table 18-5: Bandwidth Profile Table Parameter Descriptions

Parameter	Description
General	
Index [BWProfile_Index]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
Name name [BWProfile_Name]	Defines an arbitrary name to easily identify the row. The valid value is a string of up to 20 characters.
Egress Audio Bandwidth egress-audio-bandwidth [BWProfile_EgressAudioBandwidth]	Defines the major (total) threshold for outgoing audio traffic (in Kbps).
Ingress Audio Bandwidth ingress-audio-bandwidth [BWProfile_IngressAudioBandwidth]	Defines the major (total) threshold for incoming audio traffic (in Kbps).
Egress Video Bandwidth	Defines the major (total) threshold for outgoing video traffic (in Kbps).

Parameter	Description
egress-video-bandwidth [BWProfile_EgressVideoBandwidth]	
Ingress Video Bandwidth ingress-video-bandwidth [BWProfile_IngressVideoBandwidth]	Defines the major (total) threshold for incoming video traffic (in Kbps).
Total Egress Bandwidth total-egress-bandwidth [BWProfile_TotalEgressBandwidth]	Defines the major (total) threshold for video and audio outgoing bandwidth (in Kbps).
Total Ingress Bandwidth total-ingress-bandwidth [BWProfile_TotalIngressBandwidth]	Defines the major (total) threshold for video and audio incoming bandwidth (in Kbps).
Thresholds	
Minor Threshold minor-threshold [BWProfile_MinorThreshold]	<p>Defines the Minor threshold value, which is the lower threshold located between the Yellow and Green states. The parameter is configured as a percentage of the major (total) bandwidth threshold (configured by the above bandwidth parameters). For example, if you configure the parameter to 50 and the 'Egress Audio Bandwidth' parameter to 64,000, the Minor threshold for outgoing audio bandwidth is 32,000 (i.e., 50% of 64,000).</p> <p>To consider a threshold crossing:</p> <ul style="list-style-type: none"> ▪ Increase in severity (i.e., Green to Yellow): Only this value is used. ▪ Decrease in severity (Red to Green, or Yellow to Green): This value is used with the hysteresis, configured by the 'Hysteresis' parameter (see below). <p>Note: The parameter applies to all your configured bandwidths.</p>
Hysteresis hysteresis [BWProfile_Hysteresis]	<p>Defines the amount of fluctuation (hysteresis) from the configured bandwidth threshold in order for the threshold to be considered as crossed (i.e., avoids false reports of threshold crossings). The hysteresis is used only to determine threshold crossings when severity is reduced (i.e., from Red to Yellow, Yellow to Green, or Red to Green). The parameter is configured as a percentage of the Major (total) bandwidth threshold.</p> <p>For example, if you configure the parameter to 10 and the 'Egress Audio Bandwidth' parameter to 64,000, the hysteresis is 6,400 (10% of 64,000) and threshold crossings are considered at the following bandwidths:</p> <ul style="list-style-type: none"> ▪ Red-to-Yellow (Yellow-Minor alarm severity): 57,600 Kbps [64,000 - (10% x 64,000)] ▪ Yellow-to-Green (Green-alarm cleared): 25,600 Kbps [32,000 - (10% x 64,000)]
Generate Alarm generate-alarms [BWProfile_GenerateAlarms]	<p>Enables the device to send an SNMP alarm if a bandwidth threshold is crossed.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable

18.4 Configuring Quality of Service Rules

The Quality of Service Rules table lets you configure up to 7,500 Quality of Service rules. A Quality of Service rule defines an action to perform when the threshold (major or minor) of a specific performance monitoring call metric is crossed for a specific IP Group. The call metric can be voice quality (i.e., MOS), bandwidth, Answer-seizure ratio (ASR), Network Effectiveness Ratio (NER), or Average Call Duration (ACD).

Depending on the call metric, you can configure the following actions to be performed if the threshold is crossed:

- Reject calls to the IP Group for a user-defined duration.

Rejection of calls can also trigger alternative routing. When the device rejects a call due to an ASR, NER or ACD threshold crossing, it generates the SIP response code, 850 (Signaling Limits Exceeded). When the device rejects a call due to Voice Quality and Bandwidth threshold crossing, it generates the SIP response code, 806 (Media Limits Exceeded). If you configure these SIP response codes in the Alternative Routing Reasons table (see "Configuring SIP Response Codes for Alternative Routing Reasons" on page 482) and the device rejects a call, it searches in the IP-to-IP Routing table for an alternative routing rule.

When the device rejects calls to an IP Group based on a Quality of Service rule, it raises an SNMP alarm (acIpGroupNoRouteAlarm). The alarm is also raised upon a keep-alive failure with the IP Group. For more information, refer to the *SNMP Reference Guide*.

- Use a different IP Profile for the IP Group or current call. This action can be useful, for example, when poor quality occurs due to packet loss and the device can then switch to an IP Profile configured with a higher RTP redundancy level or lower bit-rate coder.

To learn more about which actions are supported per call metric, see the description of the 'Rule Action' parameter below.

To configure thresholds, see the following sections:

- Voice Quality (MOS) - "Configuring Quality of Experience Profiles" on page 291
- Bandwidth - "Configuring Bandwidth Profiles" on page 296
- ASR, ACD and NER - "Configuring Performance Profiles" on page 651

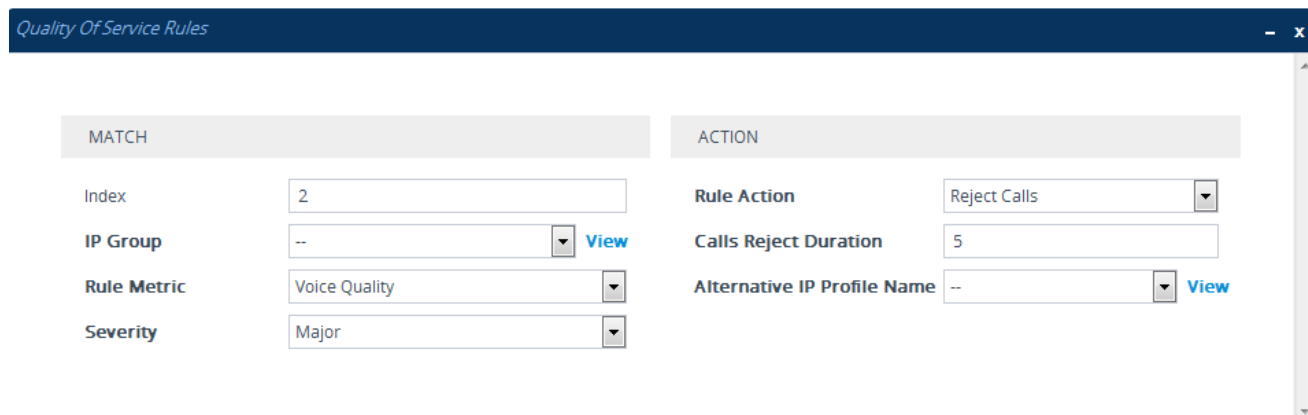
The following procedure describes how to configure Quality of Service rules through the Web interface. You can also configure it through ini file (QualityOfServiceRules) or CLI (configure voip > qoe quality-of-service-rules).

➤ To configure a Quality of Service rule:

1. Open the Quality of Service Rules table (**Setup** menu > **Signaling & Media** tab > **Media** folder > **Quality of Service Rules**).

- Click **New**; the following dialog box appears:

Figure 18-7: Quality of Service Rules Table - Dialog Box



- Configure a rule according to the parameters described in the table below.
- Click **Apply**, and then reset the device with a save-to-flash for your settings to take effect.

Table 18-6: Quality of Service Rules Table Parameter Descriptions

Parameter	Description
Match	
Index [QualityOfServiceRules_Index]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
IP Group ip-group-name [QualityOfServiceRules_IPGroup Name]	Assigns an IP Group. The rule applies to all calls belonging to the IP Group.
Rule Metric rule-metric [QualityOfServiceRules_Rule Metric]	Defines the performance monitoring call metric to which the rule applies if the metric's threshold is crossed. <ul style="list-style-type: none"> ▪ [0] Voice Quality = (Default) The device calculates MOS of calls and if the threshold is crossed (i.e., poor quality), the configured action (see 'Rule Action' parameter below) is done for all new calls and for the entire IP Group. ▪ [1] Bandwidth ▪ [2] ACD ▪ [3] ASR ▪ [4] NER ▪ [5] Poor Invoice Quality = The device calculates MOS (and TMMBR) of the call and if the threshold is crossed (i.e., poor quality), the device uses a different IP Profile (see 'Rule Action' parameter below) for the current call only (not the entire IP Group).
Severity severity [QualityOfServiceRules_Severity]	Defines the alarm severity level. When the configured severity occurs, the device performs the action of the rule. <ul style="list-style-type: none"> ▪ [0] Major (Default) ▪ [1] Minor Note: If you configure the 'Rule Metric' parameter to ACD, ASR or

Parameter	Description
	<p>NER, you must configure the parameter to Major. For all other 'Rule Metric' parameter values, you can configure the parameter to any value.</p>
<p>Action</p>	
<p>Rule Action rule-action [QualityOfServiceRules_Rule Action]</p>	<p>Defines the action to be done if the rule is matched.</p> <ul style="list-style-type: none"> ▪ [0] Reject Calls = (Default) New calls destined to the specified IP Group are rejected for a user-defined duration. To configure the duration, use the 'Calls Reject Duration' parameter (see below). ▪ [1] Alternative IP Profile = A different IP Profile is used for the IP Group or call (depending on the 'Rule Metric' parameter). To specify the IP Profile, use the 'Alternative IP Profile Name' parameter (see below). <p>Note:</p> <ul style="list-style-type: none"> ▪ If you configure the 'Rule Metric' parameter to ACD, ASR or NER, you must configure the parameter to Reject Calls. ▪ If you configure the 'Rule Metric' parameter to Voice Quality or Bandwidth: <ul style="list-style-type: none"> ✓ If you configure the 'Severity' parameter to Minor, you must configure the parameter to Alternative IP Profile. ✓ If you configure the 'Severity' parameter to Major, you can configure the parameter to any option. <p>When configured to Alternative IP Profile and the threshold is crossed, the device changes the IP Profile for the entire IP Group for all new calls.</p> <ul style="list-style-type: none"> ▪ If you configure the 'Rule Metric' parameter to Poor InVoice Quality, you must configure the parameter to Alternative IP Profile. If the threshold is crossed (i.e., poor call quality), the device changes the IP Profile for the specific call only (during the call).
<p>Calls Reject Duration calls-reject-duration [QualityOfServiceRules_Calls RejectDuration]</p>	<p>Defines the duration (in minutes) for which the device rejects calls to the IP Group if the rule is matched.</p> <p>The default is 5.</p> <p>Note: The parameter is applicable only if the 'Rule Action' parameter is configured to Reject Calls.</p>
<p>Alternative IP Profile Name alt-ip-profile-name [QualityOfServiceRules_AltIP ProfileName]</p>	<p>Assigns a different IP Profile to the IP Group or call (depending on the 'Rule Metric' parameter) if the rule is matched.</p> <p>By default, no value is defined.</p> <p>Note: The parameter is applicable only if the 'Rule Action' parameter is configured to Alternative IP Profile.</p>

19 Control Network

This section describes configuration of the network at the SIP control level.

19.1 Configuring Media Realms

The Media Realms table lets you configure a pool of up to 1,024 SIP media interfaces, termed *Media Realms*. Media Realms lets you divide a Media-type interface (configured in the IP Interfaces table) into several media realms, where each realm is specified by a UDP port range. Media Realms also define the maximum number of permitted media sessions.

Once configured, to apply Media Realms to specific calls, you need to assign them to any of the following configuration entities:

- IP Groups (see "Configuring IP Groups" on page 329)
- SIP Interfaces (see "Configuring SIP Interfaces" on page 321)

You can also apply the device's Quality of Experience feature to Media Realms:

- **Quality of Experience Profile:** Call quality monitoring based on thresholds for voice metrics (e.g., MOS) can be applied per Media Realm. For example, if MOS is considered poor, calls on this Media Realm can be rejected. To configure Quality of Experience Profiles, see "Configuring Quality of Experience Profiles" on page 291.
- **Bandwidth Profile:** Bandwidth utilization thresholds can be applied per Media Realm. For example, if bandwidth thresholds are crossed, the device can reject any new new calls on this Media Realm. To configure Bandwidth Profiles, see "Configuring Bandwidth Profiles" on page 296.

The Media Realms table provides sub-tables ("child" tables) that let you configure the following:

- Remote Media Subnets: Defines remote destination subnets per Media Realm and assigns each subnet a Quality of Experience Profile and Bandwidth Profile. For more information, see "Configuring Remote Media Subnets" on page 306.
- Media Realm Extensions: Defines port ranges for multiple Media-type interfaces per Media Realm. For more information, see "Configuring Media Realm Extensions" on page 309.



Note:

- The Media Realm assigned to an IP Group overrides any other Media Realm assigned to any other configuration entity associated with the call.
- If you modify a Media Realm that is currently being used by a call, the device does not perform Quality of Experience for the call.
- If you delete a Media Realm that is currently being used by a call, the device maintains the call until the call parties end the call.
- The device provides a preconfigured Media Realm ("DefaultRealm") in the Media Realms table, which can be modified or deleted.

The following procedure describes how to configure Media Realms through the Web interface. You can also configure it through ini file (CpMediaRealm) or CLI (configure voip > realm).

➤ **To configure a Media Realm:**

1. Open the Media Realms table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Media Realms**).

- Click **New**; the following dialog box appears:

Figure 19-1: Media Realms Table - Add Dialog Box

- Configure the Media Realm according to the parameters described in the table below.
- Click **Apply**.

Table 19-1: Media Realms table Parameter Descriptions

Parameter	Description
General	
Index [CpMediaRealm_Index]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
Name name [CpMediaRealm_MediaRealmName]	Defines an arbitrary name to easily identify the row. The valid value is a string of up to 40 characters. Note: <ul style="list-style-type: none"> The parameter is mandatory. Each row must be configured with a unique name.
Topology Location topology-location [CpMediaRealm_TopologyLocation]	Defines the display location of the Media Realm in the Topology view. <ul style="list-style-type: none"> [0] Down = (Default) The Media Realm element is displayed on the lower border of the view. [1] Up = The Media Realm element is displayed on the upper border of the view. For more information on the Topology view, see "Building and Viewing SIP Entities in Topology View" on page 350.
IPv4 Interface Name ipv4 [CpMediaRealm_IPv4IF]	Assigns an IPv4 network interface to the Media Realm. By default, no value is defined. To configure IP network interfaces, see "Configuring IP Network Interfaces" on page 130.
IPv6 Interface Name	Assigns an IPv6 network interface to the Media Realm.

Parameter	Description
ipv6if [CpMediaRealm_IPv6IF]	By default, no value is defined. To configure IP network interfaces, see Configuring IP Network Interfaces on page 130.
Port Range Start port-range-start [CpMediaRealm_PortRangeStart]	Defines the starting port for the range of media interface UDP ports. By default, no value is defined. Note: <ul style="list-style-type: none"> ▪ You must either configure all your Media Realms with port ranges or all without; not some with and some without. ▪ The available UDP port range is according to the BaseUDPPort parameter. For more information, see "Configuring RTP Base UDP Port" on page 187. ▪ The base UDP port number (BaseUDPPort parameter) must be greater than the highest UDP port configured for a SIP Interface (see "Configuring SIP Interfaces" on page 321). For example, if your highest configured UDP port for a SIP Interface is 6060, you must configure the BaseUDPPort parameter to any value greater than 6060. ▪ The port must be different from ports configured for SIP traffic (i.e., ports configured for SIP Interfaces). For example, if the RTP port range is 6000 to 6999, the SIP port can be less than 6000 or greater than 6999. ▪ Media Realms must not have overlapping port ranges.
Number of Media Session Legs session-leg [CpMediaRealm_MediaSessionLeg]	Defines the number of media sessions for the configured port range. By default, no value is defined.
Port Range End port-range-end [CpMediaRealm_PortRangeEnd]	(Read-only field) Displays the ending port for the range of media interface UDP ports. The device automatically populates the parameter with a value, calculated by the summation of the 'Port Range Start' parameter and 'Number of Media Session Legs' parameter (multiplied by the port chunk size) minus 1: $\text{start port} + (\text{sessions} * \text{port spacing}) - 1$ For example, a port starting at 6,000, 5 sessions and 10 port spacing: $6,000 + (5 * 10) - 1 = 6,000 + (50) - 1 = 6,000 + 49 = 6,049$ The device allocates the UDP ports for RTP, RTCP and T.38 traffic per leg in "jumps" (spacing) of 4, 5 or 10, configured by the UdpPortSpacing parameter. For example, if the port range starts at 6000 and the UDP port spacing is 10, the available ports include 6000, 6010, 6020, 6030, and so on (depending on number of media sessions). For RTCP and T.38 traffic, the port offset from the RTP port used for the voice session is one and two, respectively. For example, if the voice session uses RTP port 6000, the RTCP port and T.38 port for the session is 6001 and 6002, respectively. However, you can configure the device to use the same port for RTP and T.38 packets, by configuring the

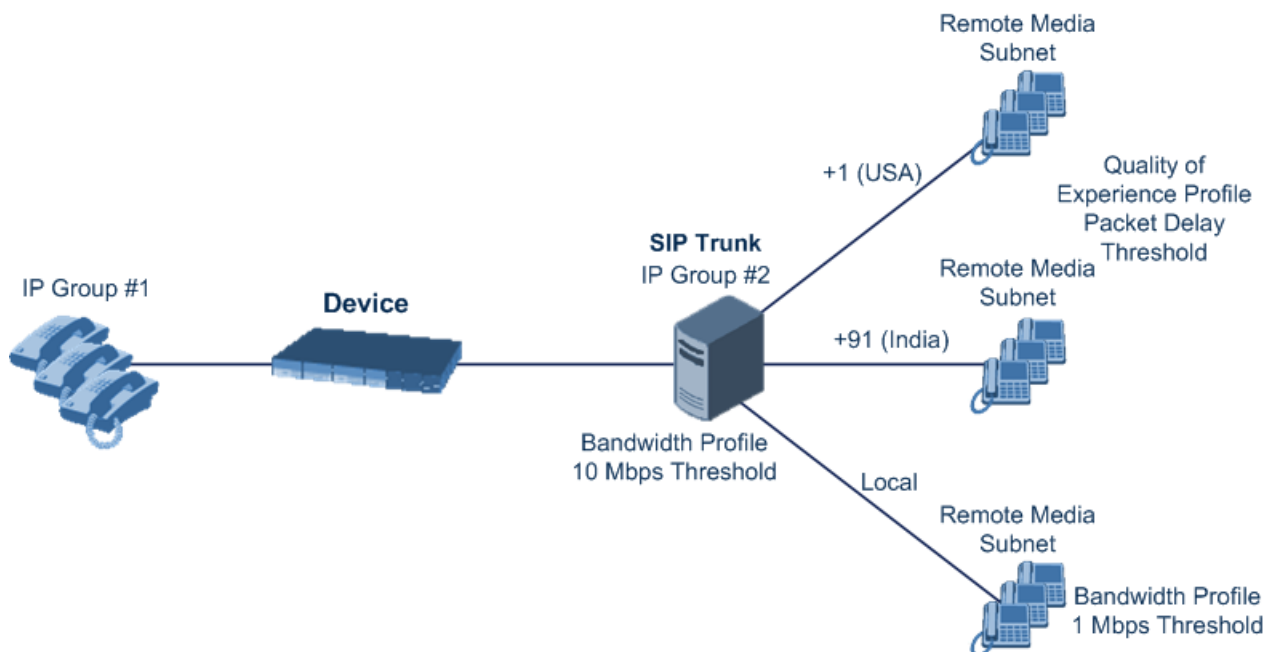
Parameter	Description
	T38UseRTPPort parameter to 1. For more information on local UDP port range, see "Configuring RTP Base UDP Port" on page 187.
Default Media Realm is-default [CpMediaRealm_IsDefault]	Defines the Media Realm as the default Media Realm. The default Media Realm is used for SIP Interfaces and IP Groups for which you have not assigned a Media Realm. <ul style="list-style-type: none"> ▪ [0] No (default) ▪ [1] Yes Note: <ul style="list-style-type: none"> ▪ You can configure the parameter to Yes for only one Media Realm; all the other Media Realms must be configured to No. ▪ If you do not configure the parameter (i.e., the parameter is No for all Media Realms), the device uses the first Media Realm in the table as the default. ▪ If the table is not configured, the default Media Realm includes all configured media interfaces.
Quality of Experience	
QoE Profile qoe-profile [CpMediaRealm_QoeProfile]	Assigns a QoE Profile to the Media Realm. By default, no value is defined. To configure QoE Profiles, see "Configuring Quality of Experience Profiles" on page 291.
BW Profile bw-profile [CpMediaRealm_BWProfile]	Assigns a Bandwidth Profile to the Media Realm. By default, no value is defined. To configure Bandwidth Profiles, see "Configuring Bandwidth Profiles" on page 296.

19.1.1 Configuring Remote Media Subnets

Remote Media Subnets define destination subnets for media (RTP/SRTP) traffic on a specific Media Realm. Each Remote Media Subnet can be assigned different call quality (Quality of Experience Profile) and bandwidth utilization (Bandwidth Profile) profiles. These profiles are configured in "Configuring Quality of Experience Profiles" on page 291 and "Configuring Bandwidth Profiles" on page 296, respectively. Thus, you can apply these profiles to remote media subnets instead of Media Realms or IP Groups. You can configure up to five Remote Media Subnets per Media Realm.

The figure below illustrates an example for implementing Remote Media Subnets. IP Group #2 represents a SIP Trunk which routes international (USA and India) and local calls. As international calls are typically more prone to higher delay than local calls, different Quality of Experience Profiles are assigned to them. This is done by creating Remote Media Subnets for each of these call destinations and assigning each Remote Media Subnet a different Quality of Experience Profile. A Quality of Experience Profile that defines a packet delay threshold is assigned to the international calls, which if crossed, a different IP Profile is used that defines higher traffic priority to voice over other traffic. In addition, IP Group #2 has a 10-Mbps bandwidth threshold and a "tighter" bandwidth limitation (e.g., 1 Mbps) is allocated to local calls. If this limit is exceeded, the device rejects new calls to this Remote Media Subnet.

Figure 19-2: Remote Media Subnets Example



The following procedure describes how to configure Remote Media Subnets through the Web interface. You can also configure it through ini file (RemoteMediaSubnet) or CLI (configure voip > remote-media-subnet).

➤ **To configure a Remote Media Subnet:**

1. Open the Media Realms table (see "Configuring Media Realms" on page 303).
2. Select the Media Realm row for which you want to add Remote Media Subnets, and then click the **Remote Media Subnet** link located below the table; the Remote Media Subnet table appears.

- Click **New**; the following dialog box appears:

Figure 19-3: Remote Media Subnet Table - Add Dialog Box

- Configure the Remote Media Subnet according to the parameters described in the table below.
- Click **Apply**.

Table 19-2: Remote Media Subnet Table Parameter Descriptions

Parameter	Description
Index [RemoteMediaSubnet_RemoteMediaSubnetIndex]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
Name name [RemoteMediaSubnet_RemoteMediaSubnetName]	Defines an arbitrary name to easily identify the row. The valid value is a string of up to 20 characters. Note: Each row must be configured with a unique name.
Prefix Length prefix-length [RemoteMediaSubnet_PrefixLength]	Defines the subnet mask in Classless Inter-Domain Routing (CIDR) notation. For example, 16 denotes 255.255.0.0. The default is 16.
Address Family address-family [RemoteMediaSubnet_AddressFamily]	Defines the IP address protocol. <ul style="list-style-type: none"> [2] IPv4 (default) [10] IPv6
Destination IP dst-ip-address [RemoteMediaSubnet_DstIPAddress]	Defines the IP address of the destination. The default is 0.0.0.0.
QoS Profile qoe-profile [RemoteMediaSubnet_QOEProfileName]	Assigns a Quality of Experience Profile to the Remote Media Subnet. By default, no value is defined. To configure QoS Profiles, see "Configuring Quality of Experience Profiles" on page 291.

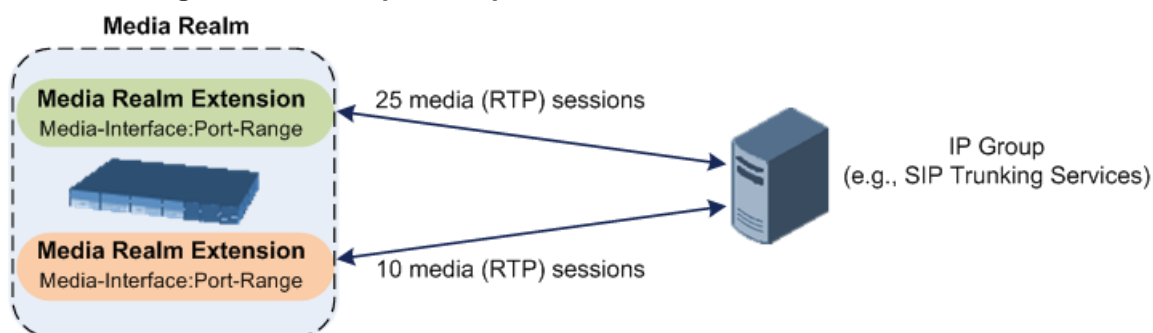
Parameter	Description
BW Profile bw-profile [RemoteMediaSubnet_BWProfileName]	Assigns a Bandwidth Profile to the Remote Media Subnet. By default, no value is defined. To configure Bandwidth Profiles, see "Configuring Bandwidth Profiles" on page 296.

19.1.2 Configuring Media Realm Extensions

The Media Realm Extension table lets you configure 5 Media Realm Extensions. A Media Realm Extension defines a port range with the number of sessions for a specific Media-type network interface (configured in the IP Interfaces table). The Media Realm Extension can be configured with any Media-type interface and port range, regardless of the specific Media-type interface assigned to its associated Media Realm. Thus, Media Realm Extensions let you configure a Media Realm with different port ranges / sessions and different interfaces (i.e., the Media Realm is distributed across multiple interfaces).

Media Realm Extensions can be useful, for example, to overcome limitations of the maximum number of media ports supported per interface. Instead of configuring only a single Media Realm in the Media Realms table (see "Configuring Media Realms" on page 303), you can also configure additional "Media Realms" in the Media Realm Extensions table associated with the single Media Realm. An IP Group that is associated with a Media Realm configured with Media Realm Extensions, allocates its media sessions / ports between the different interfaces, as configured by the Media Real and its associated Media Realm Extensions. For example, two Media Realm Extensions could be configured, whereby one allocates 25 media sessions on interface "LAN-1" and another, 10 sessions on interface "LAN-2". The Media Realm associated with these Media Realm Extensions would be assigned to the relevant IP Group.

Figure 19-4: Example of Implementation of Media Realm Extensions



The following procedure describes how to configure Media Realm Extensions through the Web interface. You can also configure it through ini file (MediaRealmExtension) or CLI (configure voip > voip-network realm-extension).

➤ **To configure a Media Realm Extension:**

1. Open the Media Realms table (see "Configuring Media Realms" on page 303).
2. Select the Media Realm for which you want to add Remote Media Extensions, and then click the **Media Realm Extension** link located below the table; the Media Realm Extension table appears.

- Click **New**; the following dialog box appears:

Figure 19-5: Media Realm Extension Table - Add Dialog Box

- Configure the Media Realm Extension according to the parameters described in the table below.
- Click **Apply**.

Table 19-3: Media Realm Extension Table Parameter Descriptions

Parameter	Description
Index [MediaRealmExtension_ExtensionIndex]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
IPv4 Interface Name [MediaRealmExtension_IPv4IF]	Assigns an IPv4 network interface (configured in the IP Interfaces table) to the Media Realm Extension. By default, no value is defined. To configure IP network interfaces, see "Configuring IP Network Interfaces" on page 130. Note: The parameter is mandatory.
IPv6 Interface Name [MediaRealmExtension_IPv6IF]	Assigns an IPv6 network interface (configured in the IP Interfaces table) to the Media Realm Extension. By default, no value is defined. Note: The parameter is mandatory.
Port Range Start [MediaRealmExtension_PortRangeStart]	Defines the first (lower) port in the range of media UDP ports for the Media Realm Extension. By default, no value is defined. Notes: <ul style="list-style-type: none"> You must either configure all your Media Realms with port ranges or all without; not some with and some without. The available UDP port range is according to the BaseUDPport parameter. For more information, see "Configuring RTP Base UDP Port" on page 187. The port range must not overlap with any other media port range that you have configured in the table or in the Media Realms table.
Port Range End	Defines the last (upper) port in the range of media UDP

Parameter	Description
[MediaRealmExtension_PortRangeEnd]	ports for the Media Realm Extension. Note: It is unnecessary to configure the parameter. The device automatically populates the parameter with a value, calculated by the summation of the 'Number of Media Session Legs' parameter (multiplied by the port chunk size) and the 'Port Range Start' parameter. After you have added the Media Realm Extension row to the table, the parameter is displayed with the calculated value.
Number Of Media Session Legs [MediaRealmExtension_MediaSessionLeg]	Defines the number of media sessions for the port range. For example, 100 ports correspond to 10 media sessions, since ports are allocated in chunks of 10. By default, no value is defined. Note: The parameter is mandatory.

19.2 Configuring SRDs

The SRDs table lets you configure up to 600 signaling routing domains (SRD). The SRD is a logical representation of an entire SIP-based VoIP network (Layer 5) consisting of groups of SIP users and servers. The SRD is associated with all the configuration entities (e.g., SIP Interfaces and IP Groups) required for routing calls within the network. Typically, only a **single** SRD is required (recommended) for most deployments. Multiple SRDs are only required for multi-tenant deployments, where the physical device is "split" into multiple logical devices. For more information on multi-tenant architecture, see "Multiple SRDs for Multi-tenant Deployments" on page 317.

As the device is shipped with a default SRD ("DefaultSRD" at Index 0), if your deployment requires only one SRD, you can use the default SRD instead of creating a new one. When only one SRD is employed and you create other related configuration entities (e.g., SIP Interfaces), the default SRD is automatically assigned to the new configuration entity. Therefore, when employing a single-SRD configuration topology, there is no need to handle SRD configuration (i.e., transparent).

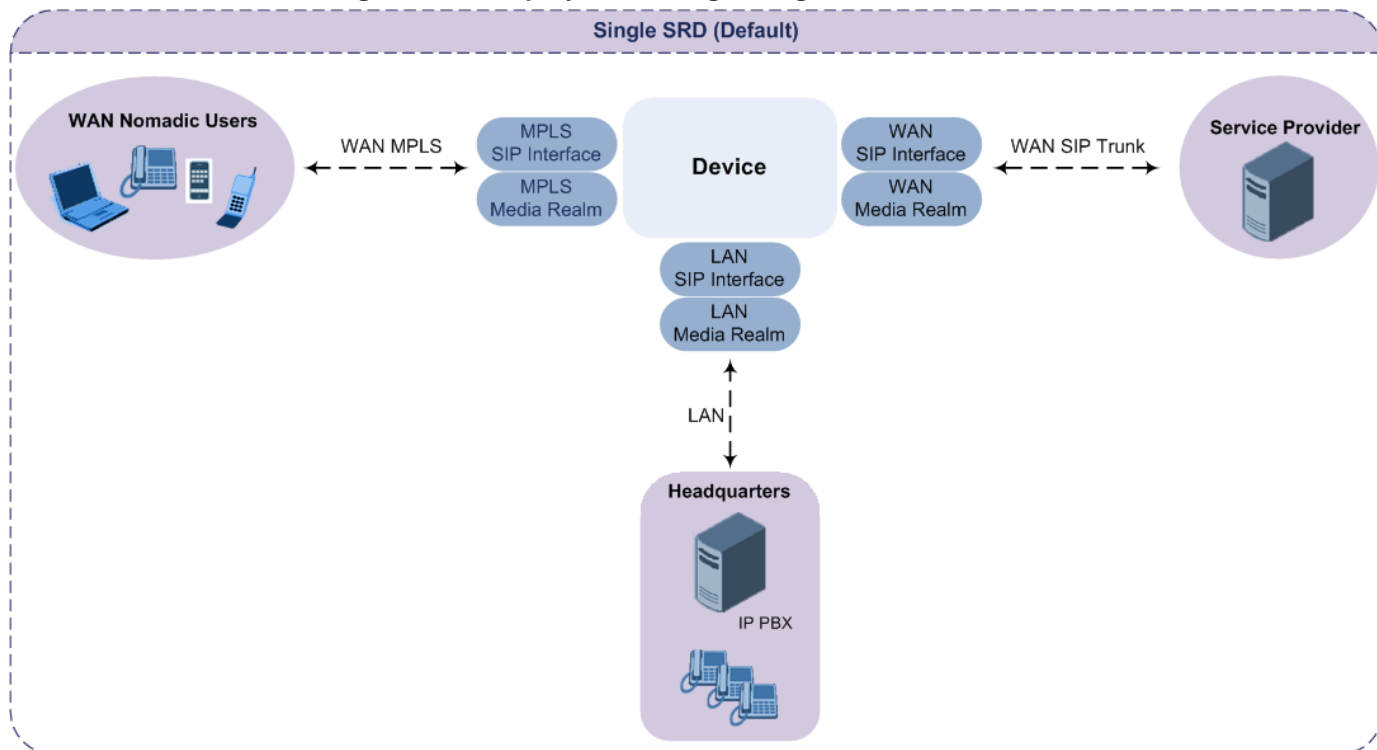
SRDs are associated with the following configuration entities:

- SIP Interface (mandatory) - see "Configuring SIP Interfaces" on page 321
- IP Group (mandatory) - see "Configuring IP Groups" on page 329
- Proxy Set (mandatory) - see "Configuring Proxy Sets" on page 341
- Admission Control rule - see Configuring Admission Control Table on page 457
- Classification rule - see Configuring Classification Rules on page 461

As mentioned previously, if you use only a single SRD, the device automatically assigns it to the above-listed configuration entities.

As each SIP Interface defines a different Layer-3 network (see "Configuring SIP Interfaces" on page 321 for more information) on which to route or receive calls and as you can assign multiple SIP Interfaces to the same SRD, for most deployment scenarios (even for multiple Layer-3 network environments), you only need to employ a single SRD to represent your VoIP network (Layer 5). For example, if your VoIP deployment consists of an Enterprise IP PBX (LAN), a SIP Trunk (WAN), and far-end users (WAN), you would only need a single SRD. The single SRD would be assigned to three different SIP Interfaces, where each SIP Interface would represent a specific Layer-3 network (IP PBX, SIP Trunk, or far-end users) in your environment. The following figure provides an example of such a deployment:

Figure 19-6: Deployment using a Single SRD



**Note:**

- It is recommended to use a single-SRD configuration topology, unless you are deploying the device in a multi-tenant environment, in which case multiple SRDs are required.
- Each SIP Interface, Proxy Set, and IP Group can be associated with only one SRD.
- If you have upgraded your device to Version 7.0 and your device was configured with multiple SRDs but not operating in a multi-tenant environment, it is recommended to gradually change your configuration to a single SRD topology.
- If you upgrade the device from an earlier release to Version 7.0, your previous SRD configuration is fully preserved regarding functionality. The same number of SRDs is maintained, but the configuration elements are changed to reflect the configuration topology of Version 7.0. Below are the main changes in configuration topology when upgrading to Version 7.0:
 - ✓ The SIP Interface replaces the associated SRD in several tables (due to support for multiple SIP Interfaces per SRD).
 - ✓ Some fields in the SRDs table were duplicated or moved to the SIP Interfaces table.
 - ✓ Indices used for associating configuration entities in tables are changed to row pointers (using the entity's name).
 - ✓ Some tables are now associated (mandatory) with an SRD (SIP Interface, IP Group, Proxy Set, and Classification).
 - ✓ Some fields used for associating configuration entities in tables now have a value of **Any** to distinguish between **Any** and **None** (deleted entity or not associated).

The following procedure describes how to configure SRDs through the Web interface. You can also configure it through ini file (SRD) or CLI (configure voip > srd).

➤ **To configure an SRD:**

1. Open the SRDs table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **SRDs**).
2. Click **New**; the following dialog box appears:

Figure 19-7: SRDs Table - Add Dialog Box

3. Configure an SRD according to the parameters described in the table below.

4. Click **Apply**.

Table 19-4: SRDs table Parameter Descriptions

Parameter	Description
General	
Index [SRD_Index]	Defines an index for the new table row. Note: Each row must be configured with a unique index.
Name name [SRD_Name]	Defines an arbitrary name to easily identify the row. The valid value can be a string of up to 40 characters. Note: <ul style="list-style-type: none"> ▪ The parameter is mandatory. ▪ Each row must be configured with a unique name.
Sharing Policy type [SRD_SharingPolicy]	Defines the sharing policy of the SRD, which determines whether the SRD shares its SIP resources (SIP Interfaces, Proxy Sets, and IP Groups) with all other SRDs (Shared and Isolated). <ul style="list-style-type: none"> ▪ [0] Shared = (Default) SRD shares its resources with other SRDs (Isolated and Shared) and calls can thus be routed between the SRD and other SRDs. ▪ [1] Isolated = SRD does not share its resources with other SRDs and calls cannot be routed between the SRD and other Isolated SRDs. However, calls can be routed between the SRD and other Shared SRDs. For more information on SRD Sharing Policy, see Multiple SRDs for Multi-tenant Deployments on page 317.
SBC Operation Mode sbc-operation-mode [SRD_SBCOperationMode]	Defines the device's operational mode for the SRD. <ul style="list-style-type: none"> ▪ [0] B2BUA = (Default) Device operates as a back-to-back user agent (B2BUA), changing the call identifiers and headers between the inbound and outbound legs. ▪ [1] Call Stateful Proxy = Device operates as a Stateful Proxy, passing the SIP message transparently between inbound and outbound legs. In other words, the same SIP dialog identifiers (tags, Call-Id and CSeq) occur on both legs (as long as no other configuration disrupts the CSeq compatibility). ▪ [2] Microsoft Server = Operating mode for the One-Voice Resiliency feature, whereby the device is deployed together with Skype for Business-compatible IP Phones at small remote branch offices in a Microsoft® Skype for Business™ environment. For more information on B2BUA and Stateful Proxy modes, see B2BUA and Stateful Proxy Operating Modes on page 422. Note: <ul style="list-style-type: none"> ▪ The settings of the parameter also determines the default behavior of related parameters in the IP Profiles table (SBCRemoteRepresentationMode, SBCKeepVIAHeaders, SBCKeepUserAgentHeader, SBCKeepRoutingHeaders, SBCRemoteMultipleEarlyDialogs). ▪ If the 'SBC Operation Mode' parameter is configured in the IP Groups table, the 'SBC Operation Mode' parameter in the SRDs table is ignored.
SBC Routing Policy sbc-routing-policy-name	Assigns a Routing Policy to the SRD. By default, no value is defined if you have configured multiple Routing Policies. If you have configured only one Routing Policy, the

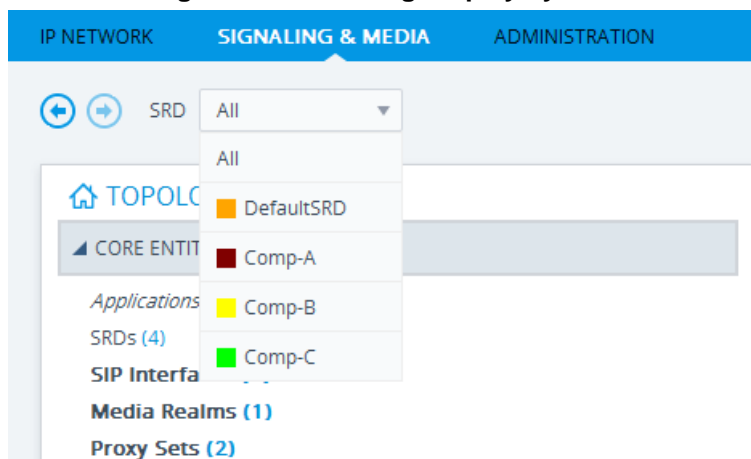
Parameter	Description
[SRD_SBCRoutingPolicyName]	<p>device assigns it to the SRD by default.</p> <p>For more information on Routing Policies, see Configuring SBC Routing Policy Rules on page 484.</p> <p>Note:</p> <ul style="list-style-type: none"> ▪ If you have assigned a Routing Policy to a Classification rule that is associated with the SRD, the Routing Policy assigned to the SRD is ignored. ▪ You can assign the same Routing Policy to multiple SRDs.
Used By Routing Server used-by-routing-server [SIPInterface_UsedByRoutingServer]	<p>Enables the SRD to be used by a third-party routing server for call routing decisions.</p> <ul style="list-style-type: none"> ▪ [0] Not Used (default) ▪ [1] Used <p>For more information on the third-party routing server feature, see "Centralized Third-Party Routing Server" on page 266.</p>
Registration	
Max. Number of Registered Users max-reg-users [SRD_MaxNumOfRegUsers]	<p>Defines the maximum number of users belonging to the SRD that can register with the device.</p> <p>The default is -1, which means that the number of allowed user registrations is unlimited.</p>
User Security Mode block-un-reg-users [SRD_BlockUnRegUsers]	<p>Defines the blocking (reject) policy for incoming SIP dialog-initiating requests (e.g., INVITE messages) from registered and unregistered users belonging to the SRD.</p> <ul style="list-style-type: none"> ▪ [0] Accept All = (Default) Accepts requests from registered and unregistered users. ▪ [1] Accept Registered Users = Accepts requests only from users registered with the device. Requests from users not registered are rejected. ▪ [2] Accept Registered Users from Same Source = Accepts requests only from registered users whose source address is the same as that registered with the device (during the REGISTER message process). All other requests are rejected. The device verifies whether the IP address and port are different only if the transport protocol is UDP; otherwise, the device verifies only the IP address. The verification is performed before any of the device's call handling processes (i.e., Classification, Manipulation and Routing). <p>Note:</p> <ul style="list-style-type: none"> ▪ The parameter is applicable only to calls belonging to User-type IP Groups. ▪ The feature is not applicable to REGISTER requests. ▪ The option, Accept Registered Users from Same Source [2] does not apply to registration refreshes. These requests are accepted even if the source address is different to that registered with the device. ▪ When the device rejects a call, it sends a SIP 500 "Server Internal Error" response to the user. In addition, it reports the rejection (Dialog establish failure - Classification failure) using the Intrusion Detection System (IDS) feature (see Configuring IDS Policies on page 164), by sending an SNMP trap.

Parameter	Description
	<ul style="list-style-type: none"> When the corresponding parameter in the SIP Interfaces table (SIPInterface_BlockUnRegUsers) is configured to any value other than default [-1] for a SIP Interface that is associated with the SRD, the parameter in the SRDs table is ignored for calls belonging to the SIP Interface.
Enable Un-Authenticated Registrations enable-un-auth-registrs [SRD_EnableUnAuthenticated Registrations]	<p>Enables the device to accept REGISTER requests and register them in its registration database from new users that have not been authenticated by a proxy/registrar server (due to proxy down) and thus, re-routed to a User-type IP Group.</p> <p>In normal operation scenarios in which the proxy server is available, the device forwards the REGISTER request to the proxy and if authenticated by the proxy (i.e., device receives a success response), the device adds the user to its registration database. The routing to the proxy is according to the SBC IP-to-IP Routing table where the destination is the proxy's IP Group. However, when the proxy is unavailable (e.g., due to network connectivity loss), the device can accept REGISTER requests from new users if a matching alternative routing rule exists in the SBC IP-to-IP Routing table where the destination is the user's User-type IP Group (i.e., call survivability scenarios) and if the parameter is enabled.</p> <ul style="list-style-type: none"> [0] Disable = The device rejects REGISTER requests from new users that were not authenticated by a proxy server. [1] Enable = (Default) The device accepts REGISTER requests from new users even if they were not authenticated by a proxy server, and registers the user in its registration database. <p>Note:</p> <ul style="list-style-type: none"> Regardless of the parameter, the device always accepts registration refreshes from users that are already registered in its database. For a SIP Interface that is associated with the SRD, if the corresponding parameter in the SIP Interfaces table (SIPInterface_EnableUnAuthenticatedRegistrations) is configured to Disable or Enable, the parameter in the SRD is ignored for calls belonging to the SIP Interface.

19.2.1 Filtering Tables in Web Interface by SRD

When your configuration includes multiple SRDs, you can filter tables in the Web interface by SRD. The filter is configured in the SRD Filter drop-down list, located on the Web interface's toolbar, as shown below.

Figure 19-8: Filtering Display by SRD



The filter is applied throughout the Web GUI. When you select an SRD for filtering, the Web interface displays only table rows associated with the filtered SRD. When you add a new row to a table, the filtered SRD is automatically selected as the associated SRD. For example, if you filter the Web display by SRD "Comp-A" and you then add a new Proxy Set, the Proxy Set is automatically associated with this SRD (i.e., the 'SRD' parameter is set to "Comp-A"). All other parameters in the dialog box are also automatically set to values associated with the filtered SRD.

The SRD filter also affects display of number of configured rows and invalid rows by status icons on table items in the Navigation tree. The status icons only display information relating to the filtered SRD.

SRD filtering is especially useful in multi-tenant setups where multiple SRDs may be configured. In such a setup, SRD filtering eliminates configuration clutter by "hiding" SRDs that are irrelevant to the current configuration and facilitates configuration by automatically associating the filtered SRD, and other configuration elements associated with the filtered SRD, wherever applicable.

19.2.2 Multiple SRDs for Multi-tenant Deployments

The device can be deployed in a multi-tenant architecture, serving multiple customers (tenants) from a single, shared physical entity. The device's multi-tenant feature is fully scalable, offering almost "non-bleeding" partition per tenant, whereby users of one tenant can't infringe on the space of users of another tenant. The device provides per tenant configuration, monitoring, reporting, analytics, alarms and interfacing. The device is a real-time multi-tenant system that provides each tenant with optimal real-time performance, as each session received by the device is classified and processed only through the tenant's "orbit".

While some enterprises are large enough to justify a dedicated standalone device, many enterprises require only a fraction of the device's capacity and capabilities. Service providers offering SIP Trunking services can funnel multiple enterprises into a single device and thereby, reap significant cost improvements over a device-per-customer model. Tenant size in a multi-tenant architecture can vary and therefore, the instance CPU, memory and interface allocations should be optimized so as not to waste resources for small-sized

tenants on the one hand, and not to allocate too many instances for a single tenant/customer on the other. For example, it would be a waste to allocate a capacity of 100 concurrent sessions to a small tenant for which 10 concurrent sessions suffice.

In a multi-tenant deployment, each tenant is represented by a dedicated SRD. The different Layer-3 networks (e.g., LAN IP-PBX users, WAN SIP Trunk, and WAN far-end users) of the tenant are represented by SIP Interfaces, which are all associated with the tenant's SRD. As related configuration entities (SIP Interfaces, IP Groups, Proxy Sets, Classification rules, and IP-to-IP Routing rules) are associated with the specific SRD, each SRD has its own logically separated configuration tables (although configured in the same tables). Therefore, full logical separation (on the SIP application layer) between tenants is achieved by SRD.

To create a multi-tenant configuration topology that is as non-bleeding as possible, you can configure an SRD (tenant) as *Isolated* and *Shared*:

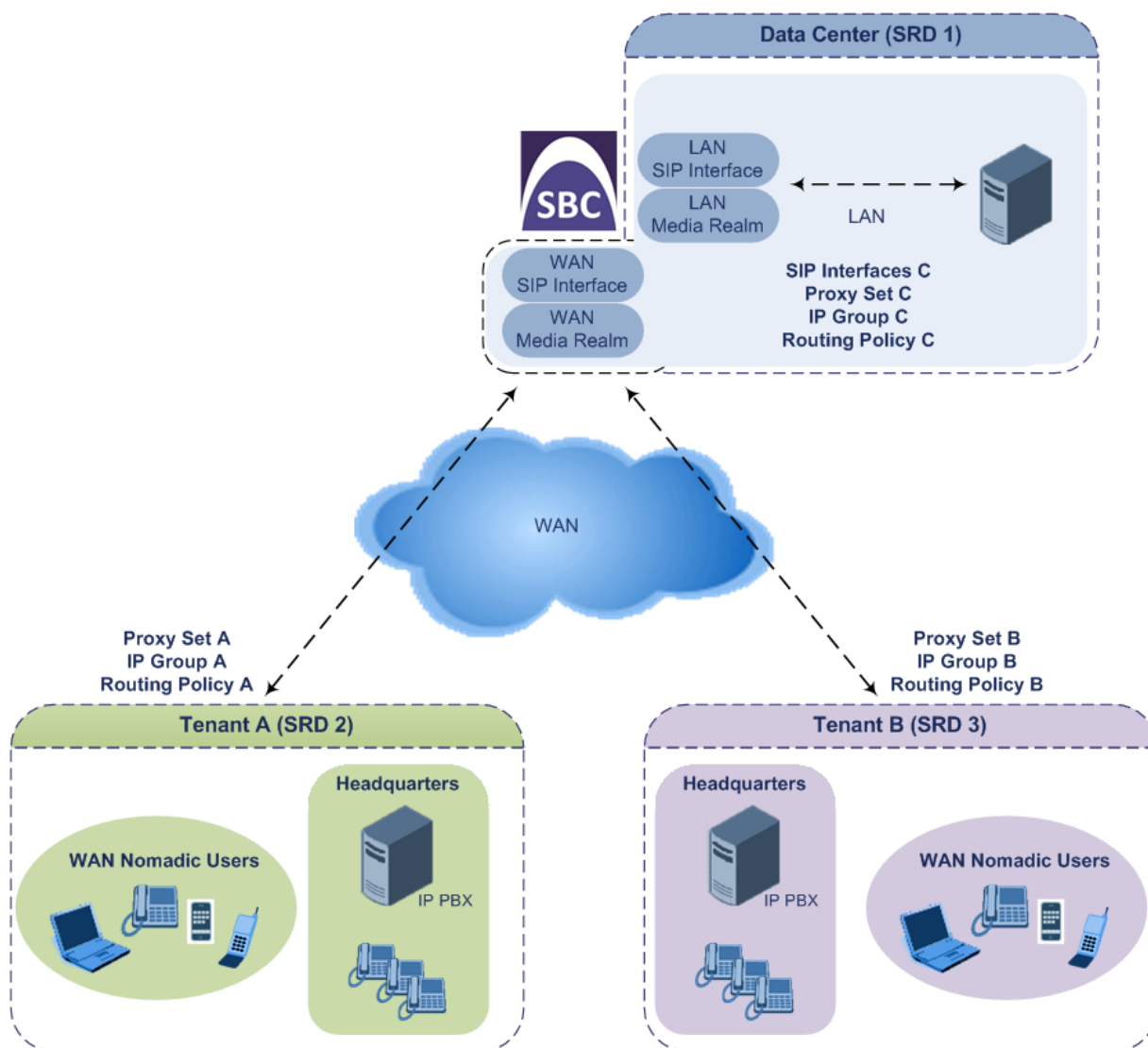
- **Isolated SRD:** An Isolated SRD has its own dedicated SIP resources (SIP Interfaces, Proxy Sets, and IP Groups). No other SRD can use the SIP resources of an Isolated SRD. Thus, call traffic of an Isolated SRD is kept separate from other SRDs (tenants), preventing any risk of traffic "leakage" with other SRDs.

Isolated SRDs are more relevant when each tenant needs its own separate (dedicated) routing "table" for non-bleeding topology. Separate routing tables are implemented using Routing Policies. In such a non-bleeding topology, routing between Isolated SRDs is not possible. This enables accurate and precise routing per SRD, eliminating any possibility of erroneous call routing between SRDs, restricting routing to each tenant's (SRD's) sphere. Configuring only one Routing Policy that is shared between Isolated SRDs is not best practice for non-bleeding environments, since it allows routing between these SRDs.

- **Shared SRD:** Isolated SRDs have their own dedicated SIP resources (SIP Interfaces, Proxy Sets, and IP Groups). This may not be possible in some deployments. For example, in deployments where all tenants use the same SIP Trunking service, or use the same SIP Interface due to limited SIP interface resources (e.g., multiple IP addresses cannot be allocated and SIP port 5060 must be used). In contrast to Isolated SRDs, a Shared SRD can share its' SIP resources with all other SRDs (Shared and Isolated). This is typically required when tenants need to use common resources. In the SIP Trunk example, the SIP Trunk would be associated with a Shared SRD, enabling all tenants to route calls with the SIP Trunk.

Another configuration entity that can be used for multi-tenant deployments is the Routing Policy. Routing Policies allow each SRD (or tenant) to have its own routing rules, manipulation rules, Least Cost Routing (LCR) rules, and/or LDAP-based routing configuration. However, not all multi-tenant deployments need multiple Routing Policies and typically, their configuration is not required. Isolated SRDs are more relevant only when each tenant requires its own dedicated Routing Policy to create separate, dedicated routing "tables"; for all other scenarios, SRDs can be Shared. For more information on Routing Policies, see "Configuring SBC Routing Policy Rules" on page 484.

The figure below illustrates a multi-tenant architecture with Isolated SRD tenants ("A" and "B") and a Shared SRD tenant ("Data Center") serving as a SIP Trunk:



To facilitate multi-tenant configuration through CLI, you can access a specific tenant "view". Once in a specific tenant view, all configuration commands apply only to the currently viewed tenant. Only table rows (indexes) belonging to the viewed tenant can be modified. New table rows are automatically associated with the viewed tenant (i.e., SRD name). The display of tables and show running-configuration commands display only rows relevant to the viewed tenant (and shared tenants). The show commands display only information relevant to the viewed tenant. To support this CLI functionality, use the following commands:

- To access a specific tenant view:

```
# srd-view <SRD name>
```

Once accessed, the tenant's name (i.e., SRD name) forms part of the CLI prompt, for example:

```
# srd-view datacenter
(srd-datacenter)#
```

- To exit the tenant view:

```
# no srd-view
```

19.2.3 Cloning SRDs

You can clone (duplicate) existing SRDs. This is especially useful when operating in a multi-tenant environment and you need to add new tenants (SRDs). The new tenants can quickly and easily be added by simply cloning one of the existing SRDs. Once cloned, all you need to do is tweak configuration entities associated with the SRD clone.

When an SRD is cloned, the device adds the new SRD clone to the next available index row in the SRDs table. The SRD clone is assigned a unique name in the following syntax format: <unique clone ID>_<original SRD index>_CopyOf_<name, or index if no name, of original SRD>. For example, if you clone SRD "SIP-Trunk" at index 2, the new SRD clone is assigned the name, "36454371_2_CopyOf_SIP-Trunk".

The SRD clone has identical settings as the original SRD. In addition, all configuration entities associated with the original SRD are also cloned and these clones are associated with the SRD clone. The naming convention of these entities is the same as the SRD clone (see above) and all have the same unique clone ID ("36454371" in the example above) as the cloned SRD. These configuration entities include IP Groups, SIP Interfaces, Proxy Sets (without addresses), Classification rules, and Admission Control rules. If the Routing Policy associated with the original SRD is not associated with any other SRD, the Routing Policy is also cloned and its' clone is associated with the SRD clone. All configuration entities associated with the original Routing Policy are also cloned and these clones are associated with the Routing Policy clone. These configuration entities include IP-to-IP Routing rules, Inbound Manipulation rules, and Outbound Manipulation rules.

When any configuration entity is cloned (e.g., an IP-to-IP Routing rule) as a result of a cloned SRD, all fields of the entity's row which "point" to other entities (e.g., SIP Interface, Source IP Group, and Destination IP Group) are replaced by their corresponding clones.



Note: For some cloned entities such as SIP Interfaces, some parameter values may change. This occurs in order to avoid the same parameter having the same value in more than one table row (index), which would result in invalid configuration. For example, a SIP Interface clone will have an empty Network Interface setting. After the clone process finishes, you thus need to update the Network Interface for valid configuration.

➤ **To clone an SRD:**





- Web interface: In the SRDs table, select an SRD to clone, and then click the **Clone** button.
- CLI:

```
(config-voip)# srd clone <SRD index that you want cloned>
```


19.2.4 Color-Coding of SRDs in Web Interface

To easily identify your configured SRDs, the Web interface displays each SRD in a unique color. The color is automatically and randomly assigned to new SRDs and is displayed in a box alongside the name of the SRD in tables where the SRD is configured or assigned. This is applied throughout the Web interface. The following example shows SRDs assigned with unique color codes.

Figure 19-9: Color-Coding of SRDs

INDEX ↕	NAME
0	 DefaultSRD (#0)
1	 Comp-A (#1)
2	 Comp-B (#2)
3	 Comp-C (#3)

↑

19.2.5 Automatic Configuration based on SRD

To facilitate configuration and eliminate possible flaws in configuration due to invalid associations between configuration entities, the Web interface automatically configures configuration entities based on SRD:

- If you delete an SRD (in the SRDs table) that is associated with other configuration entities in other tables, the device automatically deletes the associated table rows. For example, if you delete an SRD that is associated with a Proxy Set, the device automatically deletes the Proxy Set.
- If you associate an SRD with a configuration entity in another table (i.e., other than the SRDs table), the device automatically configures certain parameters of the configuration entity according to the SRD or associated SRD. For example, if you add a rule in the IP-to-IP Routing table and you select a Routing Policy, the 'Source IP Group' and 'Destination IP Group' parameters list only IP Groups that are associated with the SRD to which the Routing Policy is assigned (and IP Groups belonging to a Shared SRD, if exists).
- If your configuration setup includes only a single SRD, the device automatically selects the SRD when adding related configuration entities. For example, when adding an IP Group, the single SRD is automatically selected in the Add Row dialog box.

19.3 Configuring SIP Interfaces

The SIP Interfaces table lets you configure up to 1,200 SIP Interfaces. A SIP Interface represents a Layer-3 network in your deployment environment, by defining a local, listening port number and type (e.g., UDP), and assigning an IP network interface for SIP signaling traffic. For example, if your deployment consists of an IP PBX in the LAN, a SIP Trunk in the WAN, and remote far-end users in the WAN, you would need to configure a SIP Interface for each of these SIP entities. You can also configure various optional features for the SIP Interface such as assigning it a Media Realm, blocking calls received on the SIP Interface from users not registered with the device, and enabling direct media.

Each SIP Interface can be associated with only one SRD. As the SRD configuration entity represents your VoIP deployment SIP network (Layer 5), you need to associate your SIP Interfaces with a specific SRD in order to represent your Layer-3 networks. For most

deployments (except multi-tenant deployments), your SRD represents your entire network and thus, only one SRD is required. The device provides a default SRD and in such scenarios where only a single SRD is required, your SIP Interfaces are automatically assigned to the default SRD. Therefore, there is no need to even handle SRD configuration entity.

Once configured, you can apply SIP Interfaces to calls, by assigning them to the following configuration entities in their respective tables:

- (Mandatory) Proxy Set to specify the SIP Interface for communication with the proxy server (i.e., IP Group). For more information, see "Configuring Proxy Sets" on page 341.
- Intrusion Detection System (IDS) for applying the IDS policy to a specific SIP Interface. For more information, see "Configuring IDS Policies" on page 164.
- SBC application:
 - IP-to-IP Routing rules for specifying the destination SIP Interface to where you want to route the call. For more information, see Configuring SBC IP-to-IP Routing Rules on page 470.
 - Classification rules for specifying the SIP Interface as a matching characteristic of the incoming call. This is especially useful for the single SRD-configuration topology, where each SIP Interface represents a Layer-3 network (SIP entity). Therefore, classification of calls to IP Groups (SIP entities) can be based on SIP Interface. For more information, see Configuring Classification Rules on page 461.
 - Admission Control rules to apply call admission control per SIP Interface. For more information, see "Configuring Admission Control" on page 457.



Note: The device terminates active calls associated with a SIP Interface in the following scenarios:

- If you delete the associated SIP Interface.
- If you edit any of the following fields of the associated SIP Interface: 'Application Type', 'UDP Port', 'TCP Port', 'TLS Port' or 'SRD' fields.
- If you edit or delete a network interface in the IP Interfaces table that is associated with the SIP Interface.

The following procedure describes how to configure SIP interfaces through the Web interface. You can also configure it through ini file (SIPInterface) or CLI (configure voip > sip-interface).

➤ **To configure a SIP Interface:**

1. Open the SIP Interfaces table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **SIP Interfaces**).
2. Click **New**; the following dialog box appears:

3. Configure a SIP Interface according to the parameters described in the table below.
4. Click **Apply**.

Table 19-5: SIP Interfaces table Parameter Descriptions

Parameter	Description
SRD srd [SIPInterface_SRDName]	<p>Assigns an SRD to the SIP Interface.</p> <p>If only one SRD is configured in the SRDs table, the SRD is assigned to the SIP Interface by default. If multiple SRDs are configured in the SRDs table, no value is defined and you must assign an SRD.</p> <p>To configure SRDs, see "Configuring SRDs" on page 311.</p> <p>Note:</p> <ul style="list-style-type: none"> ▪ The parameter is mandatory. ▪ You can assign the same SRD to multiple SIP Interfaces.
General	
Index [SIPInterface_Index]	<p>Defines an index for the new table row.</p> <p>Note: Each row must be configured with a unique index.</p>
Name interface-name [SIPInterface_InterfaceName]	<p>Defines an arbitrary name to easily identify the row.</p> <p>The valid value is a string of up to 21 characters. By default, if you do not configure a name, the device automatically assigns the name "SIPInterface_<row index>" (e.g., "SIPInterface_1" when added to Index 1).</p>
Topology Location topology-location [SIPInterface_TopologyLocation]	<p>Defines the display location of the SIP Interface in the Topology view.</p> <ul style="list-style-type: none"> ▪ [0] Down = (Default) The SIP Interface element is displayed on the lower border of the view. ▪ [1] Up = The SIP Interface element is displayed on the upper border of the view. <p>For more information on the Topology view, see "Building and</p>

Parameter	Description
	Viewing SIP Entities in Topology View" on page 350.
Network Interface network-interface [SIPInterface_NetworkInterface]	Assigns a Control-type IP network interface to the SIP Interface. By default, no value is defined. To configure network interfaces, see "Configuring IP Network Interfaces" on page 130. Note: The parameter is mandatory.
Application Type application-type [SIPInterface_ApplicationType]	Defines the application for which the SIP Interface is used. <ul style="list-style-type: none"> ▪ [2] SBC = SBC application.
UDP Port udp-port [SIPInterface_UDPPort]	Defines the device's listening and source port for SIP signaling traffic over UDP. The valid range is 1 to 65534. The default is 5060. Note: <ul style="list-style-type: none"> ▪ The port must be different from ports configured for RTP traffic (i.e., ports configured for Media Realms). For example, if the RTP port range is 6000 to 6999, the SIP port can either be less than 6000 or greater than 6999. ▪ The base UDP port number (BaseUDPPort parameter) for RTP traffic must be greater than the highest UDP port configured for a SIP Interface. For example, if your highest configured UDP port for a SIP Interface is 6060, you must configure the BaseUDPPort parameter to any value greater than 6060. For more information on base UDP port, see "Configuring RTP Base UDP Port" on page 187. ▪ Each SIP Interface must have a unique signaling port (i.e., no two SIP Interfaces can share the same port - no port overlapping).
TCP Port tcp-port [SIPInterface_TCPPort]	Defines the device's listening port for SIP signaling traffic over TCP. The valid range is 1 to 65534. The default is 5060. Note: <ul style="list-style-type: none"> ▪ The port must be different from ports configured for RTP traffic (i.e., ports configured for Media Realms). For example, if the RTP port range is 6000 to 6999, the SIP port can either be less than 6000 or greater than 6999. ▪ Each SIP Interface must have a unique signaling port (i.e., no two SIP Interfaces can share the same port - no port overlapping).
TLS Port tls-port [SIPInterface_TLSPort]	Defines the device's listening port for SIP signaling traffic over TLS. The valid range is 1 to 65534. The default is 5061. Note: <ul style="list-style-type: none"> ▪ The port must be different from ports configured for RTP traffic (i.e., ports configured for Media Realms). For example, if the RTP port range is 6000 to 6999, the SIP port can either be less than 6000 or greater than 6999. ▪ Each SIP Interface must have a unique signaling port (i.e., no two SIP Interfaces can share the same port - no port overlapping).

Parameter	Description
Encapsulating Protocol encapsulating-protocol [SIPInterface_EncapsulatingP rotocol]	Defines the type of incoming traffic (SIP messages) expected on the SIP Interface. <ul style="list-style-type: none"> ▪ [0] No Encapsulation (default) = Regular (non-WebSocket) traffic. ▪ [1] WebSocket = Traffic received on the SIP Interface is identified by the device as WebSocket signaling traffic (encapsulated by WebSocket frames). For outgoing traffic, the device encapsulates the traffic using the WebSocket protocol (frames) on the TCP/TLS ports. For more information on WebSocket, see SIP over WebSocket on page 526. Note: WebSocket encapsulation is not supported for UDP ports.
Enable TCP Keepalive tcp-keepalive-enable [SIPInterface_TCPKeepaliveE nable]	Enables the TCP Keep-Alive mechanism with the IP entity on this SIP Interface. TCP keep-alive 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. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable Note: To configure TCP keepalive, use the following ini file parameters: TCPKeepAliveTime, TCPKeepAliveInterval, and TCPKeepAliveRetry.
Used By Routing Server used-by-routing-server [SIPInterface_UsedByRouting Server]	Enables the SIP Interface to be used by a third-party routing server for call routing decisions. <ul style="list-style-type: none"> ▪ [0] Not Used (default) ▪ [1] Used For more information on the third-party routing server feature, see Centralized Third-Party Routing Server on page 266.
Classification	
Classification Failure Response Type classification_fail_response_ty pe [SIPInterface_ClassificationFa ilureResponseType]	Defines the SIP response code that the device sends if a received SIP request (OPTIONS, REGISTER, or INVITE) fails the SBC Classification process. 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). 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. Note: <ul style="list-style-type: none"> ▪ The parameter is applicable only if you configure the device to reject unclassified calls, which is done using the 'Unclassified Calls' parameter (see Configuring Classification Rules on page 461).

Parameter	Description
Pre Classification Manipulation Set ID preclassification-manset [SIPInterface_PreClassificationManipulationSet]	<ul style="list-style-type: none"> ▪ Assigns a Message Manipulation Set ID to the SIP Interface. This lets you apply SIP message manipulation rules on incoming SIP initiating-dialog request messages (not in-dialog), received on this SIP Interface, prior to the Classification process. By default, no Message Manipulation Set ID is defined. To configure Message Manipulation rules, see Configuring SIP Message Manipulation on page 362. Note: <ul style="list-style-type: none"> ▪ The Message Manipulation Set assigned to a SIP Interface that is associated with an outgoing call, is ignored. Only the Message Manipulation Set assigned to the associated IP Group is applied to the outgoing call. ▪ If both the SIP Interface and IP Group associated with the incoming call are assigned a Message Manipulation Set, the one assigned to the SIP Interface is applied first.
Media	
Media Realm media-realm-name [SIPInterface_MediaRealm]	Assigns a Media Realm to the SIP Interface. By default, no value is defined. To configure Media Realms, see "Configuring Media Realms" on page 303.
Direct Media intra-srd-media-anchoring [SIPInterface_SBCDirectMedia]	Enables direct media (RTP/SRTP) flow (i.e., no Media Anchoring) between endpoints associated with the SIP Interface. <ul style="list-style-type: none"> ▪ [0] Disable = (Default) Media Anchoring is employed, whereby the media stream traverses the device (and each leg uses a different coder or coder parameters). ▪ [1] Enable = No Media Anchoring. Media stream flows directly between endpoints (i.e., does not traverse the device - no Media Anchoring). ▪ [2] Enable when Same NAT = No Media Anchoring. Media stream flows directly between endpoints if they are located behind the same NAT. Note: <ul style="list-style-type: none"> ▪ If the parameter is enabled for direct media and the two endpoints belong to the same SIP Interface, calls cannot be established if the following scenario exists: <ol style="list-style-type: none"> a. One of the endpoints is defined as a foreign user (for example, "follow me service") b. and one endpoint is located on the WAN and the other on the LAN. The reason for the above is that in direct media, the device does not interfere in the SIP signaling such as manipulation of IP addresses, which is necessary for calls between LAN and WAN. ▪ To enable direct media for all calls, use the global parameter SBCDirectMedia. If enabled, even if the SIP Interface is disabled for direct media, direct media is employed for calls belonging to the SIP Interface. ▪ If you enable direct media for the SIP Interface, make sure that your Media Realm provides sufficient ports, as media may traverse the device for mid-call services (e.g., call transfer).

Parameter	Description
	<ul style="list-style-type: none"> For more information on direct media, see Direct Media on page 432.
Security	
TLS Context Name tls-context-name [SIPInterface_TLSTContext]	Assigns a TLS Context (SSL/TLS certificate) to the SIP Interface. The default TLS Context ("default" at Index 0) is assigned to the SIP Interface by default. Note: <ul style="list-style-type: none"> For incoming calls: The assigned TLS Context is used if no TLS Context is configured for the Proxy Set associated with the call or classification to an IP Group based on Proxy Set fails. For outgoing calls: The assigned TLS Context is used if no TLS Context is configured for the Proxy Set associated with the call. To configure TLS Contexts, see "Configuring SSL/TLS Certificates" on page 99.
TLS Mutual Authentication tls-mutual-auth [SIPInterface_TLSMutualAuth entication]	Enables TLS mutual authentication for the SIP Interface (when the device acts as a server). <ul style="list-style-type: none"> [0] Disable = Device does not request the client certificate for TLS connection on the SIP Interface. [1] Enable = Device requires receipt and verification of the client certificate to establish the TLS connection on the SIP Interface. By default, no value is defined and the SIPRequireClientCertificate global parameter setting is applied.
Message Policy message-policy [SIPInterface_MessagePolicy Name]	Assigns a SIP message policy to the SIP interface. To configure SIP Message Policy rules, see "Configuring SIP Message Policy Rules".
User Security Mode block-un-reg-users [SIPInterface_BlockUnRegUsers]	Defines the blocking (reject) policy for incoming SIP dialog-initiating requests (e.g., INVITE messages) from registered and unregistered users belonging to the SIP Interface. <ul style="list-style-type: none"> [-1] Not Configured = (Default) The corresponding parameter in the SRDs table (SRD_BlockUnRegUsers) of the SRD that is associated with the SIP Interface is applied. [0] Accept All = Accepts requests from registered and unregistered users. [1] Accept Registered Users = Accepts requests only from users registered with the device. Requests from users not registered are rejected. [2] Accept Registered Users from Same Source = Accepts requests only from registered users whose source address is the same as that registered with the device (during the REGISTER message process). All other requests are rejected. The device verifies whether the IP address and port are different only if the transport protocol is UDP; otherwise, the device verifies only the IP address. The verification is performed before any of the device's call handling processes (i.e., Classification, Manipulation and Routing). Note: <ul style="list-style-type: none"> The parameter is applicable only to calls belonging to User-type

Parameter	Description
	<p>IP Groups.</p> <ul style="list-style-type: none"> ▪ The feature is not applicable to REGISTER requests. ▪ The option, Accept Registered Users from Same Source [2] does not apply to registration refreshes. These requests are accepted even if the source address is different to that registered with the device. ▪ When the device rejects a call, it sends a SIP 500 "Server Internal Error" response to the user. In addition, it reports the rejection (Dialog establish failure - Classification failure) using the Intrusion Detection System (IDS) feature (see Configuring IDS Policies on page 164), by sending an SNMP trap. ▪ If you configure the parameter to any value other than default [-1], it overrides the corresponding parameter in the SRDs table (SRD_BlockUnRegUsersInterface) for the SRD associated with the SIP Interface.
<p>Enable Un-Authenticated Registrations enable-un-auth-registr [SIPInterface_EnableUnAuthenticatedRegistrations]</p>	<p>Enables the device to accept REGISTER requests and register them in its registration database from new users that have not been authenticated by a proxy/registrar server (due to proxy down) and thus, re-routed to a User-type IP Group.</p> <p>In normal operation scenarios in which the proxy server is available, the device forwards the REGISTER request to the proxy and if authenticated by the proxy (i.e., device receives a success response), the device adds the user to its registration database. The routing to the proxy is according to the SBC IP-to-IP Routing table where the destination is the proxy's IP Group. However, when the proxy is unavailable (e.g., due to network connectivity loss), the device can accept REGISTER requests from new users if a matching alternative routing rule exists in the SBC IP-to-IP Routing table where the destination is the user's User-type IP Group (i.e., call survivability scenarios) and if the parameter is enabled.</p> <ul style="list-style-type: none"> ▪ [-1] Not Configured = (Default) The corresponding parameter in the SRDs table (SRD_EnableUnAuthenticatedRegistrations) of the SRD associated with the SIP Interface is applied. ▪ [0] Disable = The device rejects REGISTER requests from new users that were not authenticated by a proxy server. ▪ [1] Enable = The device accepts REGISTER requests from new users even if they were not authenticated by a proxy server, and registers the user in its registration database. <p>Note:</p> <ul style="list-style-type: none"> ▪ Regardless of the parameter, the device always accepts registration refreshes from users that are already registered in its database. ▪ If configured to Disable or Enable, the parameter overrides the 'Enable Un-Authenticated Registrations' parameter settings of the SRD (in the SRDs table) that is associated with the SIP Interface.
<p>Max. Number of Registered Users max-reg-users [SIPInterface_MaxNumOfRegUsers]</p>	<p>Defines the maximum number of users belonging to the SIP Interface that can register with the device.</p> <p>By default, no value is defined (i.e., the number of allowed user registrations is unlimited).</p>

19.4 Configuring IP Groups

The IP Groups table lets you configure up to 1,500 IP Groups. An IP Group represents a SIP entity in the network with which the device communicates. This can be a server (e.g., IP PBX or ITSP) or 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 on page 341).

You can use IP Groups for the following:

- Classification of incoming SIP dialog-initiating requests (e.g., INVITE messages) to IP Groups based on Proxy Set. If the source address of the incoming SIP dialog is defined for a Proxy Set, the device assigns ("bonds") the SIP dialog to the IP Group associated with the Proxy Set. The feature is configured using the IP Groups table's 'Classify by Proxy Set' parameter. For more information and recommended security guidelines, see the parameter's description, later in this section.
- Representing the source and destination of the call in IP-to-IP Routing rules (see Configuring SBC IP-to-IP Routing Rules on page 470).
- SIP dialog registration and authentication (digest user/password) of specific IP Groups (Served IP Group, e.g., corporate IP-PBX) with other IP Groups (Serving IP Group, e.g., ITSP). This is configured in the Accounts table (see "Configuring Registration Accounts" on page 355).
- Included in routing decisions by a third-party routing server. If deemed necessary for routing, the routing server can even create an IP Group. For more information, see Centralized Third-Party Routing Server on page 266.

You can also apply the device's Quality of Experience feature to IP Groups:

- **Quality of Experience Profile:** Call quality monitoring based on thresholds for voice metrics (e.g., MOS) can be applied per IP Group. For example, if MOS is considered poor, calls belonging to this IP Group can be rejected. To configure Quality of Experience Profiles, see "Configuring Quality of Experience Profiles" on page 291.
- **Bandwidth Profile:** Bandwidth utilization thresholds can be applied per IP Group. For example, if bandwidth thresholds are crossed, the device can reject any new calls on this IP Group. To configure Bandwidth Profiles, see "Configuring Bandwidth Profiles" on page 296.



Note: If you delete an IP Group or modify the 'Type' or 'SRD' parameters, the device immediately terminates currently active calls that are associated with the IP Group. In addition, all users belonging to the IP Group are removed from the device's users database.

The following procedure describes how to configure IP Groups through the Web interface. You can also configure it through ini file (IPGroup) or CLI (configure voip > ip-group).

➤ To configure an IP Group:

1. Open the IP Groups table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **IP Groups**).
2. Click **New**; the following dialog box appears:

IP Groups

SRD #0 [DefaultSRD]

GENERAL	QUALITY OF EXPERIENCE
Index: 1	QoE Profile: -- View
Name:	Bandwidth Profile: -- View
Topology Location: Down	
Type: Server	MESSAGE MANIPULATION
Proxy Set: -- View	Inbound Message Manipulation Set: -1
IP Profile: -- View	Outbound Message Manipulation Set: -1
Media Realm: -- View	Message Manipulation User-Defined String 1:
SIP Group Name:	Message Manipulation User-Defined String 2:
Created By Routing Server:	
Used By Routing Server: Not Used	SBC REGISTRATION AND AUTHENTICATION

3. Configure an IP Group according to the parameters described in the table below.
4. Click **Apply**.

Table 19-6: IP Groups Table Parameter Descriptions

Parameter	Description
SRD srd-name [IPGroup_SRDName]	Assigns an SRD to the IP Group. If only one SRD is configured in the SRDs table, the SRD is assigned by default. If multiple SRDs are configured in the SRDs table, no value is assigned by default and you must assign one. To configure SRDs, see <i>Configuring SRDs</i> on page 311. Note: <ul style="list-style-type: none"> The parameter is mandatory. For the parameter to take effect, a device reset is required.
General	
Index [IPGroup_Index]	Defines an index for the new table row. Note: Each row must be configured with a unique index.
Name name [IPGroup_Name]	Defines an arbitrary name to easily identify the row. The valid value is a string of up to 40 characters. Note: Each row must be configured with a unique name.
Topology Location topology-location [IPGroup_TopologyLocation]	Defines the display location of the IP Group in the Topology view. <ul style="list-style-type: none"> [0] Down = (Default) The IP Group element is displayed on the lower border of the view. [1] Up = The IP Group element is displayed on the upper border of the view. For more information on the Topology view, see "Building and Viewing SIP Entities in Topology View" on page 350.
Type	Defines the type of IP Group:

Parameter	Description
type [IPGroup_Type]	<ul style="list-style-type: none"> ▪ [0] Server = Applicable when the destination address of the IP Group (e.g., ITSP, Proxy, IP-PBX, or Application server) is known. The address is configured by the Proxy Set that is associated with the IP Group. ▪ [1] User = 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). 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 registration database with the AOR and contacts of the users. 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. 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. 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. ▪ [2] Gateway = In scenarios where the device receives requests to and from a gateway representing multiple users. This IP Group type is necessary for any of the following scenarios: <ul style="list-style-type: none"> ✓ The IP Group cannot be defined as a Server-type since its address is initially unknown and therefore, a Proxy Set cannot be configured for it. ✓ The IP Group cannot be defined as a User-type 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. The IP address of the Gateway-type 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 (i.e., IP Group is registered with the device). 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. You can view the registration status of the Gateway-type IP Group in the 'GW Group Registered Status' field, and view the IP address of the IP Group in the 'GW Group Registered IP Address' field if it is registered with the device.

Parameter	Description
Proxy Set proxy-set-id [IPGroup_ProxySetName]	Assigns a Proxy Set to the IP Group. All INVITE messages destined to the IP Group are sent to the IP address configured for the Proxy Set. To configure Proxy Sets, see "Configuring Proxy Sets" on page 341. Note: <ul style="list-style-type: none"> ▪ The Proxy Set must be associated with the same SRD as that assigned to the IP Group. ▪ You can assign the same Proxy Set to multiple IP Groups. ▪ Proxy Sets are used for Server-type IP Groups, but may in certain scenarios also be used for User-type IP Groups. For example, this is required in deployments where the device mediates between an IP PBX and a SIP Trunk, and the SIP Trunk requires SIP registration for each user that requires service. In such a scenario, the device must register all the users to the SIP Trunk on behalf of the IP PBX. This is done by using the User Info table where each user is associated with the source IP Group (i.e., the IP PBX). To configure the User Info table, see SBC User Information for SBC User Database on page 593.
IP Profile ip-profile-name [IPGroup_ProfileName]	Assigns an IP Profile to the IP Group. By default, no value is defined. To configure IP Profiles, see "Configuring IP Profiles" on page 388.
Media Realm media-realm-name [IPGroup_MediaRealm]	Assigns a Media Realm to the IP Group. The Media Realm determines the UDP port range and maximum sessions on a specific interface for media traffic associated with the IP Group. By default, no value is defined. To configure Media Realms, see Configuring Media Realms on page 303. Note: <ul style="list-style-type: none"> ▪ For the parameter to take effect, a device reset is required. ▪ If you delete a Media Realm from the Media Realms table that is assigned to the IP Group, the parameter value reverts to None.
Contact User contact-user [IPGroup_ContactUser]	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. By default, no value is defined. Note: <ul style="list-style-type: none"> ▪ The parameter is applicable only to Server-type IP Groups. ▪ The parameter is overridden by the 'Contact User' parameter in the Accounts table (see "Configuring Registration Accounts" on page 355).
SIP Group Name sip-group-name [IPGroup_SIPGroupName]	Defines the SIP Request-URI host name in INVITE and REGISTER messages sent to the IP Group, or the host name in the From header of INVITE messages received from the IP Group. In other words, it replaces the original host name. The valid value is a string of up to 100 characters. By default, no value is defined.

Parameter	Description
	<p>Note:</p> <ul style="list-style-type: none"> ▪ If the parameter is not configured, the value of the global parameter, ProxyName is used instead (see "Configuring Proxy and Registration Parameters" on page 359). ▪ The parameter overrides inbound message manipulation rules that manipulate the host name in Request-URI, To, and/or From SIP headers. If you configure the parameter and you want to manipulate the host name in any of these SIP headers, you must apply your manipulation rule (Manipulation Set ID) to the IP Group as an Outbound Message Manipulation Set (see the IPGroup_OutboundManSet parameter), when the IP Group is the destination of the call. If you apply the Manipulation Set as an Inbound Message Manipulation Set (see the IPGroup_InboundManSet parameter), when the IP Group is the source of the call, the manipulation rule is overridden by the SIP Group Name parameter.
Created By Routing Server [IPGroup_CreatedByRoutingServer]	<p>(Read-only) Indicates whether the IP Group was created by a third-party routing server:</p> <ul style="list-style-type: none"> ▪ [0] No ▪ [1] Yes <p>For more information on the third-party routing server feature, see Centralized Third-Party Routing Server on page 266.</p>
Used By Routing Server used-by-routing-server [IPGroup_UsedByRoutingServer]	<p>Enables the IP Group to be used by a third-party routing server for call routing decisions.</p> <ul style="list-style-type: none"> ▪ [0] Not Used (default) ▪ [1] Used <p>For more information on the third-party routing server feature, see Centralized Third-Party Routing Server on page 266.</p>
Proxy Set Connectivity show voip proxy sets status [IPGroup_ProxySetConnectivity]	<p>(Read-only field) Displays the connectivity status with Server-type IP Groups. As the Proxy Set defines the address of the IP Group, the connectivity check (keep-alive) by the device is done to this address.</p> <ul style="list-style-type: none"> ▪ "NA": Functionality is not applicable due to one of the following: <ul style="list-style-type: none"> ✓ User-type IP Group. ✓ Server-type IP Group, but the keep-alive mechanism of its' associated Proxy Set is disabled. ▪ "Not Connected": Keep-alive failure (i.e., no connectivity with the IP Group). ▪ "Connected": Keep-alive success (i.e., connectivity with the IP Group). <p>The connectivity status is also displayed in the Topology View page (see "Building and Viewing SIP Entities in Topology View" on page 350).</p> <p>Note:</p> <ul style="list-style-type: none"> ▪ The feature is applicable only to Server-type IP Groups. ▪ To support the feature, you must enable the keep-alive mechanism of the Proxy Set that is associated with the IP Group (see "Configuring Proxy Sets" on page 341). ▪ If the Proxy Set is configured with multiple proxies (addresses) and at least one of them is "alive", the displayed status is

Parameter	Description
	<p>"Connected". To view the connected proxy server, see "Viewing Call Routing Status" on page 658.</p> <ul style="list-style-type: none"> The "Connected" status also applies to scenarios where the device rejects calls with the IP Group due to low QoE (e.g., low MOS), despite connectivity.
SBC General	
Classify By Proxy Set classify-by-proxy-set [IPGroup_ClassifyByProxySet]	<p>Enables classification of incoming SIP dialogs (INVITEs) to Server-type IP Groups based on Proxy Set (assigned using the IPGroup_ProxySetName parameter).</p> <ul style="list-style-type: none"> [0] Disable [1] Enable = (Default) The device searches the Proxy Sets table for a Proxy Set that is configured with the same source IP address as that of the incoming INVITE (if host name, then according to the dynamically resolved IP address list). If such a Proxy Set is found, the device classifies the INVITE as belonging to the IP Group associated with the Proxy Set. <p>Note:</p> <ul style="list-style-type: none"> The parameter is applicable only to Server-type IP Groups. For security, it is recommended to classify SIP dialogs based on Proxy Set only if the IP address of the IP Group is unknown. In other words, if the Proxy Set associated with the IP Group is configured with an FQDN. In such cases, the device classifies incoming SIP dialogs to the IP Group based on the DNS-resolved IP address. If the IP address is known, it is recommended to use a Classification rule instead (and disable the Classify by Proxy Set feature), where the rule is configured with not only the IP address, but also with SIP message characteristics to increase the strictness of the classification process (see Configuring Classification Rules on page 461). The reason for preferring classification based on Proxy Set when the IP address is unknown is that IP address forgery (commonly known as IP spoofing) is more difficult than malicious SIP message tampering and therefore, using a Classification rule without an IP address offers a weaker form of security. When classification is based on Proxy Set, the Classification table for the specific IP Group is ignored. If you have assigned the same Proxy Set to multiple IP Groups, disable the parameter and instead, use Classification rules to classify incoming SIP dialogs to these IP Groups. If the parameter is enabled, the device is unable to correctly classify incoming INVITEs to their appropriate IP Groups. Classification by Proxy Set occurs only if classification based on the device's registration database fails (i.e., the INVITE is not from a registered user).
SBC Operation Mode sbc-operation-mode [IPGroup_SBCOperationMode]	<p>Defines the device's operational mode for the IP Group.</p> <ul style="list-style-type: none"> [-1] Not Configured = (Default) [0] B2BUA = Device operates as a back-to-back user agent (B2BUA), changing the call identifiers and headers between the inbound and outbound legs. [1] Call Stateful Proxy = Device operates as a Stateful Proxy, passing the SIP message transparently between inbound and outbound legs. In other words, the same SIP dialog identifiers

Parameter	Description
	<p>(tags, Call-Id and CSeq) occur on both legs (as long as no other configuration disrupts the CSeq compatibleness).</p> <ul style="list-style-type: none"> [2] Microsoft Server = Operating mode for the One-Voice Resiliency feature, whereby the device is deployed together with Skype for Business-compatible IP Phones at small remote branch offices in a Microsoft® Skype for Business™ environment. <p>For more information on B2BUA and Stateful Proxy modes, see B2BUA and Stateful Proxy Operating Modes on page 422.</p> <p>Note: If configured, the parameter overrides the 'SBC Operation Mode' parameter in the SRDs table.</p>
<p>SBC Client Forking Mode enable-sbc-client-forking [IPGroup_EnableSBCClientForking]</p>	<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"> [0] 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. [1] Parallel = Sends the INVITE simultaneously to all contacts. The call is established with the first contact that answers. [2] 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. <p>Note: 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>
Advanced	
<p>Local Host Name local-host-name [IPGroup_ContactName]</p>	<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 sent to a specific IP Group, and the Contact header in SIP 18x and 200 OK responses for incoming INVITE messages received from a specific IP Group. The IP-to-Tel Routing table can be used to identify the source IP Group from where the INVITE message was received.</p> <p>If the parameter is not configured, these headers are populated with the device's dotted-decimal IP address of the network interface on which the message is sent.</p> <p>By default, no value is defined.</p> <p>Note: To ensure proper device handling, the parameter should be a valid FQDN.</p>
<p>UUI Format uui-format</p>	<p>Enables the generation of the Avaya UCID value, adding it to the outgoing INVITE sent to this IP Group.</p>

Parameter	Description
[IPGroup_UUIFormat]	<ul style="list-style-type: none"> ▪ [0] Disabled (default) ▪ [1] Enabled <p>This provides support for interworking with Avaya equipment by generating Avaya's UCID value in outgoing INVITE messages sent to Avaya's network. The device adds the UCID in the User-to-User SIP header.</p> <p>Avaya's UCID value has the following format (in hexadecimal): 00 + FA + 08 + node ID (2 bytes) + sequence number (2 bytes) + timestamp (4 bytes)</p> <p>This is interworked in to the SIP header as follows:</p> <p style="background-color: #f0f0f0; padding: 2px;">User-to-User: 00FA080019001038F725B3;encoding=hex</p> <p>Note: To define the Network Node Identifier of the device for Avaya UCID, use the 'Network Node ID' (NetworkNodeId) parameter.</p>
Always Use Src Address always-use-source-addr [IPGroup_AlwaysUseSourceAddr]	<p>Enables the device to always send SIP requests and responses, within a SIP dialog, to the source IP address received in the previous SIP message packet. This feature is especially useful in scenarios where the IP Group endpoints are located behind a NAT firewall (and the device is unable to identify this using its regular NAT mechanism).</p> <ul style="list-style-type: none"> ▪ [0] No = (Default) The device sends SIP requests according to the settings of the global parameter, SIPNatDetection. ▪ [1] Yes = The device sends SIP requests and responses to the source IP address received in the previous SIP message packet. <p>For more information on NAT traversal, see "Remote UA behind NAT" on page 144.</p>
SBC Advanced	
Source URI Input src-uri-input [IPGroup_SourceUriInput]	<p>Defines the SIP header in the incoming INVITE that is used for call matching characteristics based on source URIs.</p> <ul style="list-style-type: none"> ▪ [-1] Not Configured (default) ▪ [0] From ▪ [1] To ▪ [2] Request-URI ▪ [3] P-Asserted - First Header ▪ [4] P-Asserted - Second Header ▪ [5] P-Preferred ▪ [6] Route ▪ [7] Diversion ▪ [8] P-Associated-URI ▪ [9] P-Called-Party-ID ▪ [10] Contact ▪ [11] Referred-by <p>Note:</p> <ul style="list-style-type: none"> ▪ The parameter is applicable only when classification is done according to the Classification table. ▪ If the configured SIP header does not exist in the incoming INVITE message, the classification of the message to a source IP Group fails. ▪ If the device receives an INVITE as a result of a REFER request

Parameter	Description
	<p>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 the parameter setting.</p>
<p>Destination URI Input dst-uri-input [IPGroup_DestUriInput]</p>	<p>Defines the SIP header in the incoming INVITE to use as a call matching characteristic based on destination URIs. The parameter is used for classification and routing purposes. The device first uses the parameter's settings as a matching characteristic (input) to classify the incoming INVITE to an IP Group (source IP Group) in the Classification table. Once classified, the device uses the parameter for routing the call. For example, if set to To, the URI in the To header of the incoming INVITE is used as a matching characteristic for classifying the call to an IP Group in the Classification table. Once classified, the device uses the URI in the To header as the destination.</p> <ul style="list-style-type: none"> ▪ [-1] Not Configured (default) ▪ [0] From ▪ [1] To ▪ [2] Request-URI ▪ [3] P-Asserted - First Header ▪ [4] P-Asserted - Second Header ▪ [5] P-Preferred ▪ [6] Route ▪ [7] Diversion ▪ [8] P-Associated-URI ▪ [9] P-Called-Party-ID ▪ [10] Contact ▪ [11] Referred-by <p>Note:</p> <ul style="list-style-type: none"> ▪ The parameter is applicable only when classification is done according to the Classification table. ▪ If the configured SIP header does not exist in the incoming INVITE message, the classification of the message to a source IP Group fails. ▪ If the device receives an INVITE as a result of a REFER request or a 3xx response, 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 the parameter setting.
<p>SIP Connect sip-connect [IPGroup_SIPConnect]</p>	<p>Defines the IP Group as a registered server that represents multiple users. The device saves registrations received from the IP Group, with the IP address as a key in its registration database. The device classifies incoming SIP dialog requests (e.g., INVITEs) from the IP Group according to the received IP address. For requests routed to the IP Group users, the device replaces the Request-URI header with the incoming To header (which contains the remote phone number).</p> <ul style="list-style-type: none"> ▪ [0] No (default)

Parameter	Description
	<ul style="list-style-type: none"> ▪ [1] Yes <p>Note: The parameter is applicable only to User-type IP Groups.</p>
SBC PSAP Mode sbc-psap-mode [IPGroup_SBCPSAPMode]	Enables E9-1-1 emergency call routing in a Microsoft Skype for Business environment. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable For more information, see E9-1-1 Support for Microsoft Skype for Business on page 277.
Route Using Request URI Port use-requri-port [IPGroup_SBCRouteUsingRequestURIPort]	Enables the device to use the port indicated in the Request-URI of the incoming message as the destination port when routing the message to the IP Group. The device uses the IP address (and not port) that is configured for the Proxy Set associated with the IP Group. The parameter thus allows the device to route calls to the same server (IP Group), but different port. <ul style="list-style-type: none"> ▪ [0] Disable = (Default) The port configured for the associated Proxy Set is used as the destination port. ▪ [1] Enable = The port indicated in the Request-URI of the incoming message is used as the destination port.
DTLS Context dtls-context [IPGroup_DTLSContext]	Assigns a TLS Context (certificate) to the IP Group, which is used for DTLS sessions (handshakes) with the IP Group. By default, no value is defined. To configure TLS Contexts, see Configuring TLS Certificate Contexts on page 99.
Keep Original Call-ID sbc-keep-call-id [IPGroup_SBCKeepOriginalCallID]	Enables the device to use the same call identification (SIP Call-ID header value) received in incoming messages for the call identification in outgoing messages. The call identification value is contained in the SIP Call-ID header. <ul style="list-style-type: none"> ▪ [0] No = (Default) The device creates a new Call-ID value for the outgoing message. ▪ [1] Yes = The device uses the same Call-ID value received in the incoming message for the Call-ID in the outgoing message. <p>Note: When the device sends an INVITE as a result of a REFER/3xx termination, the device always creates a new Call-ID value and ignores the parameter's settings.</p>
Dial Plan sbc-dial-plan-name [IPGroup_SBCDialPlanName]	Assigns a Dial Plan to the IP Group. The device searches the Dial Plan for a dial plan rule that matches the source number and if not found, for a rule that matches the destination number. If a matching dial plan rule is found, the rule's tag is used in the routing and/or manipulation processes as source and/or destination tags. To configure Dial Plans, see Configuring Dial Plans on page 503.
Call Setup Rules Set ID call-setup-rules-set-id [IPGroup_CallSetupRulesSetId]	Assigns a Call Setup Rule Set ID to the IP Group. The device runs the Call Setup rule immediately before the routing stage (i.e., only after the classification and manipulation stages). By default, no value is assigned. To configure Call Setup Rules, see Configuring Call Setup Rules on page 370.
Quality of Experience	

Parameter	Description
QoE Profile qoe-profile [IPGroup_QOEProfile]	Assigns a Quality of Experience Profile rule. By default, no value is defined. To configure Quality of Experience Profiles, see "Configuring Quality of Experience Profiles" on page 291.
Bandwidth Profile bandwidth-profile [IPGroup_BWProfile]	Assigns a Bandwidth Profile rule. By default, no value is defined. To configure Bandwidth Profiles, see "Configuring Bandwidth Profiles" on page 296.
Message Manipulation	
Inbound Message Manipulation Set inbound-mesg-manipulation-set [IPGroup_InboundManSet]	Assigns a Message Manipulation Set (rule) to the IP Group for SIP message manipulation on the inbound leg. By default, no value is defined. To configure Message Manipulation rules, see Configuring SIP Message Manipulation on page 362. Note: <ul style="list-style-type: none"> The IPGroup_SIPGroupName parameter overrides inbound message manipulation rules (assigned to the IPGroup_InboundManSet parameter) that manipulate the host name in Request-URI, To, and/or From SIP headers. If you want to manipulate the host name using message manipulation rules in any of these SIP headers, you must apply your manipulation rule (Manipulation Set ID) to the IP Group as an Outbound Message Manipulation Set (see the IPGroup_OutboundManSet parameter), when the IP Group is the destination of the call.
Outbound Message Manipulation Set outbound-mesg-manipulation-set [IPGroup_OutboundManSet]	Assigns a Message Manipulation Set (rule) to the IP Group for SIP message manipulation on the outbound leg. By default, no value is defined. To configure Message Manipulation rules, see "Configuring SIP Message Manipulation" on page 362. Note: If you assign a Message Manipulation Set ID that includes rules for manipulating the host name in the Request-URI, To, and/or From SIP headers, the parameter overrides the IPGroup_SIPGroupName parameter.
Message Manipulation User-Defined String 1 msg-man-user-defined-string1 [IPGroup_MsgManUserDef1]	Defines a value for the SIP user part that can be used in Message Manipulation rules configured in the Message Manipulations table. The Message Manipulation rule obtains this value from the IP Group, by using the following syntax: <pre>param.ipg.<src dst>.user-defined.<0>.</pre> The valid value is a string of up to 30 characters. By default, no value is defined. To configure Message Manipulation rules, see "Configuring SIP Message Manipulation" on page 362.
Message Manipulation User-Defined String 2 msg-man-user-defined-string2 [IPGroup_MsgManUserDef2]	Defines a value for the SIP user part that can be used in Message Manipulation rules configured in the Message Manipulations table. The Message Manipulation rule obtains this value from the IP Group, by using the following syntax: param.ipg.<src dst>.user-defined.<1>.

Parameter	Description
	The valid value is a string of up to 30 characters. By default, no value is defined. To configure Message Manipulation rules, see "Configuring SIP Message Manipulation" on page 362.
SBC Registration and Authentication	
Max. Number of Registered Users max-num-of-reg-users [IPGroup_MaxNumOfRegUsers]	Defines the maximum number of users in this IP Group that can register with the device. The default is -1, meaning that no limitation exists for registered users. Note: The parameter is applicable only to User-type IP Groups.
Registration Mode registration-mode [IPGroup_RegistrationMode]	Defines the registration mode for the IP Group: <ul style="list-style-type: none"> ▪ [0] User Initiates Registration (default) ▪ [1] SBC Initiates Registration = Used when the device serves as a client (e.g., with an IP PBX). This functions only with the User Info file. ▪ [2] Registrations not Needed = The device adds users to its database in active state.
Authentication Mode authentication-mode [IPGroup_AuthenticationMode]	Defines the authentication mode. <ul style="list-style-type: none"> ▪ [0] User Authenticates = (Default) The device does not handle the authentication, but simply forwards the authentication messages between the SIP user agents. ▪ [1] 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., username and password) according to one of the following: 1)Account configured in the Accounts 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). For more information on Accounts, see Configuring Registration Accounts on page 355. ▪ [2] SBC as Server = The device acts as an Authentication server: <ul style="list-style-type: none"> ✓ Authenticates SIP clients, using the usernames and passwords in the User Information table (see SBC User Information for SBC User Database on page 593). This is applicable only to User-type IP Groups. ✓ Authenticates SIP servers. This is applicable only to Server-type IP Groups.
Authentication Method List authentication-method-list [IPGroup_MethodList]	Defines SIP methods received from the IP Group that must be challenged by the device when the device acts as an Authentication server. If no methods are configured, the device doesn't challenge any methods. By default, no value is defined. To define multiple SIP methods, use the backslash (\) to separate each method (e.g., INVITE\REGISTER). Note: The parameter is applicable only if the 'Authentication Mode' parameter is set to SBC as Server [2].
Username	Defines the shared username for authenticating the IP Group,

Parameter	Description
username [IPGroup_Username]	<p>when the device acts as an Authentication server.</p> <p>The valid value is a string of up to 51 characters. By default, no username is defined.</p> <p>Note:</p> <ul style="list-style-type: none"> The parameter is applicable only to Server-type IP Groups and when the 'Authentication Mode' parameter is set to SBC as Server (i.e., authentication of servers). To specify the SIP request types (e.g., INVITE) that must be challenged by the device, use the 'Authentication Method List' parameter.
Password password IPGroup_Password]	<p>Defines the shared password for authenticating the IP Group, when the device acts as an Authentication server.</p> <p>The valid value is a string of up to 51 characters. By default, no password is defined.</p> <p>Note:</p> <ul style="list-style-type: none"> The parameter is applicable only to Server-type IP Groups and when the 'Authentication Mode' parameter is set to SBC as Server (i.e., authentication of servers). To specify the SIP request types (e.g., INVITE) that must be challenged by the device, use the 'Authentication Method List' parameter.
GW Group Status	
GW Group Registered IP Address	<p>(Read-only field) Displays the IP address of the IP Group entity (gateway) if registered with the device; otherwise, the field is blank.</p> <p>Note: The field is applicable only to Gateway-type IP Groups (i.e., the 'Type' parameter is configured to Gateway).</p>
GW Group Registered Status	<p>(Read-only field) Displays whether the IP Group entity (gateway) is registered with the device ("Registered" or "Not Registered").</p> <p>Note: The field is applicable only to Gateway-type IP Groups (i.e., the 'Type' parameter is configured to Gateway).</p>

19.5 Configuring Proxy Sets

The Proxy Sets table lets you configure up to 1500 Proxy Sets. A Proxy Set defines the address and transport type (e.g., UDP or TCP) of a SIP server (e.g., SIP proxy and SIP registrar server). The Proxy Set represents the destination (address) of the IP Group configuration entity. Each Proxy Set can be configured with up to 10 addresses configured as an IP address and/or DNS host name (FQDN), enabling you to implement load balancing and redundancy (Proxy Hot-Swap feature) between multiple servers. If you configure the address as an FQDN, you can configure the method (A-record DNS, SRV, or NAPTR) for resolving the domain name to an IP address. The device supports up to 30 DNS-resolved IP addresses. (If the DNS resolution provides more than this number, the device uses the first 30 IP addresses in the received list and ignores the rest.) Each Proxy Set can be assigned a specific SSL/TLS certificate the (TLS Context), enabling you to use different TLS certificates per SIP entity (IP Group). In addition, each Proxy Set must be assigned a SIP Interface (and SRD), which determines, amongst others, the device's local network interface through which communication with the Proxy Set is done.

To use a configured Proxy Set, you need to assign it to an IP Group in the IP Groups table (see "Configuring IP Groups" on page 329). When the device sends INVITE messages to an IP Group, it sends it to the address configured for the Proxy Set. You can assign the same Proxy Set to multiple IP Groups (belonging to the same SRD).

You can also enable the device to classify incoming SBC SIP dialogs to IP Groups, based on Proxy Set. If the source address of the incoming SIP dialog is the same as the address of a Proxy Set, the device classifies the SIP dialog as belonging to the IP Group that is associated with the Proxy Set.



Note:

- It is recommended to classify incoming SIP dialogs to IP Groups, based on the Classification table (see Configuring Classification Rules on page 461) instead of based on Proxy Set.
- You can view the device's connectivity status with proxy servers in the Tel-to-IP Routing table, for Tel-to-IP routing rules whose destination is an IP Group that is associated with a Proxy Set. The status is only displayed for Proxy Sets enabled with the Proxy Keep-Alive feature.

The Proxy Set is configured using two tables, one a "child" of the other:

- Proxy Sets table: Defines the attributes of the Proxy Set such as associated SIP Interface and redundancy features - ini file parameter, ProxySet or CLI command, `configure voip > proxy-set`
- Proxy Set Address table ("child"): Defines the addresses of the Proxy Set - table ini file parameter, ProxyIP or CLI command, `configure voip > proxy-ip > proxy-set-id`

➤ **To configure a Proxy Set:**

1. Open the Proxy Sets table (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Proxy Sets**).
2. Click **New**; the following dialog box appears:

3. Configure a Proxy Set according to the parameters described in the table below.
4. Click **Apply**.
5. Select the index row of the Proxy Set that you added, and then click the **Proxy Address** link located below the table; the Proxy Address table opens.
6. Click **New**; the following dialog box appears:

Figure 19-10: Proxy Address Table - Add Dialog Box

7. Configure the address of the Proxy Set according to the parameters described in the table below.
8. Click **Apply**.

Table 19-7: Proxy Sets Table and Proxy Address Table Parameter Description

Parameter	Description
SRD	Assigns an SRD to the Proxy Set.

Parameter	Description
voip-network proxy-set > srd-id [ProxySet_SRDName]	<p>Note:</p> <ul style="list-style-type: none"> ▪ The parameter is mandatory and must be configured first before you can configure the other parameters in the table. ▪ To configure SRDs, see Configuring SRDs on page 311.
General	
Index configure voip > voip-network proxy-set [ProxySet_Index]	Defines an index number for the new table row. <p>Note: Each row must be configured with a unique index.</p>
Name proxy-name [ProxySet_ProxyName]	Defines an arbitrary name to easily identify the row. The valid value is a string of up to 20 characters. <p>Note: Each row must be configured with a unique name.</p>
SBC IPv4 SIP Interface sbcipv4-sip-int-name [ProxySet_SBCIPv4SIPInterfaceName]	Assigns an IPv4-based SIP Interface for SBC calls to the Proxy Set. <p>Note:</p> <ul style="list-style-type: none"> ▪ At least one SIP Interface must be assigned to the Proxy Set. ▪ The parameter appears only if you have configured a network interface with an IPv4 address in the IP Interfaces table (see Configuring IP Network Interfaces on page 130). ▪ To configure SIP Interfaces, see "Configuring SIP Interfaces" on page 321.
SBC IPv6 SIP Interface sbcipv6-sip-int-name [ProxySet_SBCIPv6SIPInterfaceName]	Assigns an IPv6-based SIP Interface for SBC calls to the Proxy Set. <p>Note:</p> <ul style="list-style-type: none"> ▪ At least one SIP Interface must be assigned to the Proxy Set. ▪ The parameter appears only if you have configured a network interface with an IPv6 address in the IP Interfaces table.
TLS Context Index tls-context-index [ProxySet_TLSContextName]	Assigns a TLS Context (SSL/TLS certificate) to the Proxy Set. By default, no TLS Context is assigned. If you assign a TLS Context, the TLS Context is used as follows: <ul style="list-style-type: none"> ▪ Incoming calls: If the 'Transport Type' parameter (in this table) is set to TLS and the incoming call is successfully classified to an IP Group based on the Proxy Set, this TLS Context is used. If the 'Transport Type' parameter is set to UDP or classification to this Proxy Set fails, the TLS Context is not used. Instead, the device uses the TLS Context configured for the SIP Interface (see "Configuring SIP Interfaces" on page 321) used for the call; otherwise, the default TLS Context (ID 0) is used. ▪ Outgoing calls: If the 'Transport Type' parameter is set to TLS and the outgoing call is sent to an IP Group that is associated with this Proxy Set, this TLS Context is used. Instead, the device uses the TLS Context

Parameter	Description
	<p>configured for the SIP Interface used for the call; otherwise, the default TLS Context (ID 0) is used. If the 'Transport Type' parameter is set to UDP, the device uses UDP to communicate with the proxy and no TLS Context is used.</p> <p>To configure TLS Contexts, see "Configuring TLS Certificate Contexts" on page 99.</p>
Keep Alive	
<p>Proxy Keep-Alive proxy-enable-keep-alive [ProxySet_EnableProxyKeepAlive]</p>	<p>Enables the device's Proxy Keep-Alive feature, which checks communication with the proxy server.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default). ▪ [1] Using OPTIONS = Enables the Proxy Keep-Alive feature using SIP OPTIONS messages. The device sends an OPTIONS message every user-defined interval, configured by the 'Proxy Keep-Alive Time' parameter (in this table). If the device receives a SIP response code that is configured in the 'Keep-Alive Failure Responses' parameter (in this table), the device considers the proxy as down. You can also configure whether to use the device's IP address or string name ("gateway name") in the OPTIONS message (see the UseGatewayNameForOptions parameter). ▪ [2] Using REGISTER = Enables the Proxy Keep-Alive feature using SIP REGISTER messages. The device sends a REGISTER message every user-defined interval, configured by the SBCProxyRegistrationTime parameter. Any SIP response from the proxy - success (200 OK) or failure (4xx response) - is considered as if the proxy is "alive". If the proxy does not respond to INVITE messages sent by the device, the proxy is considered as down (offline). <p>If you enable the Proxy Keep-Alive feature, the device can operate with multiple proxy servers (addresses) for redundancy and load balancing (see the 'Proxy Load Balancing Method' parameter).</p> <p>Note:</p> <ul style="list-style-type: none"> ▪ For Survivability mode for User-type IP Groups, the parameter must be enabled (1 or 2). ▪ If the parameter is enabled and the proxy uses the TCP/TLS transport type, you can enable CRLF Keep-Alive feature, using the UsePingPongKeepAlive parameter.
<p>Proxy Keep-Alive Time proxy-keep-alive-time [ProxySet_ProxyKeepAliveTime]</p>	<p>Defines the interval (in seconds) between keep-alive messages sent by the device when the Proxy Keep-Alive feature is enabled (see the 'Proxy Keep-Alive' parameter in this table).</p> <p>The valid range is 5 to 2,000,000. The default is 60.</p> <p>Note: The parameter is applicable only if the 'Proxy Keep-Alive' parameter is set to Using Options.</p>
<p>Keep-Alive Failure Responses</p>	<p>Defines SIP response codes that if any is received in response to a keep-alive message using SIP OPTIONS,</p>

Parameter	Description
keepalive-fail-resp [ProxySet_KeepAliveFailureResp]	<p>the device considers the proxy as down.</p> <p>Up to three response codes can be configured, where each code is separated by a comma (e.g., 407,404). By default, no response code is defined. If no response code is configured, or if response codes received are not those configured, the proxy is considered "alive".</p> <p>Note: The SIP 200 response code is not supported for this feature.</p>
Redundancy	
Redundancy Mode proxy-redundancy-mode [ProxySet_ProxyRedundancyMode]	<p>Determines whether the device switches from a redundant proxy to the primary proxy when the primary proxy becomes available again.</p> <ul style="list-style-type: none"> ▪ [-1] = Not configured (Default). Proxy redundancy method is according to the settings of the global parameter, ProxyRedundancyMode. ▪ [0] Parking = The device continues operating with the redundant (now active) proxy even if the primary proxy returns to service. If the redundant proxy subsequently becomes unavailable, the device operates with the next configured redundant proxy. ▪ [1] Homing = The device always attempts to operate with the primary proxy. The device switches back to the primary proxy whenever it becomes available. <p>Note:</p> <ul style="list-style-type: none"> ▪ To enable this functionality, you must also enable the Proxy Keep-Alive feature (see the 'Proxy Keep-Alive' parameter in this table). ▪ The Homing option can only be used if the 'Proxy Keep-Alive' parameter is set to Using Options.
Proxy Hot Swap is-proxy-hot-swap [ProxySet_IsProxyHotSwap]	<p>Enables the Proxy Hot-Swap feature, whereby the device switches to a redundant proxy upon a failure in the primary proxy (no response is received).</p> <ul style="list-style-type: none"> ▪ [0] Disable = (Default) Disables the Proxy Hot-Swap feature. If a failure occurs in the primary proxy, the device does not connect with any other address (proxy) configured for the Proxy Set. ▪ [1] Enable = The device sends the SIP INVITE/REGISTER message to the first address listed in the Proxy Address table configured for the Proxy Set. If a SIP response is received and this response code is defined in the 'Keep-Alive Failure Responses' parameter (in this table), the device assumes the proxy is down and sends the message again; otherwise, the device assumes the proxy is up and does not send the message again. Each time a defined response code is received, the device re-sends the message. This can occur until a user-defined maximum number of retransmissions (see the HotSwapRtx parameter), after which the device sends the same message to the next address in the list, and so on. If there is no response from any of the Proxies, the device goes through the list again until a "live" proxy is located.

Parameter	Description
Proxy Load Balancing Method proxy-load-balancing-method [ProxySet_ProxyLoadBalancingMethod]	Enables load balancing between proxy servers of the Proxy Set. <ul style="list-style-type: none"> ▪ [0] Disable = (Default) Disables proxy load balancing. ▪ [1] Round Robin = A list of all possible proxy IP addresses is compiled. This list includes all IP addresses of the Proxy Set after DNS resolutions (including NAPTR and SRV, if configured). After this list is compiled, the Proxy Keep-Alive feature (enabled by the 'Proxy Keep-Alive' and 'Proxy Keep-Alive Time' parameters in this table) tags each entry as "offline" or "online". Load balancing is only performed on proxy servers that are tagged as "online". All outgoing messages are equally distributed across the list of IP addresses. REGISTER messages are also distributed unless a RegistrarIP is configured. The IP address list is refreshed every user-defined interval (see the ProxyIPListRefreshTime parameter). If a change in the order of the IP address entries in the list occurs, all load statistics are erased and balancing starts over again. ▪ [2] Random Weights = The outgoing requests are not distributed equally among the Proxies. The weights are received from the DNS server, 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. Random Weights Load Balancing is not used in the following scenarios: <ul style="list-style-type: none"> ✓ More than one IP address has been configured for the Proxy Set. ✓ The proxy address is not configured as an FQDN (only IP address). ✓ SRV is disabled (see the DNSQueryType parameter). ✓ The SRV response includes several records with a different Priority value.
Advanced	
Classification Input classification-input [ProxySet_ClassificationInput]	Defines how the device classifies incoming IP calls to the Proxy Set. <ul style="list-style-type: none"> ▪ [0] IP Address Only = (Default) Classifies calls to the Proxy Set according to IP address only. ▪ [1] IP Address, Port & Transport Type = Classifies calls to the Proxy Set according to IP address, port, and transport type. Note: <ul style="list-style-type: none"> ▪ The parameter is applicable only if the IP Groups table's parameter, 'Classify by Proxy Set' is set to Enable (see Configuring IP Groups on page 329). ▪ If more than one Proxy Set is configured with the same IP address and associated with the same SIP Interface, the device may classify and route the SIP dialog to an incorrect IP Group. In such a scenario, a warning is generated in the Syslog message. However, if some


Parameter	Description
	<p>Proxy Sets are configured with the same IP address but different ports (e.g., 10.1.1.1:5060 and 10.1.1.1:5070) and the parameter is configured to IP Address, Port & Transport Type, classification to the correct IP Group is achieved. Therefore, when classification is by Proxy Set, pay attention to the configured IP addresses and this parameter. When more than one Proxy Set is configured with the same IP address, the device selects the matching Proxy Set in the following order:</p> <ul style="list-style-type: none"> ✓ Selects the Proxy Set whose IP address, port, and transport type match the source of the incoming dialog (regardless of the settings of this parameter). ✓ If no match is found for above, it selects the Proxy Set whose IP address and transport type match the source of the incoming dialog (if the parameter is configured to IP Address Only). ✓ If no match is found for above, it selects the Proxy Set whose IP address match the source of the incoming dialog (if the parameter is configured to IP Address Only).
DNS Resolve Method dns-resolve-method [ProxySet_DNSResolveMethod]	<p>Defines the DNS query record type for resolving the proxy server's host name (FQDN) into an IP address(es).</p> <ul style="list-style-type: none"> ▪ [-1] = Not configured. DNS resolution method is according to the settings of the global parameter, ProxyDNSQueryType. ▪ [0] A-Record = (Default) DNS A-record query is used to resolve DNS to IP addresses. ▪ [1] SRV = If the proxy address is configured with a domain name without a port (e.g., domain.com), an SRV query is done. The SRV query returns the host names (and their weights). The device then performs DNS A-record queries per host name (according to the received weights). If the configured proxy address contains a domain name with a port (e.g., domain.com:5080), the device performs a regular DNS A-record query. ▪ [2] NAPTR = NAPTR query is done. If successful, an SRV query is sent according to the information received in the NAPTR response. If the NAPTR query fails, an SRV query is done according to the configured transport type. If the configured proxy address contains a domain name with a port (e.g., domain.com:5080), the device performs a regular DNS A-record query. If the transport type is configured for the proxy address, a NAPTR query is not performed. ▪ [3] Microsoft Skype for Business = SRV query as required by Microsoft when the device is deployed in a Microsoft Skype for Business environment. The device sends a special SRV query to the DNS server according to the transport protocol configured in the 'Transport Type' parameter (described later in this section): <ul style="list-style-type: none"> ✓ TLS: "_sipinternaltls_tcp.<domain>" and "_sip_tls.<domain>". For example, if the configured domain name (in the 'Proxy Address' parameter) is "ms-server.com", the device queries for "_sipinternaltls_tcp.ms-server.com" and

Parameter	Description
	<p>"_sip_tls.ms-server.com".</p> <ul style="list-style-type: none"> ✓ TCP: "_sipinternal_tcp.<domain>" and "_sip_tcp.<domain>". ✓ Undefined: "_sipinternaltls_tcp.<domain>", "_sipinternal_tcp.<domain>", "_sip_tls.<domain>" and "_sip_tcp.<domain>". <p>The SRV query returns the host names (and their weights). The device then performs DNS A-record queries per host name (according to the received weights) to resolve into IP addresses.</p> <p>Note: An SRV query can return up to four host names. For each host name, the subsequent DNS A-record query can resolve into up to 15 IP addresses. However, the device supports up to 30 DNS-resolved IP addresses. If the device receives more than this number of IP addresses, it uses the first 30 IP addresses in the received list and ignores the rest.</p>
Proxy Address Table	
Index proxy-ip-index [ProxyIp_ProxyIpIndex]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
Proxy Address proxy-address [ProxyIp_IpAddress]	Defines the address of the proxy. Up to 10 addresses can be configured per Proxy Set. 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 using the following format: <ul style="list-style-type: none"> ▪ IPv4 address: <IP address>:<port> (e.g., 201.10.8.1:5060) ▪ IPv6 address: <[IPV6 address]>:<port> (e.g., [2000::1:200:200:86:14]:5060) <p>Note: You can configure the device to use the port indicated in the Request-URI of the incoming message, instead of the port configured for the parameter. To enable this, use the IPGroup_SBCRouteUsingRequestURIPort parameter for the IP Group that is associated with the Proxy Set (Configuring IP Groups on page 329).</p>
Transport Type transport-type [ProxyIp_TransportType]	Defines the transport type for communicating with the proxy. <ul style="list-style-type: none"> ▪ [0] UDP ▪ [1] TCP ▪ [2] TLS ▪ [-1] = (Default) The transport type is according to the settings of the global parameter, SIPTransportType.

19.6 Building and Viewing SIP Entities in Topology View

The Topology view lets you easily build and view your main SIP entities, including IP Groups, SIP Interfaces, and Media Realms. The Topology view graphically displays these entities and the associations between them, giving you a better understanding of your SIP topology and configuration. The Topology view also lets you configure additional SIP settings that are important to your deployment such as routing and manipulation. You can use the Topology view as an alternative to configuring the entities in their respective Web pages or you can use it in combination.

➤ **To access the Topology view:**

- Click the Topology View home  icon (**Setup** menu > **Signaling & Media** tab > **Topology View**).

The main areas of the Topology view is shown below and described in the subsequent table.

Figure 19-11: Areas of Topology View

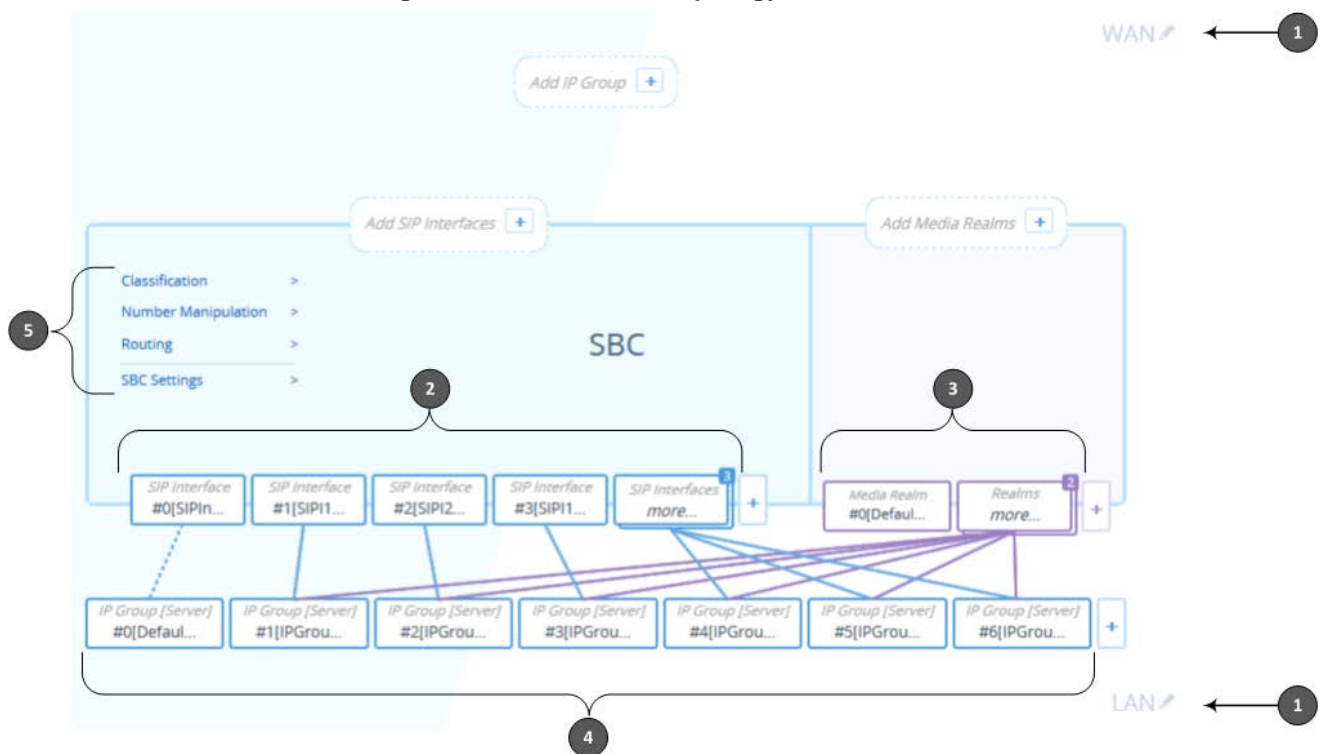

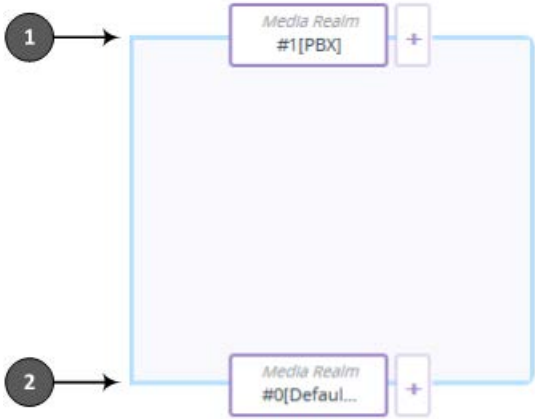

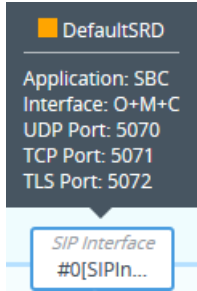










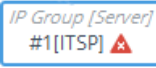


Table 19-8: Description of Topology View

Item #	Description
1	<p>Demarcation area of the topology. By default, the Topology view displays the following names to represent the different demarcations of your voice configuration:</p> <ul style="list-style-type: none"> ■ "WAN": Indicates the external network side ■ "LAN": Indicates the internal network (e.g., inside the Enterprise) <p>To modify a demarcation name, do the following:</p> <ol style="list-style-type: none"> 1 Click the demarcation name; the name becomes editable in a text box, as shown in the example below:

Item #	Description
	<p data-bbox="742 293 976 331">  </p> <p data-bbox="327 342 1374 405"> 2 Type a name as desired, and then click anywhere outside of the text box to apply the name. </p> <p data-bbox="327 414 1407 600"> You can use demarcation to visually separate your voice network to provide a clearer understanding of your topology. This is especially useful for IP Groups, SIP Interfaces, and Media Realms, where you can display them on the top or bottom border of the Topology view (as shown in the figure below for callouts #1 and #2, respectively). For example, on the top border you can position all entities relating to WAN, and on the bottom border all entities relating to LAN. </p> <p data-bbox="555 611 1171 645"> Figure 19-12: Display Location in Topology View </p> <div data-bbox="592 667 1129 1084" style="text-align: center;">  </div> <p data-bbox="327 1115 1390 1205"> By default, configuration entities are displayed on the bottom border. To define the position, use the 'Topology Location' parameter when configuring the entity, where Down is the bottom border and Up the top border: </p> <p data-bbox="518 1220 1206 1254"> Figure 19-13: Configuration Postion in Topology View </p> <div data-bbox="502 1265 1220 1310" style="text-align: center;"> <p>Topology Location <input data-bbox="774 1265 1220 1310" type="text" value="Down"/></p> </div>
<p data-bbox="236 1335 256 1361">2</p>	<p data-bbox="327 1335 1310 1397"> Configured SIP Interfaces. Each SIP Interface is displayed using the following "SIP Interface"-titled icon, which includes the name and row index number: </p> <div data-bbox="790 1402 933 1467" style="text-align: center;">  </div> <p data-bbox="327 1473 1358 1536"> If you hover your mouse over the icon, a pop-up appears displaying the following basic information (example): </p> <div data-bbox="762 1543 959 1832" style="text-align: center;">  </div> <p data-bbox="327 1839 1278 1872"> If you click the icon, a drop-down menu appears listing the following commands: </p>

Item #	Description
	<div data-bbox="790 257 938 436" style="border: 1px solid gray; padding: 5px; margin-bottom: 10px;"> <p style="text-align: center;">EDIT</p> <hr style="width: 50%; margin: 0 auto;"/> <p style="text-align: center;">SHOW LIST</p> <hr style="width: 50%; margin: 0 auto;"/> <p style="text-align: center;">DELETE</p> </div> <ul style="list-style-type: none"> ▪ Edit: Opens a dialog box in the SIP Interfaces table to modify the SIP Interface. ▪ Show List: Opens the SIP Interfaces table. ▪ Delete: Opens the SIP Interfaces table where you are prompted to confirm deletion of the SIP Interface. <p>To add a SIP Interface, do the following:</p> <ol style="list-style-type: none"> 1 Click the Add SIP Interface  plus icon. The icon appears next to existing SIP Interfaces, or as  when no SIP Interfaces exist on a topology border, or as  when there are no SIP Interfaces at all. The SIP Interfaces table opens with a new dialog box for adding a SIP Interface to the next available index row. 2 Configure the SIP Interface as desired, and then click Apply; the SIP Interfaces table closes and you are returned to the Topology View, displaying the new SIP Interface. <p>For more information on configuring SIP Interfaces, see "Configuring SIP Interfaces" on page 321.</p>
3	<p>Configured Media Realms. Each Media Realm is displayed using the following "Media Realm"-titled icon, which includes the name and row index number:</p> <div data-bbox="782 1093 941 1153" style="border: 1px solid gray; padding: 2px; margin: 10px auto; width: fit-content;"> <p style="text-align: center; font-size: small;">Media Realm #0[Defaul...</p> </div> <p>If you hover your mouse over the icon, a pop-up appears displaying the following basic information (example):</p> <div data-bbox="726 1232 997 1422" style="border: 1px solid gray; padding: 5px; margin: 10px auto; width: fit-content;"> <p style="font-size: small;">Interface: O+M+C Start Port: 6000 Number of Sessions: 5953</p> <div data-bbox="782 1361 941 1422" style="border: 1px solid gray; padding: 2px; margin: 5px auto; width: fit-content;"> <p style="text-align: center; font-size: small;">Media Realm #0[Defaul...</p> </div> </div> <p>If you click the icon, a drop-down menu appears listing the following commands:</p> <div data-bbox="790 1473 938 1653" style="border: 1px solid gray; padding: 5px; margin: 10px auto; width: fit-content;"> <p style="text-align: center;">EDIT</p> <hr style="width: 50%; margin: 0 auto;"/> <p style="text-align: center;">SHOW LIST</p> <hr style="width: 50%; margin: 0 auto;"/> <p style="text-align: center;">DELETE</p> </div> <ul style="list-style-type: none"> ▪ Edit: Opens a dialog box in the Media Realms table to modify the Media Realm. ▪ Show List: Opens the Media Realms table. ▪ Delete: Opens the Media Realms table where you are prompted to confirm deletion of the Media Realm. <p>To add a Media Realm, do the following:</p> <ol style="list-style-type: none"> 1 Click the Add Media Realm  plus icon. The icon appears next to existing Media Realms, or as  when no Media Realms exist on a topology

Item #	Description
	<p>border, or as  when there are no Media Realms at all. The Media Realms table opens with a new dialog box for adding a Media Realm to the next available index row.</p> <p>2 Configure the Media Realm as desired, and then click Apply; the Media Realms table closes and you are returned to the Topology View, displaying the new Media Realm. For more information on configuring Media Realms, see "Configuring Media Realms" on page 303.</p>
4	<p>Configured IP Groups. Each IP Group is displayed using the following "IP Group [Server]" or "IP Group [User]" titled icon (depending on whether it's a Server- or User-type IP Group respectively), which includes the name and row index number (example of a Server-type):</p> <div data-bbox="775 680 948 743" style="border: 1px solid black; padding: 2px; margin: 10px auto; width: fit-content;"> <p>IP Group [Server] #0[Defaul...</p> </div> <p>If you hover your mouse over the icon, a pop-up appears displaying the following basic information (example):</p> <div data-bbox="603 824 1123 976" style="border: 1px solid black; padding: 5px; margin: 10px auto;"> <div style="display: flex; align-items: center;"> <div style="border: 1px solid black; padding: 2px; margin-right: 5px;"> <p>IP Group [Server] #0[Defaul...</p> </div> <div style="background-color: #333; color: white; padding: 5px;"> <p style="margin: 0;">DefaultSRD</p> <hr style="border: 0.5px solid white;"/> <p style="margin: 0;">Type: Server</p> <p style="margin: 0;">Name: Default_IPG</p> <p style="margin: 0;">SIP Interface: #0[SIPinterface_0]</p> </div> </div> </div> <p>If you click the icon, a drop-down menu appears listing the following commands:</p> <div data-bbox="788 1025 938 1200" style="border: 1px solid black; padding: 5px; margin: 10px auto; width: fit-content;"> <p style="text-align: center; margin: 0;">EDIT</p> <hr style="border: 0.5px solid black;"/> <p style="text-align: center; margin: 0;">SHOW LIST</p> <hr style="border: 0.5px solid black;"/> <p style="text-align: center; margin: 0;">DELETE</p> </div> <ul style="list-style-type: none"> ▪ Edit: Opens a dialog box in the IP Groups table to modify the IP Group. ▪ Show List: Opens the IP Groups table. ▪ Delete: Opens the IP Groups table where you are prompted to confirm deletion of the IP Group. <p>To add an IP Group, do the following:</p> <p>1 Click the Add IP Group  plus icon. The icon appears next to existing IP Groups, or as  when no IP Groups exist on a topology border, or as  when there are no IP Groups at all. The IP Groups table opens with a new dialog box for adding a IP Group to the next available index row.</p> <p>2 Configure the IP Group as desired, and then click Apply; the IP Groups table closes and you are returned to the Topology View, displaying the new IP Group. For more information on configuring IP Groups, see "Configuring IP Groups" on page 329. IP Group icons also display connectivity status with Server-type IP Groups:</p> <ul style="list-style-type: none"> ▪  (Green with check mark): Keep-alive is successful and connectivity exists with IP Group. ▪  (Red with "x"): Keep-alive has failed and there is a loss of connectivity

Item #	Description
	<p>with the IP Group.</p> <p>The line type connecting between an IP Group and a SIP Interface indicates whether a routing rule has been configured for the IP Group. A solid line indicates that you have configured a routing rule for the IP Group; a dashed line indicates that you have yet to configure a routing rule.</p> <p>Note:</p> <ul style="list-style-type: none"> ▪ You can also view connectivity status in the IP Groups table. ▪ To support the connectivity status feature, you must enable the keep-alive mechanism for the Proxy Set that is associated with the IP Group (see "Configuring Proxy Sets" on page 341). ▪ The green-color state also applies to scenarios where the device rejects calls with the IP Group due to low QoE (e.g., low MOS), despite connectivity.
5	<p>Links to Web pages relating to commonly required SBC configuration:</p> <ul style="list-style-type: none"> ▪ Classification: Opens the Classification table where you can configure Classification rules (see "Configuring Classification Rules" on page 461). ▪ Number Manipulation: Opens the Outbound Manipulations table where you can configure manipulation rules on SIP Request-URI user parts (source or destination) or calling names in outbound SIP dialog requests (see "Configuring IP-to-IP Outbound Manipulations" on page 497). ▪ Routing: Opens the IP-to-IP Routing table where you can configure IP-to-IP routing rules (see "Configuring SBC IP-to-IP Routing Rules" on page 470). ▪ SBC Settings: Opens the SBC General Settings page where you can configure miscellaneous settings.

20 SIP Definitions

This section describes configuration of various SIP-related functionalities.

20.1 Configuring Registration Accounts

The Accounts table lets you configure up to 1,500 Accounts. An Account defines registration information for registering and authenticating (digest) IP Groups (e.g., IP PBX) with a "serving" IP Group (e.g., ITSP).

The device initiates registration with a "serving" IP Group on behalf of the "served" IP Group. Therefore, Accounts are typically required when the "served" IP Group is unable to register or authenticate itself for whatever reason. Registration information includes username, password, host name (AOR), and contact user name (AOR). The device includes this information in the REGISTER message sent to the serving IP Group. Up to 10 Accounts can be configured per "served" IP Group. A IP Group can register to more than one IP Group (e.g., multiple ITSPs). This is done by configuring multiple entries in the Accounts table for the same served IP Group, but with different serving IP Groups, username/password, host name, and contact user values.

Authentication is typically required for INVITE messages sent to the "serving" IP Group. If the device receives a SIP 401 (Unauthorized) in response to a sent INVITE, the device checks for a matching "serving" and "served" entry in the Accounts table. If a matching row exists, the device authenticates the INVITE by providing the corresponding MD5 authentication username and password to the "serving" IP Group.



Note: If no match is found in the Accounts table for incoming or outgoing calls, the username and password is taken from:

- 'UserName' and 'Password' parameters on the Proxy & Registration page

The following procedure describes how to configure Accounts through the Web interface. You can also configure it through ini file (Account) or CLI (configure voip > sip-definition account).

➤ **To configure an Account:**

1. Open the Accounts table (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Accounts**).

- Click **New**; the following dialog box appears:

Figure 20-1: Accounts Table - Add Dialog Box

The screenshot shows a dialog box titled "Accounts" with a dark blue header. Below the header, there is a "Served IP Group" dropdown menu with "--" selected. The dialog is divided into two main sections: "GENERAL" and "CREDENTIALS".

GENERAL Section:

- Index: Text input field containing "0".
- Application Type: Dropdown menu with "SBC" selected.
- Serving IP Group: Dropdown menu with "--" selected, followed by a "View" link.
- Host Name: Text input field.
- Register: Dropdown menu with "No" selected.
- Contact User: Text input field.

CREDENTIALS Section:

- User Name: Text input field.
- Password: Text input field.

- Configure an account according to the parameters described in the table below.
- Click **Apply**.

Once you have configured Accounts, you can register or un-register them, as described below:

➤ **To register or un-register an Account:**

- In the table, select the required Account entry row.
- From the **Action** drop-down list, choose one of the following commands:
 - Register** to register the Account.
 - Un-Register** to un-register the Account.

To view Account registration status, see "Viewing Registration Status" on page 658.

Table 20-1: Accounts Table Parameter Descriptions

Parameter	Description
General	
Index	Defines an index for the new table row. Note: Each row must be configured with a unique index.
Application Type application-type [Account_ApplicationType]	Defines the application type: <ul style="list-style-type: none"> [2] SBC = SBC application.
Served IP Group served-ip-group-name [Account_ServedIPGroupName]	Defines the IP Group (e.g., IP-PBX) that you want to register and/or authenticate upon its behalf. Note: <ul style="list-style-type: none"> By default, all IP Groups are displayed. However, if you filter

Parameter	Description
	the Web display by SRD (using the SRD Filter box), only IP Groups associated with the filtered SRD are displayed.
Serving IP Group serving-ip-group-name [Account_ServingIPGroupName]	<p>Defines the IP Group (<i>Serving IP Group</i>) to where the device sends the SIP REGISTER requests (if enabled) for registration and authentication (of the Served IP Group).</p> <p>Note:</p> <ul style="list-style-type: none"> By default, only IP Groups associated with the SRD to which the Served IP Group is associated are displayed, as well as IP Groups of Shared SRDs. However, if you filter the Web display by SRD (using the SRD Filter box), only IP Groups associated with the filtered SRD are displayed, as well as IP Groups of Shared SRDs. The parameter is mandatory.
Host Name host-name [Account_HostName]	<p>Defines the Address of Record (AOR) host name. The host name appears in SIP REGISTER From/To headers as ContactUser@HostName. For a successful registration, the host name is also included in the URI of the INVITE From header.</p> <p>The valid value is a string of up to 49 characters.</p> <p>Note: If the parameter is not configured or if registration fails, the 'SIP Group Name' parameter value configured in the IP Groups table is used instead.</p>
Register register [Account_Register]	<p>Enables registration.</p> <ul style="list-style-type: none"> [0] No= (Default) The device only performs authentication (not registration). Authentication is typically done for INVITE messages sent to the "serving" IP Group. If the device receives a SIP 401 (Unauthorized) in response to a sent INVITE, the device checks for a matching "serving" and "served" entry in the table. If a matching row exists, the device authenticates the INVITE by providing the corresponding MD5 authentication username and password to the "serving" IP Group. [1] Regular = Regular registration process. For more information, see "Regular Registration Mode" on page 358. [2] GIN = Registration for legacy PBXs, using Global Identification Number (GIN). For more information, see "Single Registration for Multiple Phone Numbers using GIN" on page 358. <p>Note: The account registration is not affected by the IsRegisterNeeded parameter.</p>
Contact User contact-user [Account_ContactUser]	<p>Defines the AOR username. This appears in REGISTER From/To headers as ContactUser@HostName, and in INVITE/200 OK Contact headers as ContactUser@<device's IP address>.</p> <p>Note:</p> <ul style="list-style-type: none"> If the parameter is not configured, the 'Contact User' parameter in the IP Groups table is used instead. If registration fails, the user part in the INVITE Contact header contains the source party number.
Credentials	
User Name user-name	<p>Defines the digest MD5 Authentication username.</p> <p>The valid value is a string of up to 50 characters.</p>

Parameter	Description
[Account_Username]	
Password password [Account_Password]	Defines the digest MD5 Authentication password. The valid value is a string of up to 50 characters.

20.1.1 Regular Registration Mode

When you configure the registration mode in the Accounts table to **Regular**, the device sends REGISTER requests to the Serving IP Group. The host name (in the SIP From/To headers) and contact user (user in From/To and Contact headers) are taken from the configured Accounts table upon successful registration. See the example below:

```
REGISTER sip:xyz SIP/2.0
Via: SIP/2.0/UDP 10.33.37.78;branch=z9hG4bKac1397582418
From: <sip:ContactUser@HostName>;tag=1c1397576231
To: <sip: ContactUser@HostName >
Call-ID: 1397568957261200022256@10.33.37.78
CSeq: 1 REGISTER
Contact: <sip:ContactUser@10.33.37.78>;expires=3600
Expires: 3600
User-Agent: Sip-Gateway/v.7.20A.000.038
Content-Length: 0
```

20.1.2 Single Registration for Multiple Phone Numbers using GIN

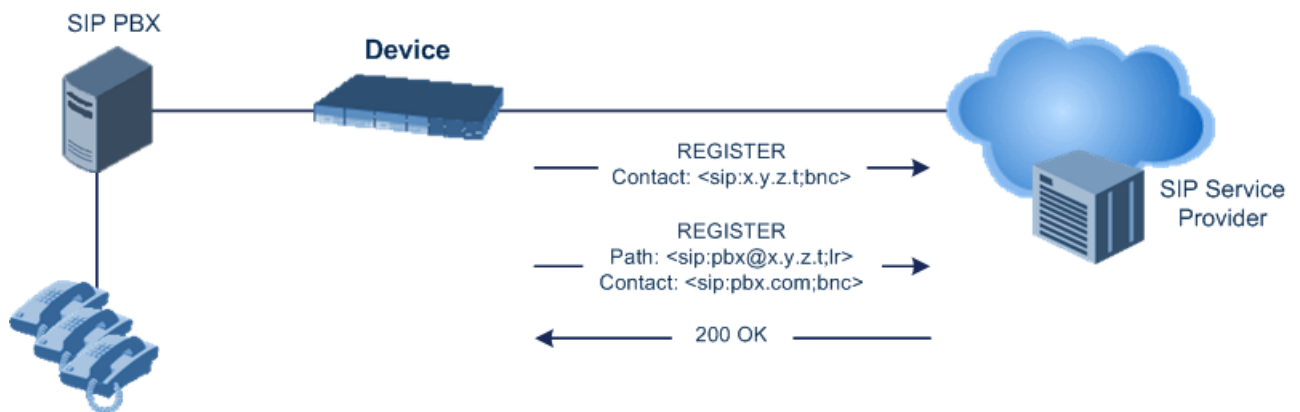
When you configure the registration mode in the Accounts table to **GIN**, the Global Identifiable Number (GIN) registration method is used, according to RFC 6140. The device performs GIN-based registration of users to a SIP registrar on behalf of a SIP PBX. In effect, the PBX registers with the service provider, just as a directly hosted SIP endpoint would register. However, because a PBX has multiple user agents, it needs to register a contact address on behalf of each of these. Rather than performing a separate registration procedure for each user agents, GIN registration mode does multiple registrations using a single REGISTER transaction.

According to this mechanism, the PBX delivers to the service provider in the Contact header field of a REGISTER request a template from which the service provider can construct contact URIs for each of the AORs assigned to the PBX and thus, can register these contact URIs within its location service. These registered contact URIs can then be used to deliver to the PBX inbound requests targeted at the AORs concerned. The mechanism can be used with AORs comprising SIP URIs based on global E.164 numbers and the service provider's domain name or sub-domain name.

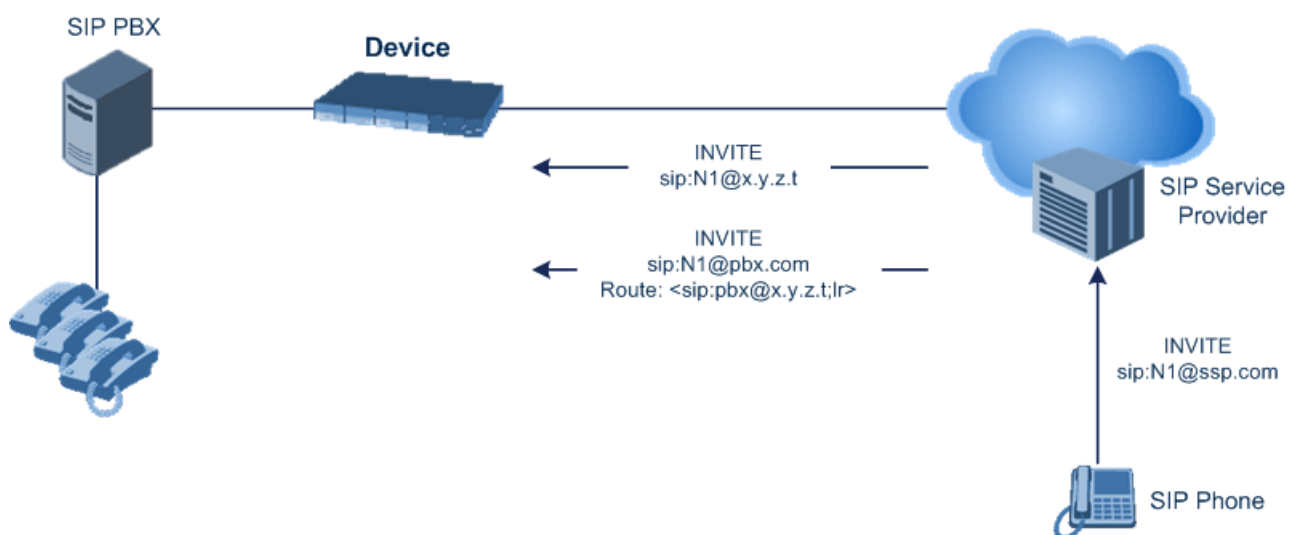
The SIP REGISTER request sent by the device for GIN registration with a SIP server provider contains the Require and Proxy-Require headers. These headers contain the token 'gin'. The Supported header contains the token 'path' and the URI in the Contact header contains the parameter 'bnc' without a user part:

```
Contact: <sip:198.51.100.3;bnc>;
```

The figure below illustrates the GIN registration process:



The figure below illustrates an incoming call using GIN:



20.2 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 733. To configure Proxy servers (Proxy Sets), see "Configuring Proxy Sets" on page 341.



Note: To view the registration status of endpoints with a SIP Registrar/Proxy server, see "Viewing Registration Status" on page 658.

➤ To configure the Proxy and registration parameters:

1. Open the Proxy & Registration page (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Proxy & Registration**).
2. Configure the parameters as required.
3. Click **Apply**.

➤ **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 - Accounts table (see "Configuring Registration Accounts" on page 355)

20.2.1 SIP Message Authentication Example

The device supports basic and digest (MD5) authentication types, according to SIP RFC 3261. 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 SBC/v.7.20A.000.038
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
SBC/v.7.20A.000.038
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
```

20.3 Configuring SIP Message Manipulation

The Message Manipulations table lets you configure up to 1,500 Message Manipulation rules. A Message Manipulation rule defines a manipulation sequence for 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. SIP message manipulations can also be implemented to resolve incompatibilities between SIP devices inside the enterprise network.

Each Message Manipulation rule is configured with a Manipulation Set ID. You can create groups (sets) of Message Manipulation rules by assigning each of the relevant Message Manipulation rules to the same Manipulation Set ID. The Manipulation Set ID is then used to assign the rules to specific calls:

- Message manipulation rules can be applied pre- or post-classification:
 - Pre-classification Process: Message manipulation can be done on incoming SIP dialog-initiating messages (e.g., INVITE) prior to the classification process. You configure this by assigning the Manipulation Set ID to the SIP Interface on which the call is received (see Configuring SIP Interfaces on page 321).
 - Post-classification Process: Message manipulation can be done on inbound and/or outbound SIP messages after the call has been successfully classified. Manipulation occurs only after the routing process - inbound message manipulation is done first, then outbound number manipulation (see Configuring IP-to-IP Outbound Manipulations on page 497), and then outbound message manipulation. For viewing the call processing flow, see Call Processing of SIP Dialog Requests on page 425. You configure this by assigning the Manipulation Set ID to the relevant IP Group in the IP Groups table (see Configuring IP Groups on page 329).

The device also supports a built-in SIP message normalization feature that can be enabled per Message Manipulation rule. The normalization feature removes unknown SIP message elements before forwarding the message. These elements can include SIP headers, SIP header parameters, and SDP body fields.

The SIP message manipulation feature supports the following:

- Manipulation on SIP message type (Method, Request/Response, and Response type)
- Addition of new SIP headers
- Removal of SIP headers ("black list")
- Modification of SIP header components such as values, header values (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 is not 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)
- Multiple manipulation rules on the same SIP message
- Apply conditions per rule - the condition can be on parts of the message or call's parameters
- Multiple manipulation rules using the same condition. The following figure shows a configuration example where rules 1 and 2 ('Row Rule' configured to **Use Previous Condition**) use the condition configured for rule 0 ('Row Rule' configured to **Use**

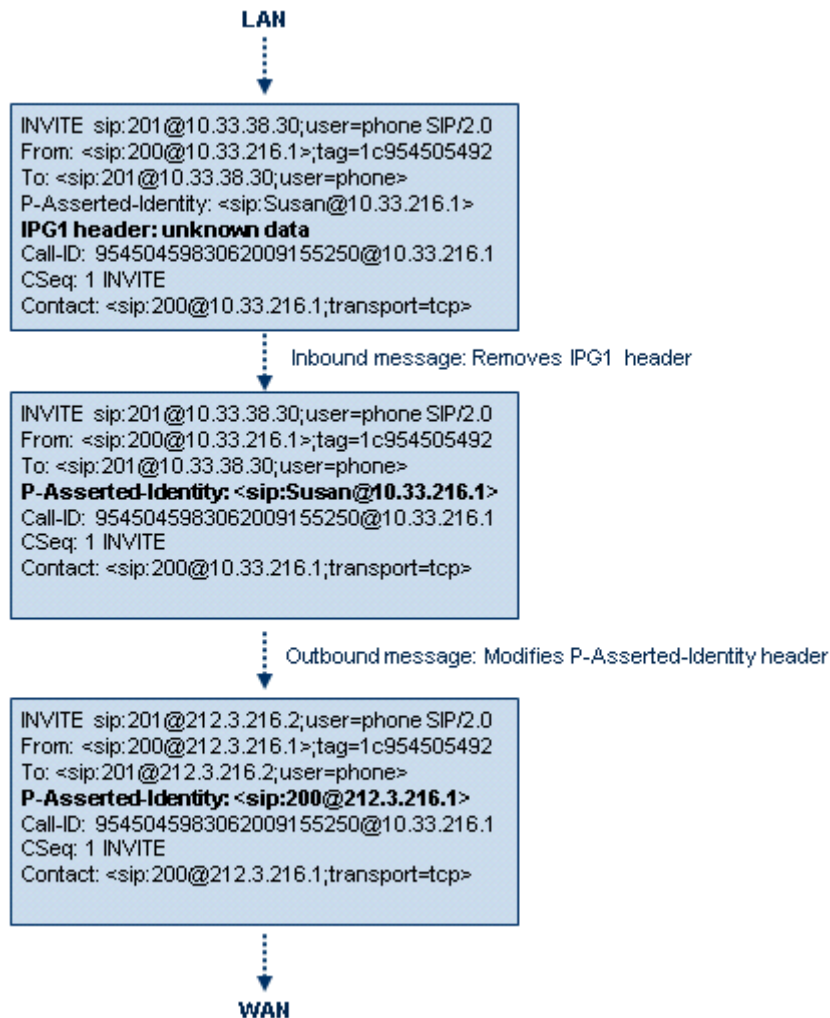
Current Condition). For more information, see the description of the 'Row Rule' parameter in this section.

Figure 20-2: Configuration Example of Message Manipulation Rules using Same Condition

INDEX	NAME	MANIPULATION SET ID	MESSAGE TYPE	CONDITION	ACTION SUBJECT	ACTION TYPE	ACTION VALUE ↕	ROW ROLE
1	Add emergency	0			header.priority	Add	'emergency'	Use Previous Condition
2	User-Agent	0			header.user-agent	Modify	'trunk-a'	Use Previous Condition
0	To Header Urgent	0	invite.request	header.request.url.uri==	header.to	Modify	header.to + ";urgent=1"	Use Current Condition

The figure below illustrates a SIP message manipulation example:

Figure 20-3: SIP Header Manipulation Example





Note:

- For a detailed description of the syntax used for configuring Message Manipulation rules, refer to the *SIP Message Manipulations Quick Reference Guide*.
- Inbound 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 SIP Group Name (IPGroup_SIPGroupName) parameter overrides inbound message manipulation rules that manipulate the host name in Request-URI, To, and/or From SIP headers. If you configure a SIP Group Name for the IP Group (see "Configuring IP Groups" on page 329) and you want to manipulate the host name in these SIP headers, you must apply your manipulation rule (Manipulation Set ID) to the IP Group as an Outbound Message Manipulation Set (IPGroup_OutboundManSet), when the IP Group is the destination of the call. If you apply the Manipulation Set as an Inbound Message Manipulation Set (IPGroup_InboundManSet), when the IP Group is the source of the call, the manipulation rule will be overridden by the SIP Group Name.

The following procedure describes how to configure Message Manipulation rules through the Web interface. You can also configure it through ini file (MessageManipulations) or CLI (configure voip > message message-manipulations).

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

1. Open the Message Manipulations page (**Setup** menu > **Signaling & Media** tab > **Message Manipulation** folder > **Message Manipulations**).
2. Click **New**; the following dialog box appears:

Figure 20-4: Message Manipulations Table - Add Dialog Box

GENERAL		ACTION	
Index	<input type="text" value="of"/>	Action Subject	<input type="text"/>
Name	<input type="text"/>	Action Type	<input type="text" value="Add"/>
Manipulation Set ID	<input type="text" value="0"/>	Action Value	<input type="text"/>
Row Role	<input type="text" value="Use Current Condition"/>		
MATCH			
Message Type	<input type="text"/>		
Condition	<input type="text"/>		

3. Configure a Message Manipulation rule according to the parameters described in the table below.
4. Click **Apply**.

An example of configured message manipulation rules are shown in the figure below:

Figure 20-5: Example of Configured Message Manipulation Rules

INDEX ↕	NAME	MANIPULATION SET ID	MESSAGE TYPE	CONDITION	ACTION SUBJECT	ACTION TYPE	ACTION VALUE
0	ITSP A	0	invite.response.200		header.to.url.user	Add Suffix	'.com'
1		0	invite.response.200		header.from.url.user	Modify	header.p-asserted-id.url.user
2		0	invite.request		header.from.url.user	Modify	'200'
3		2	invite.request	header.from.url.user=="Unknown"	header.from.url.user	Modify	param.ipg.src.user
4		2	invite.request		header.priority	Remove	

- **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.

Table 20-2: Message Manipulations Parameter Descriptions

Parameter	Description
General	
Index [MessageManipulations_Index]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
Name manipulation-name [MessageManipulations_ManipulationName]	Defines an arbitrary name to easily identify the rule. The valid value is a string of up to 16 characters.
Manipulation Set ID manipulation-set-id [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 Groups table) for inbound and/or outbound messages. The valid value is 0 to 19. The default is 0.
Row Role row-role [MessageManipulations_RowRole]	Determines which message manipulation condition (configured by the 'Condition' parameter) to use for the rule. <ul style="list-style-type: none"> ■ [0] Use Current Condition = (Default) The condition configured in the table row of the rule is used. ■ [1] Use Previous Condition = The condition configured in the first table row above the rule that is configured to Use Current Condition is used. For example, if Index 3 is configured to Use Current Condition and Index 4 and 5 are configured to Use Previous Condition, Index 4 and 5 use the condition configured for Index 3. A configuration example is shown in the beginning of this section. The option allows you to use the same condition for multiple manipulation rules. Note:

Parameter	Description
	<ul style="list-style-type: none"> ▪ When configured to Use Previous Condition, the 'Message Type' and 'Condition' parameters are not applicable and if configured are ignored. ▪ When multiple manipulation rules apply to the same header, the next rule applies to the resultant string of the previous rule.
Match	
Message Type message-type [MessageManipulations_Message Type]	Defines the SIP message type that you want to manipulate. The valid value is a string (case-insensitive) denoting the SIP message. For example: <ul style="list-style-type: none"> ▪ Empty = rule applies to all messages ▪ Invite = rule applies to all INVITE requests and responses ▪ Invite.Request = rule applies to INVITE requests ▪ Invite.Response = rule applies to INVITE responses ▪ subscribe.response.2xx = rule applies to SUBSCRIBE confirmation responses Note: Currently, SIP 100 Trying messages cannot be manipulated.
Condition condition [MessageManipulations_Condition]	Defines the condition that must exist for the rule to be applied. The valid value is a string (case-insensitive). For example: <ul style="list-style-type: none"> ▪ header.from.url.user== '100' (indicates that the user part of the From header must have the value "100") ▪ header.contact.param.expires > '3600' ▪ header.to.url.host contains 'domain' ▪ param.call.dst.user != '100'
Action	
Action Subject action-subject [MessageManipulations_ActionSubject]	Defines the SIP header upon which the manipulation is performed. The valid value is a string (case-insensitive).
Action Type action-type [MessageManipulations_ActionType]	Defines the type of manipulation. <ul style="list-style-type: none"> ▪ [0] Add (default) = Adds new header/param/body (header or parameter elements). ▪ [1] Remove = Removes header/param/body (header or parameter elements). ▪ [2] Modify = Sets element to the new value (all element types). ▪ [3] Add Prefix = Adds value at the beginning of the string (string element only). ▪ [4] Add Suffix = Adds value at the end of the string (string element only). ▪ [5] Remove Suffix = Removes value from the end of the string (string element only). ▪ [6] Remove Prefix = Removes value from the beginning of the string (string element only).

Parameter	Description
	<ul style="list-style-type: none"> ▪ [7] Normalize = Removes unknown SIP message elements before forwarding the message.
Action Value action-value [MessageManipulations_ActionValue]	Defines a value that you want to use in the manipulation. The default value is a string (case-insensitive) in the following syntax: <ul style="list-style-type: none"> ▪ string/<message-element>/<call-param> + ▪ string/<message-element>/<call-param> For example: <ul style="list-style-type: none"> ▪ 'itsp.com' ▪ header.from.url.user ▪ param.call.dst.user ▪ param.call.dst.host + '.com' ▪ param.call.src.user + '<' + header.from.url.user + '@' + header.p-asserted-id.url.host + '>' Note: Only single quotation marks must be used.

20.4 Configuring SIP Message Policy Rules

The Message Policies table lets you configure up to 20 SIP Message Policy rules. SIP Message Policy rules are used to block (blacklist) unwanted incoming SIP messages or permit (whitelist) receipt of desired SIP messages. You can configure legal and illegal characteristics of SIP messages. 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 oversized parameter or too many occurrences of a parameter.

You can also enable the Message Policy to protect the device against incoming SIP messages with malicious signature patterns, which identify specific scanning tools used by attackers to search for SIP servers in a network. To configure Malicious Signatures, see "Configuring Malicious Signatures" on page 517.

Each Message Policy rule can be configured with the following:

- Maximum message length
- Maximum 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 methods (e.g., INVITE)
- Blacklist and whitelist for defined bodies
- Malicious Signatures

The Message Policies table provides a default Message Policy called "Malicious Signature DB Protection" (Index 0), which is based only on Malicious Signatures and discards SIP messages identified with any of the signature patterns configured in the Malicious Signature table.

To apply a SIP Message Policy rule to calls, you need to assign it to the SIP Interface associated with the relevant IP Group (see "Configuring SIP Interfaces" on page 321).

The following procedure describes how to configure Message Policy rules through the Web interface. You can also configure it through ini file (MessagePolicy) or CLI (configure voip > message message-policy).

➤ **To configure SIP Message Policy rules:**

1. Open the Message Policies table (**Setup** menu > **Signaling & Media** tab > **Message Manipulation** folder > **Message Policies**).
2. Click **New**; the following dialog box appears:

Figure 20-6: Message Policies Table - Add Dialog Box

3. Configure a Message Policy rule according to the parameters described in the table below.
4. Click **Apply**.

Table 20-3: Message Policies Table Parameter Descriptions

Parameter	Description
General	
Index [MessagePolicy_Index]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
Name name [MessagePolicy_Name]	Defines an arbitrary name to easily identify the row. The valid value is a string of up to 20 characters. Note: Each row must be configured with a unique name.
Limits	
Max Message Length max-message-length [MessagePolicy_MaxMessageLength]	Defines the maximum SIP message length. The valid value is up to 32,768 characters. The default is 32,768.

Parameter	Description
Max Header Length max-header-length [MessagePolicy_MaxHeaderLength]	Defines the maximum SIP header length. The valid value is up to 512 characters. The default is 512.
Max Body Length max-body-length [MessagePolicy_MaxBodyLength]	Defines the maximum SIP message body length. This is the value of the Content-Length header. The valid value is up to 1,024 characters. The default is 1,024.
Max Num Headers max-num-headers [MessagePolicy_MaxNumHeaders]	Defines the maximum number of SIP headers. The valid value is any number up to 32. The default is 32. Note: The device supports up to 20 SIP Record-Route headers that can be received in a SIP INVITE request or a 200 OK response. If it receives more than this, it responds with a SIP 513 'Message Too Large' response.
Max Num Bodies max-num-bodies [MessagePolicy_MaxNumBodies]	Defines the maximum number of bodies (e.g., SDP) in the SIP message. The valid value is any number up to 8. The default is 8.
Policies	
Send Rejection send-rejection [MessagePolicy_SendRejection]	Defines whether the device sends a SIP response if it rejects a message request due to the Message Policy. The default response code is SIP 400 "Bad Request". To configure a different response code, use the MessagePolicyRejectResponseType parameter. <ul style="list-style-type: none"> ▪ [0] Policy Reject = (Default) The device discards the message and sends a SIP response to reject the request. ▪ [1] Policy Drop = The device discards the message without sending any response.
SIP Method Blacklist-Whitelist Policy	
Method List method-list [MessagePolicy_MethodList]	Defines SIP methods (e.g., INVITE\BYE) to blacklist or whitelist. Multiple methods are separated by a backslash (\). The method values are case-insensitive.
Method List Type method-list-type [MessagePolicy_MethodListType]	Defines the policy (blacklist or whitelist) for the SIP methods specified in the 'Method List' parameter (above). <ul style="list-style-type: none"> ▪ [0] Policy Blacklist = The specified methods are rejected. ▪ [1] Policy Whitelist = (Default) Only the specified methods are allowed; the others are rejected.
SIP Body Blacklist-Whitelist Policy	
Body List body-list [MessagePolicy_BodyList]	Defines the SIP body type (i.e., value of the Content-Type header) to blacklist or whitelist. For example, application/sdp. The values of the parameter are case-sensitive.

Parameter	Description
Body List Type body-list-type [MessagePolicy_BodyListType]	Defines the policy (blacklist or whitelist) for the SIP body specified in the 'Body List' parameter (above). <ul style="list-style-type: none"> ▪ [0] Policy Blacklist =The specified SIP body is rejected. ▪ [1] Policy Whitelist = (Default) Only the specified SIP body is allowed; the others are rejected.
Malicious Signature	
Malicious Signature Database signature-db-enable [MessagePolicy_UseMaliciousSignatureDB]	Enables the use of the Malicious Signature database (signature-based detection). <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable To configure Malicious Signatures, see "Configuring Malicious Signatures" on page 517.

20.5 Configuring Call Setup Rules

The Call Setup Rules table lets you configure up to 40 Call Setup rules. Call Setup rules define various sequences that are run upon the receipt of an incoming call (dialog) at call setup, before the device routes the call to its destination. Call Setup rules provide you with full flexibility in implementing simple or complex script-like rules that can be used for Lightweight Directory Access Protocol (LDAP) based routing as well as other advanced routing logic requirements such as manipulation. These Call Setup rules are assigned to routing rules.

Below is a summary of functions for which you can employ Call Setup rules:

- LDAP query rules: LDAP is used by the device to query Microsoft's Active Directory (AD) server for specific user details for routing, for example, office extension number, mobile number, private number, OCS (Skype for Business) address, and display name. Call Setup rules provides full flexibility in AD-lookup configuration to suite just about any customer deployment requirement:
 - Routing based on query results.
 - Queries based on any AD attribute.
 - Queries based on any attribute value (alphanumeric), including the use of the asterisk (*) wildcard as well as the source number, destination number, redirect number, and SBC SIP messages. For example, the following Call Setup rule queries the attribute "proxyAddresses" for the record value "WOW:" followed by source number: "proxyAddresses=WOW:12345*"
 - Conditional LDAP queries, for example, where the query is based on two attributes (&(telephoneNumber=4064)(company=ABC)).
 - Conditions for checking LDAP query results.
 - Manipulation of call parameters such as source number, destination number, and redirect number and SBC SIP messages, while using LDAP query results.
 - Multiple LDAP queries.
- Dial Plan queries: For SBC calls, you can use Call Setup rules to query the Dial Plan table (see Configuring Dial Plans on page 503) for a specified search key in a specified Dial Plan to obtain the corresponding Dial Plan tag. Call Setup rules can also change (modify) the name of the obtained tag. The device can then route the call using an IP-to-IP Routing rule (in the IP-to-IP Routing table) that has a matching tag (source or destination). You can also associate a Call Setup rule with an IP Group (in

the IP Group table). Once the device classifies the incoming call to a source IP Group, it processes the associated Call Setup rule and then uses the resultant tag to locate a matching IP-to-IP Routing rule. You can also use Call Setup rules for complex routing schemes by using multiple Dial Plan tags. This is typically required when the source and/or destination of the call needs to be categorized with more than one characteristics. For example, tags can be used to categorize calls by department (source user) within a company, where only certain departments are allowed to place international calls.

- Manipulation (similar to the Message Manipulations table) of call parameters (such as source number, destination number, and redirect number) and SBC SIP messages.
- Conditions for routing, for example, if the source number equals a specific value, then use the call routing rule.

You configure multiple Call Setup rules and group them using a *Set ID*. This lets you apply multiple Call Setup rules on the same call setup dialog. To use your Call Setup rule(s), you need to assign the Set ID to one of the following, using the 'Call Setup Rules Set ID' field:

- SBC IP-to-IP routing rules(see Configuring SBC IP-to-IP Routing Rules on page 470)
- IP Groups (see Configuring IP Groups on page 329)

If assigned to an IP Group, the device processes the Call Setup rule for the classified source IP Group immediately before the routing process. If assigned to a routing rule only, the device first locates a matching routing rule for the incoming call, processes the assigned Call Setup Rules Set ID, and then routes the call according to the destination configured for the routing rule.. The device uses the routing rule to route the call, depending on the result of the Call Setup Rules Set ID:

- **Rule's condition is met:** The device performs the rule's action and then runs the next rule in the Set ID until the last rule or until a rule with an **Exit** Action Type. If the **Exit** rule is configured with a "True" Action Value, the device uses the current routing rule. If the **Exit** rule is configured with a "False" Action Value, the device moves to the next routing rule. If an **Exit** Action Type is not configured and the device has run all the rules in the Set ID, the default Action Value of the Set ID is "True" (i.e., use the current routing rule).
- **Rule's condition is not met:** The device runs the next rule in the Set ID. When the device reaches the end of the Set ID and no **Exit** was performed, the Set ID ends with a "True" result.



Note: If the source and/or destination numbers are manipulated by the Call Setup rules, they revert to their original values if the device moves to the next routing rule.

The following procedure describes how to configure Call Setup Rules through the Web interface. You can also configure it through ini file (CallSetupRules) or CLI (configure voip > message call-setup-rules).

➤ **To configure a Call Setup rule:**

1. Open the Call Setup Rules table (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Call Setup Rules**).

- Click **New**; the following dialog box appears:

Figure 20-7: Call Setup Rules Table - Add Dialog Box

- Configure a Call Setup rule according to the parameters described in the table below.
- Click **Apply**, and then save your settings to flash memory.

Table 20-4: Call Setup Rules Parameter Descriptions

Parameter	Description
General	
Index [CallSetupRules_Index]	Defines an index number for the new table record. Note: Each rule must be configured with a unique index.
Rules Set ID rules-set-id [CallSetupRules_RulesSetID]	Defines a Set ID for the rule. You can define the same Set ID for multiple rules to create a group of rules. You can configure up to 10 Set IDs, where each Set ID can include up to 10 rules. The Set ID is used to assign the Call Setup rules to a routing rule in the routing table. The valid value is 0 to 9. The default is 0.
Query Type query-type [CallSetupRules_QueryType]	Defines the type of query. <ul style="list-style-type: none"> [0] None (default) [1] LDAP = The Call Setup rule performs an LDAP query with an LDAP server. [2] Dial Plan = The Call Setup rule performs a query with the Dial Plan. To specify an LDAP server or Dial Plan, use the 'Query Target' parameter (see below).
Query Target query-target [CallSetupRules_QueryTarget]	Defines one of the following, depending on the value configured for the 'Query Type' parameter (above): <ul style="list-style-type: none"> LDAP: Specifies an LDAP server (LDAP Server Group) on which to perform an LDAP query for a defined search key. To configure LDAP Server Groups, see Configuring LDAP Server Groups on page 228. Dial Plan: Specifies a Dial Plan (name) in which to search for a defined search key. To configure Dial Plans, see Configuring Dial Plans on page on page 503. To configure the search key, use the 'Search Key' parameter

Parameter	Description
	(see below). Note: The parameter is applicable only if the 'Query Type' parameter is configured to any value other than None .
Search Key attr-to-query [CallSetupRules_AttributesToQuery]	Defines the key to query. For LDAP queries, the key string is queried in the specified LDAP server. For Dial Plan queries, the key string is searched for in the specified Dial Plan. The valid value is a string of up to 100 characters. Combined strings and values can be configured like in the Message Manipulations table, using the '+' operator. Single quotes (') can be used for specifying a constant string (e.g., '12345'). Examples: <ul style="list-style-type: none"> ▪ To LDAP query the AD attribute "mobile" that has the value of the destination user part of the incoming call: <code>'mobile=' + param.call.dst.user</code> ▪ To LDAP query the AD attribute "telephoneNumber" that has a redirect number: <code>'telephoneNumber=' + param.call.redirect + '*'</code> ▪ To query a Dial Plan for the source number: <code>param.call.src.user</code> Note: The parameter is applicable only if the 'Query Type' parameter is configured to any value other than None .
Attributes To Get attr-to-get [CallSetupRules_AttributesToGet]	Defines the attributes of the queried LDAP record that the device must handle (e.g., retrieve value). The valid value is a string of up to 100 characters. Up to five attributes can be defined, each separated by a comma (e.g., msRTCSIP-PrivateLine,msRTCSIP-Line,mobile). Note: <ul style="list-style-type: none"> ▪ The parameter is applicable only if you configure the 'Query Type' parameter to LDAP. ▪ The device saves the retrieved attributes' values for future use in other rules, until the next LDAP query or until the call is connected. Thus, the device does not need to re-query the same attributes.
Row Role row-role [CallSetupRules_RowRole]	Determines which condition must be met in order for this rule to be performed. <ul style="list-style-type: none"> ▪ [0] Use Current Condition = The Condition configured for this rule must be matched in order to perform the configured action (default). ▪ [1] Use Previous Condition = The Condition configured for the rule located directly above this rule in the Call Setup table must be matched in order to perform the configured action. This option lets you configure multiple actions for the same Condition.
Condition condition [CallSetupRules_Condition]	Defines the condition that must exist for the device to perform the action. The valid value is a string of up to 200 characters (case-insensitive). Regular Expression (regex) can also be used. Examples:

Parameter	Description
	<ul style="list-style-type: none"> ▪ LDAP: <ul style="list-style-type: none"> ✓ ldap.attr.mobile exists (if Attribute "mobile" exists in AD) ✓ param.call.dst.user == ldap.attr.msRTCSIP-PrivateLine (if called number is the same as the number in the Attribute "msRTCSIP-PrivateLine") ✓ ldap.found !exists (if LDAP record not found) ✓ ldap.err exists (if LDAP error exists) ▪ Dial Plan: <ul style="list-style-type: none"> ✓ dialplan.found exists (if Dial Plan exists) ✓ dialplan.found !exists (if Dial Plan query search key not found) ▪ dialplan.result=='uk' (if corresponding tag of the searched key is "uk")
Action	
Action Subject action-subject [CallSetupRules_ActionSubject]	Defines the element (header, parameter, body, or Dial Plan tag) upon which you want to perform the action if the condition, configured in the 'Condition' parameter (see above) is met. The valid value is a string of up to 100 characters (case-insensitive). Examples: <ul style="list-style-type: none"> ▪ header.from contains '1234' ▪ param.call.dst.user (called number) ▪ param.call.src.user (calling number) ▪ param.call.src.name (calling name) ▪ param.call.redirect (redirect number) ▪ param.call.src.host (source host) ▪ param.call.dst.host (destination host) ▪ srctags (source tag) ▪ dsttags (destination tag)
Action Type action-type [CallSetupRules_ActionType]	Defines the type of action to perform. <ul style="list-style-type: none"> ▪ [0] Add (default) = Adds new message header, parameter or body elements. ▪ [1] Remove = Removes message header, parameter, or body elements. ▪ [2] Modify = Sets element to the new value (all element types). ▪ [3] Add Prefix = Adds value at the beginning of the string (string element only). ▪ [4] Add Suffix = Adds value at the end of the string (string element only). ▪ [5] Remove Suffix = Removes value from the end of the string (string element only). ▪ [6] Remove Prefix = Removes value from the beginning of the string (string element only). ▪ [20] Run Rules Set = Performs a different Rule Set ID, specified in the 'Action Value' parameter (below) ▪ [21] Exit = Stops the Rule Set ID and returns a result ("True" or "False"). .
Action Value	Defines a value that you want to use in the action.

Parameter	Description
action-value [CallSetupRules_ActionValue]	<p>The valid value is a string of up to 300 characters (case-insensitive).</p> <p>Examples:</p> <ul style="list-style-type: none"> ▪ '+9723976'+ldap.attr.alternateNumber ▪ '9764000' ▪ srctags ▪ ldap.attr.displayName ▪ true (if the 'Action Type' is set to Exit) ▪ false (if the 'Action Type' is set to Exit)

20.5.1 Call Setup Rule Examples

Below are configuration examples for using Call Setup Rules.

- **Example 1:** This example configures the device to replace (manipulate) the incoming call's source number with a number retrieved from the AD by an LDAP query. The device queries the AD server for the attribute record, "telephoneNumber" whose value is the same as the received source number (e.g., "telephoneNumber=4064"). If such an attribute is found, the device retrieves the number of the attribute record, "alternateNumber" and uses this number as the source number.

 - **Call Setup Rules table configuration:**
 - ◆ 'Rules Set ID': 1
 - ◆ 'Query Type': LDAP
 - ◆ 'Query Target': LDAP-DC-CORP
 - ◆ 'Search Key': 'telephoneNumber=' + param.call.src.user
 - ◆ 'Attributes to Get': alternateNumber
 - ◆ 'Row Role': Use Current Condition
 - ◆ 'Condition': ldap.attr.alternateNumber exists
 - ◆ 'Action Subject': param.call.src.user
 - ◆ 'Action Type': Modify
 - ◆ 'Action Value': ldap.attr.alternateNumber
 - **Routing table configuration:** A single routing rule is assigned the Call Setup Rule Set ID.
 - ◆ Index 1:
 - ✓ 'Call Setup Rules Set ID': 1
- **Example 2:** This example configures the device to replace (manipulate) the incoming call's calling name (caller ID) with a name retrieved from the AD by an LDAP query. The device queries the AD server for the attribute record, "telephoneNumber" whose value is the same as the received source number (e.g., "telephoneNumber=5098"). If such an attribute is found, the device retrieves the name from the attribute record, "displayName" and uses this as the calling name in the incoming call.

 - **Call Setup Rules table configuration:**
 - ◆ 'Rules Set ID': 2
 - ◆ 'Query Type': LDAP
 - ◆ 'Query Target': LDAP-DC-CORP
 - ◆ 'Search Key': 'telephoneNumber=' + param.call.src.user
 - ◆ 'Attributes to Get': displayName

- ◆ 'Row Role': **Use Current Condition**
- ◆ 'Condition': **ldap.attr. displayName exists**
- ◆ 'Action Subject': **param.call.src.name**
- ◆ 'Action Type': **Modify**
- ◆ 'Action Value': **ldap.attr. displayName**
- **Routing table configuration:** A single routing rule is assigned the Call Setup Rule Set ID.
 - ◆ Index 1:
 - ✓ 'Call Setup Rules Set ID': **2**
- **Example 3:** This example configures the device to route the incoming call according to whether or not the source number of the incoming call also exists in the AD server. The device queries the AD server for the attribute record, "telephoneNumber" whose value is the same as the received source number (e.g., telephoneNumber=4064"). If such an attribute is found, the device sends the call to Skype for Business; if the query fails, the device sends the call to the PBX.
 - **Call Setup Rules table configuration:**
 - ◆ 'Rules Set ID': **3**
 - ◆ 'Query Type': **LDAP**
 - ◆ 'Query Target': **LDAP-DC-CORP**
 - ◆ 'Search Key': **'telephoneNumber=' + param.call.src.user**
 - ◆ 'Attributes to Get': **telephoneNumber**
 - ◆ 'Row Role': **Use Current Condition**
 - ◆ 'Condition': **ldap.found !exists**
 - ◆ 'Action Subject': **-**
 - ◆ 'Action Type': **Exit**
 - ◆ 'Action Value': **false**

If the attribute record is found (i.e., condition is not met), the rule ends with a default exit result of true and uses the first routing rule (Skype for Business). If the attribute record does not exist (i.e., condition is met), the rule exits with a false result and uses the second routing rule (PBX).
 - **Routing table configuration:** Two routing rules are assigned with the same matching characteristics. Only the main routing rule is assigned a Call Setup Rules Set ID.
 - ◆ Index 1:
 - ✓ 'Call Setup Rules Set ID': **3**
 - ✓ 'Destination IP Group ID': **3** (IP Group for Skype for Business)
 - ◆ Index 2:
 - ✓ 'Destination IP Group ID': **4** (IP Group of PBX)

- **Example 4:** The example enables routing based on LDAP queries and destination tags. The device queries the LDAP server for the attribute record "telephoneNumber" whose value is the destination number of the incoming call (e.g., "telephoneNumber=4064"). If the attribute-value combination is found, the device retrieves the string value of the attribute record "ofiSBCRouting" and creates a destination tag with the name of the retrieved string. The destination tag is then used as a matching characteristics in the IP-to-IP Routing table.
 - Call Setup Rules table:
 - ◆ 'Rules Set ID': **4**
 - ◆ 'Query Type': **LDAP**
 - ◆ 'Query Target': **LDAP-DC-CORP**
 - ◆ 'Search Key': **'telephoneNumber='+param.call.dst.user**
 - ◆ 'Attributes to Get': **ofiSBCRouting**
 - ◆ 'Row Role': **Use Current Condition**
 - ◆ 'Condition': **ldap.found exists**
 - ◆ 'Action Subject': **dsttags**
 - ◆ 'Action Type': **Modify**
 - ◆ 'Action Value': **ldap.attr.ofiSBCrouting**
 - IP Groups table: 'Call Setup Rules Set ID': **4**
 - IP-to-IP Routing table:
 - ◆ Index 1:
'Destination Tag': **dep-sales**
'Destination IP Group': **SALES**
 - ◆ Index 2:
'Destination Tag': **dep-mkt**
'Destination IP Group': **MKT**
 - ◆ Index 3:
'Destination Tag': **dep-rd**
'Destination IP Group': **RD**

This page is intentionally left blank.

21 Coders and Profiles

This section describes configuration of the coders and SIP profiles parameters.

21.1 Configuring Coder Groups

The Coder Groups table lets you configure up to 21 *Coder Groups*. The Coder Group determines the audio (voice) coders used for calls. Each Coder Group can include up to 10 coders, where the packetization time (ptime), bit rate, payload type, and silence suppression can be configured per coder. The first coder in the Coder Group has the highest priority and is used by the device whenever possible. If the remote side cannot use the first coder, the device attempts to use the next coder in the Coder Group, and so on.

The Coder Groups table provides a pre-defined Coder Group (index 0) that is configured with the G.711 A-law coder. If no other Coder Groups are configured, the default Coder Group (which you can modify) is used for all calls. Alternatively, if you want to use specific coders or coder settings (e.g., packetization time) for different calls (entities), you need to configure a Coder Group for each entity and then assign each Coder Group to the IP Profile (see "Configuring IP Profiles" on page 388) associated with the entity (IP Group). If an IP Group is not associated with a Coder Group, the default Coder Group is used.

You can also use Coder Groups for audio coder transcoding of SBC calls. If two SIP entities need to communicate, but one does not support a coder required by the other, the device can add the required coder to the SDP offer. The added coder is referred to as an extension coder. For more information on extension coders, see Coder Transcoding on page 435.

To apply a Coder Group for transcoding to a SIP entity:

1. Configure a Coder Group in the Coder Groups table (see description below).
2. In the IP Profile associated with the SIP entity (see Configuring IP Profiles on page 388):
 - Assign the Coder Group (using the `IpProfile_SBCExtensionCodersGroupName` parameter).
 - Enable the use of the Coder Group for transcoding (by configuring the `IpProfile_SBCAllowedCodersMode` parameter to `Restriction` or `Restriction and Preference`).



Note:

- For supported audio coders, see "Supported Audio Coders" on page 382.
- Some coders are license-dependent and are available only if purchased from AudioCodes and included in the License Key installed on your device. For more information, contact your AudioCodes sales representative.
- Only the packetization time of the first coder listed in the Coder Group is declared in INVITE/200 OK SDP even if multiple coders are configured. The device always uses the packetization time requested by the remote side for sending RTP packets. If not specified, the packetization time is assigned the default value.
- The value of some fields is hard-coded according to common standards (e.g., payload type of G.711 U-law is always 0).
- The G.722 coder provides Packet Loss Concealment (PLC) capabilities, ensuring higher voice quality.
- Opus coder:
 - ✓ If one leg uses a narrowband coder (e.g., G.711) and the other leg uses the Opus coder, the device maintains the narrowband coder flavor by using the narrowband Opus coder. Alternatively, if one leg uses a wideband coder (e.g., G.722) and the other leg uses the Opus coder, the device maintains the wideband coder flavor by using the wideband Opus coder.
- For more information on V.152 and implementation of T.38 and VBD coders, see "Supporting V.152 Implementation" on page 185.

The following procedure describes how to configure the Coder Groups table through the Web interface. You can also configure it through ini file (AudioCodersGroups and AudioCoders) or CLI (configure voip > coders-and-profiles audio-coders-groups).

➤ **To configure a Coder Group:**

1. Open the Coder Groups table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **Coder Groups**).

Figure 21-1: Coder Group Table

Coder Group Name

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

2. From the 'Coder Group Name' drop-down list, select the desired Coder Group index number and name.
3. Configure the Coder Group according to the parameters described in the table below.
4. Click **Apply**, and then reset the device with a save-to-flash for your settings to take effect.

You can delete a Coder Group, as described in the following procedure.

➤ **To delete a Coder Group:**

1. From the 'Coder Group Name' drop-down list, select the Coder Group that you want to delete.
2. Click **Delete Group**.

Table 21-1: Coder Groups Table Parameter Descriptions

Parameter	Description
Coder Group Name [AudioCodersGroups_Index] [AudioCodersGroups_Name]	Defines the name and index for the Coder Group. Note: The Coder Group index/name cannot be configured.
[AudioCoders_AudioCodersIndex]	Index row of the coder per Coder Group Note: The parameter is applicable only to the ini file.
Coder Name name [AudioCoders_Name]	Defines the coder type. For coder names, see "Supported Audio Coders" on page 382. Note: Each coder type (e.g., G.729) can be configured only once in the table.
Packetization Time p-time [AudioCoders_pTime]	Defines the packetization time (in msec) for the coder. The packetization time determines how many coder payloads are combined into a single RTP packet. For ptime, see "Supported Audio Coders" on page 382.
Rate rate [AudioCoders_rate]	Defines the bit rate (in kbps) for the coder. For rates, see "Supported Audio Coders" on page 382.
Payload Type payload-type [AudioCoders_PayloadType]	Defines the payload type if the payload type (i.e., format of the RTP payload) for the coder is dynamic. For payload types, see "Supported Audio Coders" on page 382.
Silence Suppression silence-suppression [AudioCoders_Sce]	Enables silence suppression for the coder. <ul style="list-style-type: none"> ▪ [0] Disable (Default) ▪ [1] Enable ▪ [2] Enable w/o Adaptation Note: <ul style="list-style-type: none"> ▪ If you disable silence suppression for a coder, the settings of the EnableSilenceCompression parameter is applied. ▪ Option [2] Enable w/o Adaptation is applicable only to G.729. ▪ If you disable silence suppression for G.729, the device includes 'annexb=no' in the SDP of the relevant SIP messages. If you enable silence suppression, 'annexb=yes' is included. An exception is when the remote gateway is Cisco equipment (IsCiscoSCEMode).
Coder Specific coder-specific [AudioCoders_CoderSpecific]	Defines additional settings specific to the coder. Currently, the parameter is applicable only to the AMR coder and is used to configure the payload format type. <ul style="list-style-type: none"> ▪ [0] 0 = Bandwidth Efficient ▪ [1] 1 = Octet Aligned (default)

Parameter	Description
	Note: The AMR payload type can be configured globally using the AmrOctetAlignedEnable parameter. However, the Coder Group configuration overrides the global parameter.

21.1.1 Supported Audio Coders

The table below lists the coders supported by the device.

Table 21-2: Supported Audio Coders

Coder Name	Packetization Time (msec)	Rate (kbps)	Payload Type	Silence Suppression
	[1] 10, [2] 20, [3] 30, [4] 40, [5] 50, [6] 60, [8] 80, [9] 90, [10] 100, [12] 120			
G.711 A-law g711-alaw [1]	10, 20 (default), 30, 40, 50, 60, 80, 100, 120	[90] 64	8	<ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable
G.711 U-law g711-ulaw [2]	10, 20 (default), 30, 40, 50, 60, 80, 100, 120	[90] 64	0	<ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable
G.711A-law_VBD g711a-law-vbd [23]	10, 20 (default), 30, 40, 50, 60, 80, 100, 120	[90] 64	8 or Dynamic (default 118)	N/A
G.711U-law_VBD g711u-law-vbd [24]	10, 20 (default), 30, 40, 50, 60, 80, 100, 120	[90] 64	0 or Dynamic (default 110)	N/A
G.722 g722 [20]	20 (default), 40, 60, 80, 100, 120	[90] 64 (default)	9	N/A
G.723.1 g723-1 [0]	30 (default), 60, 90, 120, 150	<ul style="list-style-type: none"> ▪ [7] 5.3 (default) ▪ [11] 6.3 	4	<ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable
G.726 g726 [5]	10, 20 (default), 30, 40, 50, 60, 80	<ul style="list-style-type: none"> ▪ [43] 16 ▪ [57] 24 ▪ [64] 32 (default) ▪ [70] 40 	Dynamic (default 2)	<ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable
G.729 g729 [3]	10, 20 (default), 30, 40, 50, 60, 80, 100	[19] 8	18	<ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable ▪ [2] Enable w/o Adaptation

Coder Name	Packetization Time (msec) [1] 10, [2] 20, [3] 30, [4] 40, [5] 50, [6] 60, [8] 80, [9] 90, [10] 100, [12] 120	Rate (kbps)	Payload Type	Silence Suppression
				s
AMR amr [14]	20 (default)	<ul style="list-style-type: none"> ▪ [4] 4.75 ▪ [6] 5.15 ▪ [9] 5.90 ▪ [14] 6.70 ▪ [16] 7.40 ▪ [18] 7.95 ▪ [27] 10.2 ▪ [30] 12.2 (default) 	Dynamic	<ul style="list-style-type: none"> ▪ [0] Disable ▪ [1] Enable
AMR-WB amr-wb [15]	20 (default)	<ul style="list-style-type: none"> ▪ [13] 6.6 ▪ [21] 8.85 ▪ [32] 12.65 ▪ [37] 14.25 ▪ [41] 15.85 ▪ [48] 18.25 ▪ [49] 19.85 ▪ [53] 23.05 ▪ [55] 23.8 (default) 	Dynamic	<ul style="list-style-type: none"> ▪ [0] Disable ▪ [1] Enable
SILK-NB silk-nb [35]	20 (default), 40, 60, 80, and 100	[19] 8	Dynamic (default 76)	N/A
SILK-WB silk-wb [36]	20 (default), 40, 60, 80, and 100	[43] 16	Dynamic (default 77)	N/A
T.38 t-38 [4]	N/A	N/A	N/A	N/A
Opus opus [40]	20 (default), 40, 60, 80, 120	N/A	Dynamic (default 111)	N/A

21.1.2 Configuring Various Codec Attributes

The following procedure describes how to configure various coder attributes such as bitrate.

➤ **To configure codec attributes:**

1. Open the Coder Settings page (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **Coder Settings**).

2. Configure the following parameters:

- AMR coder:
 - ◆ 'AMR Payload Format' (AmrOctetAlignedEnable): Defines the AMR payload format type:

AMR CODER

AMR Payload Format Octet Aligned ▼

- SILK coder (Skype's default audio codec):
 - ◆ 'Silk Tx Inband FEC': Enables forward error correction (FEC) for the SILK coder.
 - ◆ 'Silk Max Average Bit Rate': Defines the maximum average bit rate for the SILK coder.

Figure 21-2: Configuring SILK Coder Attributes

SILK CODER

SILK Tx Inband FEC Disable ▼

SILK Max Average Bit Rate 50000

- Opus coder:
 - ◆ 'Opus Max Average Bitrate' (OpusMaxAverageBitRate): Defines the maximum average bit rate (in bps) for the Opus coder.

Figure 21-3: Configuring Opus Coder Attributes

OPUS CODER

Opus Max Average Bitrate [bps] 50000

3. Click **Apply**.

21.2 Configuring Allowed Audio Coder Groups

The Allowed Audio Coders Groups table lets you configure up to 20 Allowed Audio Coders Groups. For each Allowed Audio Coders Group, you can configure up to 10 audio coders. The coders can include pre-defined coders and user-defined (string) coders for non-standard or unknown coders.

Allowed Audio Coders Groups restrict coders for SIP entities. Only coders listed in the Allowed Audio Coders Group (i.e., allowed coders) that is associated with the SIP entity can be used. If the coders in the SDP offer ('a=rtpmap' field) of the incoming SIP message are not listed in the Allowed Audio Coders Group, the device rejects the calls, unless transcoding is configured, whereby "extension" coders are added to the SDP, as described in Coder Transcoding on page 435. If the SDP offer contains some coders that are listed in the Allowed Audio Coders Group, the device manipulates the SDP offer by removing the coders that are not listed in the Allowed Audio Coders Group, before routing the SIP message to its destination. Thus, only coders that are common between the coders in the SDP offer and the coders in the Allowed Audio Coders Group are used. For more information on coder restriction, see "Restricting Audio Coders" on page 434.

For example, assume the following:

- The SDP offer in the incoming SIP message contains the G.729, G.711, and G.723 coders.
- The allowed coders configured for the SIP entity include G.711 and G.729.

The device removes the G.723 coder from the SDP offer, re-orders the coder list so that G.711 is listed first, and sends the SIP message containing only the G.711 and G.729 coders in the SDP.

To apply an Allowed Audio Coders Group for restricting coders to a SIP entity:

1. Configure an Allowed Audio Coders Group in the Allowed Audio Coders Groups table (see description below).
2. In the IP Profile associated with the SIP entity (see "Configuring IP Profiles" on page 388):
 - Assign the Allowed Audio Coders Group (using the `IpProfile_SBCAllowedAudioCodersGroupName` parameter).
 - Enable the use of Allowed Audio Coders Groups (by configuring the `IpProfile_SBCAllowedCodersMode` parameter to **Restriction** or **Restriction and Preference**).

The device also re-orders (prioritizes) the coder list in the SDP according to the order of appearance of the coders listed in the Allowed Audio Coders Group. The first listed coder has the highest priority and the last coder has the lowest priority. For more information, see "Prioritizing Coder List in SDP Offer" on page 438.



Note:

- The Allowed Audio Coders Group for coder restriction takes precedence over the Coder Group for extension coders. In other words, if an extension coder is not listed as an allowed coder, the device does not add the extension coder to the SDP offer.
- To configure "extension" coders for adding to the SDP offer for audio transcoding, use the Coder Groups table (see Configuring Coder Groups on page 379).

The following procedure describes how to configure Allowed Audio Coders Groups through the Web interface. You can also configure it through ini file (`AllowedAudioCodersGroups` and `AllowedAudioCoders`) or CLI (`configure voip > coders-and-profiles allowed-audio-coders-groups; configure voip > coders-and-profiles allowed-audio-coders <group index/coder index>`).

➤ **To configure an Allowed Audio Coders Group:**

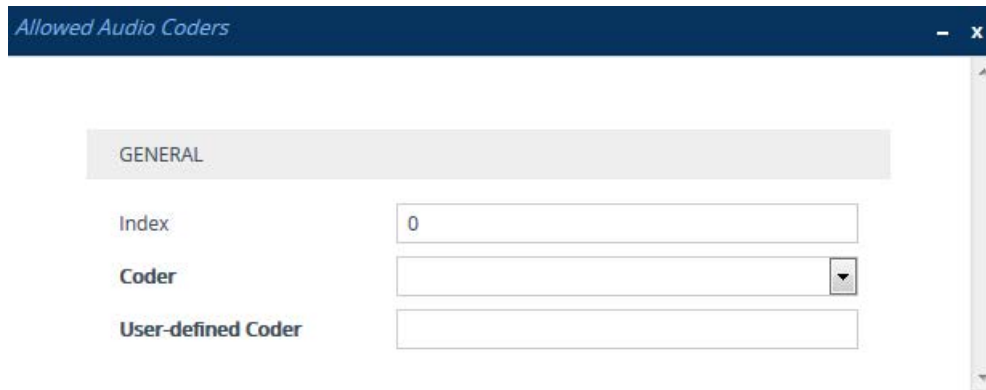
1. Open the Allowed Audio Coders Groups table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **Allowed Audio Coders Groups**).
2. Click **New**; the following dialog box appears:

Figure 21-4: Allowed Audio Coders Groups table - Add Dialog Box

The screenshot shows a dialog box titled "Allowed Audio Coders Groups". It has a "GENERAL" tab selected. There are two input fields: "Index" with the value "0" and "Name" which is currently empty.

3. Configure a name for the Allowed Audio Coders Group according to the parameters described in the table below.
4. Click **Apply**.

5. Select the new row that you configured, and then click the **Allowed Audio Coders** link located below the table; the Allowed Audio Coders table opens.
6. Click **New**; the following dialog box appears:

Figure 21-5: Allowed Audio Coders Table - Add Dialog Box


7. Configure coders for the Allowed Audio Coders Group according to the parameters described in the table below.
8. Click **Apply**.

Table 21-3: Allowed Audio Coders Groups and Allowed Audio Coders Tables Parameter Descriptions

Parameter	Description
Allowed Audio Coders Groups Table	
Index allowed-audio-coders-groups <index> [AllowedAudioCodersGroups_Index]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
Name coders-group-name [AllowedAudioCodersGroups_Name]	Defines an arbitrary name to easily identify the row. The valid value is a string of up to 41 characters. Note: Each row must be configured with a unique name.
Allowed Audio Coders Table	
Index allowed-audio-coders <group index/coder index> [AllowedAudioCoders_AllowedAudioCodersIndex]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
Coder coder [AllowedAudioCoders_CoderID]	Selects a coder from the list of coders. Note: Each coder can be configured only once per Allowed Audio Coders Group.
User-defined Coder user-define-coder [AllowedAudioCoders_UserDefineCoder]	Defines a user-defined coder. The valid value is a string of up to 24 characters (case-insensitive). For example, "HD.123" (without quotes). Note: Each coder can be configured only once per Allowed Audio Coders Group.

21.3 Configuring Allowed Video Coder Groups

The Allowed Video Coders Groups table lets you configure up to four Allowed Video Coders Groups. Each Allowed Video Coders Group can be configured with up to 10 coders. An Allowed Video Coders Group defines a list of video coders that can be used when forwarding video streams to a specific SIP entity. The coders can include pre-defined video coders and user-defined (string) video coders for non-standard or unknown coders.

Allowed Video Coders Groups are assigned to SIP entities, using IP Profiles (see "Configuring IP Profiles" on page 388). The video coders appear in the SDP media type "video" ('m=video' line). Coders that are not listed in the Allowed Video Coders Group are removed from the SDP offer that is sent to the SIP entity. Only coders that are common between the coders in the SDP offer and the coders listed in the Allowed Video Coders Group are used. Thus, Allowed Video Coders Groups enable you to enforce the use of only specified coders. For more information, see "Restricting Audio Coders" on page 434.

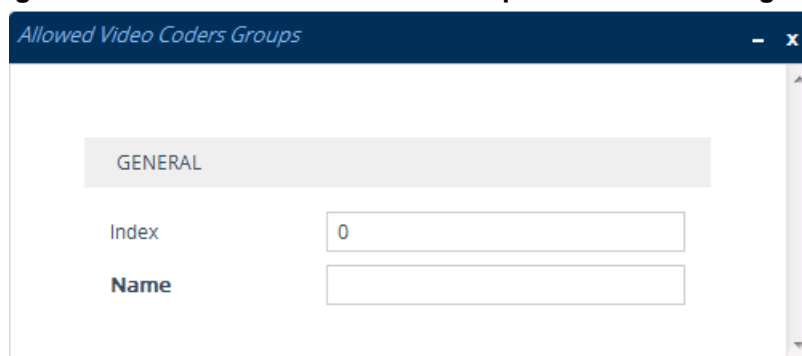
The order of appearance of the coders listed in the Allowed Video Coders Group determines the priority (preference) of the coders in the SDP offer. The device arranges the SDP offer's coder list according to their order in the Allowed Video Coders Group. The priority is in descending order, whereby the first coder in the list is given the highest priority and the last coder, the lowest priority. For more information, see "Prioritizing Coder List in SDP Offer" on page 438.

The following procedure describes how to configure Allowed Video Coders Groups through the Web interface. You can also configure it through ini file (AllowedVideoCodersGroups and AllowedVideoCoders) or CLI (configure voip > coders-and-profiles allowed-video-coders-groups; configure voip > coders-and-profiles allowed-video-coders <group index/coder index>).

➤ **To configure an Allowed Video Coders Group:**

1. Open the Allowed Video Coders Groups table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **Allowed Video Coders Groups**).
2. Click **New**; the following dialog box appears:

Figure 21-6: Allowed Video Coders Groups Table - Add Dialog Box

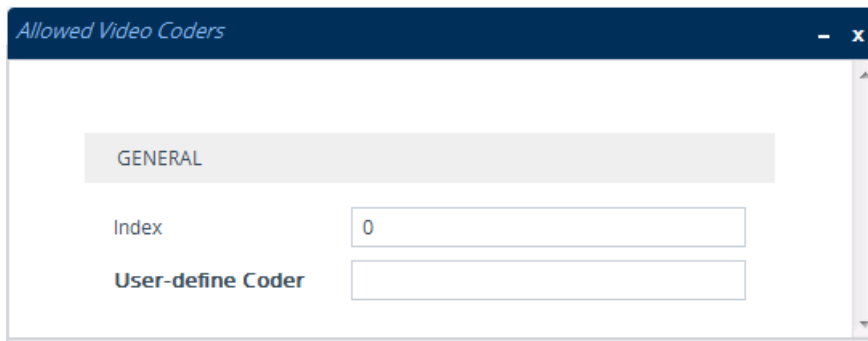


GENERAL	
Index	<input type="text" value="0"/>
Name	<input type="text"/>

3. Configure a name for the Allowed Video Coders Group according to the parameters described in the table below.
4. Click **Apply**.
5. Select the new row that you configured, and then click the **Allowed Video Coders** link located below the table; the Allowed Video Coders table opens.

- Click **New**; the following dialog box appears:

Figure 21-7: Allowed Video Coders Table - Add Dialog Box



- Configure coders for the Allowed Video Coders Group according to the parameters described in the table below.
- Click **Apply**.

Table 21-4: Allowed Video Coders Groups and Allowed Video Coders Tables Parameter Descriptions

Parameter	Description
Allowed Video Coders Groups Table	
Index allowed-video-coders-groups <index> [AllowedVideoCodersGroups_Index]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
Name coders-group-name [AllowedVideoCodersGroups_Name]	Defines an arbitrary name to easily identify the row. The valid value is a string of up to 41 characters. Note: Each row must be configured with a unique name.
Allowed Video Coders Table	
Index allowed-video-coders <group index/coder index> [AllowedVideoCoders_AllowedVideoCodersIndex]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
User Define Coder user-define-coder [AllowedVideoCoders_UserDefineCoder]	Defines a user-defined coder. The valid value is a string of up to 24 characters (case-insensitive). For example, "HD.123" (without quotes). Note: Each coder can be configured only once per Allowed Video Coders Group.

21.4 Configuring IP Profiles

The IP Profiles table lets you configure up to 300 IP Profiles. An IP Profile is a set of parameters with user-defined settings relating to signaling (e.g., SIP message terminations such as REFER) and media (e.g., coder type). An IP Profile can later be assigned to specific IP calls (inbound and/or outbound). Thus, IP Profiles provide high-level adaptation when the device interworks between different IP entities, each of which may require different handling by the device. This can include, for example, transcoding or even

transrating (of packetization time). 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.

To use your IP Profile for specific calls, you need to assign it to any of the following:

- IP Groups - see "Configuring IP Groups" on page 329

Many of the parameters in the IP Profiles table have a corresponding "global" parameter. For calls that are not associated with any IP Profile, the settings of the "global" parameters are applied.



Note: IP Profiles can also be implemented when using a Proxy server (when the AlwaysUseRouteTable parameter is set to 1).

The following procedure describes how to configure IP Profiles through the Web interface. You can also configure it through ini file (IPProfile) or CLI (configure voip > coders-and-profiles ip-profile).

➤ **To configure an IP Profile:**

1. Open the IP Profiles table (**Setup** menu > **Signaling & Media** tab > **Coders & Profiles** folder > **IP Profiles**).
2. Click **New**; the following dialog box appears:

Figure 21-8: IP Profiles Table - Add Dialog Box

3. Configure an IP Profile according to the parameters described in the table below.
4. Click **Apply**.

Table 21-5: IP Profiles Table Parameter Descriptions

Parameter	Description
General	
Index [IpProfile_Index]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
Name	Defines an arbitrary name to easily identify the row.

Parameter	Description
profile-name [IpProfile_ProfileName]	The valid value is a string of up to 40 characters.
Media Security	
SBC Media Security Mode sbc-media-security-behaviour [IpProfile_SBCMediaSecurityBehaviour]	Defines the handling of RTP and SRTP for the SIP entity associated with the IP Profile. <ul style="list-style-type: none"> ▪ [0] As is = (Default) No special handling for RTP\SRTP is done. ▪ [1] SRTP = SBC legs negotiate only SRTP media lines, and RTP media lines are removed from the incoming SDP offer-answer. ▪ [2] RTP = SBC legs negotiate only RTP media lines, and SRTP media lines are removed from the incoming offer-answer. ▪ [3] Both = Each offer-answer is extended (if not already) to two media lines - one RTP and the other SRTP. 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: <ul style="list-style-type: none"> ▪ At least one supported SDP "crypto" attribute and parameters. ▪ EnableMediaSecurity must be set to 1. If one of the above transcoding prerequisites is not met, then: <ul style="list-style-type: none"> ▪ any value other than "As is" is discarded. ▪ if the incoming offer is SRTP, force transcoding, coder transcoding, and DTMF extensions are not applied.
Symmetric MKI enable-symmetric-mki [IpProfile_EnableSymmetricMKI]	Enables symmetric MKI negotiation. <ul style="list-style-type: none"> ▪ [0] Disable = (Default) The device includes the MKI in its SIP 200 OK response according to the SRTPTxPacketMKISize parameter (if set to 0, it is not included; if set to any other value, it is included with this value). ▪ [1] 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 data-bbox="708 1592 1390 1778"> 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:bnuYZnMxSfUiGitviWJZmzr70F3AiRO015Vnh0kH 2^31 </pre> 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

Parameter	Description
	<p>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:R1VyAlxV/qwBjkEklU4kSJy13wCtYeZLq1/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>Note: The corresponding global parameter is EnableSymmetricMKI.</p>
<p>MKI Size mki-size [IpProfile_MKISize]</p>	<p>Defines the size (in bytes) of the Master Key Identifier (MKI) in SRTP Tx packets.</p> <p>The valid value is 0 to 4. The default is 0 (i.e., new keys are generated without MKI).</p> <p>Note:</p> <ul style="list-style-type: none"> ▪ The device can forward MKI size as is for SRTP-to-SRTP flows or override the MKI size during negotiation. This can be done on the inbound or outbound leg. ▪ The corresponding global parameter is SRTPTxPacketMKISize.
<p>SBC Enforce MKI Size sbc-enforce-mki-size [IpProfile_SBCEnforceMKISize]</p>	<p>Enables negotiation of the Master Key Identifier (MKI) length for SRTP-to-SRTP flows between SIP networks (i.e., IP Groups). This includes the capability of modifying the MKI length on the inbound or outbound SBC call leg for the SIP entity associated with the IP Profile.</p> <ul style="list-style-type: none"> ▪ [0] Don't enforce = (Default) Device forwards the MKI size as is. ▪ [1] Enforce = Device changes the MKI length according to the settings of the IP Profile parameter, MKISize.
<p>SBC Media Security Method sbc-media-security-method [IpProfile_SBCMediaSecurityMethod]</p>	<p>Defines the media security protocol for SRTP, for the SIP entity associated with the IP Profile.</p> <ul style="list-style-type: none"> ▪ [0] SDES = (Default) The device secures RTP using the Session Description Protocol Security Descriptions (SDES) protocol to negotiate the cryptographic keys (RFC 4568). The keys are sent in the SDP body ('a=crypto') of the SIP message and are typically secured using SIP over TLS (SIPS). The encryption of the keys is in plain text in the SDP. SDES implements TLS over TCP. ▪ [1] DTLS = The device uses Datagram Transport Layer Security (DTLS) protocol to secure UDP-based media streams (RFCs 5763 and 5764). For more information on DTLS, see SRTP using DTLS Protocol on page 199. ▪ [2] Both = SDES and DTLS protocols are supported. <p>Note:</p> <ul style="list-style-type: none"> ▪ To support DTLS, you must also configure the following for the SIP entity: <ul style="list-style-type: none"> ✓ TLS Context for DTLS (see Configuring TLS

Parameter	Description
	<p>Certificate Contexts on page 99). The server cipher ('Cipher Server') must be configured to All.</p> <ul style="list-style-type: none"> ✓ IpProfile_SBCMediaSecurityBehaviourMedia configured to SRTP or Both. ✓ IpProfile_SBCRTCPMux configured to Supported. The setting is required as the DTLS handshake is done for the port used for RTP. Therefore, RTCP and RTP should be multiplexed over the same port. <ul style="list-style-type: none"> ▪ The device does not support forwarding of DTLS transparently between endpoints (SIP entities). ▪ As DTLS has been defined by the WebRTC standard as mandatory for encrypting media channels for SRTP key exchange, the support is important for deployments implementing WebRTC. For more information on WebRTC, see WebRTC on page 524.
Reset SRTP Upon Re-key reset-srtp-upon-re-key [IpProfile_ResetSRTPStateUponRekey]	<p>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.</p> <ul style="list-style-type: none"> ▪ [0] Disable = (Default) ROC is not reset on the device side. ▪ [1] Enable = 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. <p>Note:</p> <ul style="list-style-type: none"> ▪ If this feature is disabled and the server resets the ROC upon a re-key generation, one-way voice may occur. ▪ The corresponding global parameter is ResetSRTPStateUponRekey.
Generate SRTP Keys Mode generate-srtp-keys [IpProfile_GenerateSRTPKeys]	<p>Enables the device to generate a new SRTP key upon receipt of a re-INVITE with the SIP entity associated with the IP Profile.</p> <ul style="list-style-type: none"> ▪ [0] Only If Required= (Default) The device generates an SRTP key only if necessary. ▪ [1] Always = The device always generates a new SRTP key.
SBC Remove Crypto Lifetime in SDP sbc-sdp-remove-crypto-lifetime [IpProfile_SBCRemoveCryptoLifetimeInSDP]	<p>Defines the handling of the lifetime field in the 'a=crypto' attribute of the SDP for the SIP entity associated with the IP Profile. The SDP field defines the lifetime of the master key as measured in maximum number of SRTP or SRTCP packets using the master key.</p> <ul style="list-style-type: none"> ▪ [0] No = (Default) The device retains the lifetime field (if present) in the SDP. ▪ [1] Yes = The device removes the lifetime field from the 'a=crypto' attribute. <p>Note: If you configure the parameter to Yes, the following IP Profile parameters must be configured as follows:</p>

Parameter	Description
	<ul style="list-style-type: none"> ▪ IpProfile_EnableSymmetricMKI configured to Enable [1]. ▪ IpProfile_MKISize configured to 0. ▪ IpProfile_SBCEnforceMKISize configured to Enforce [1].
SBC Early Media	
Remote Early Media sbc-rmt-early-media-supp [IpProfile_SBCRemoteEarlyMediaSupport]	Defines whether the remote side can accept early media or not. <ul style="list-style-type: none"> ▪ [0] Not Supported = Early media is not supported. ▪ [1] Supported = (Default) Early media is supported.
Remote Multiple 18x sbc-rmt-mltple-18x-supp [IpProfile_SBCRemoteMultiple18xSupport]	Defines whether multiple 18x responses including 180 Ringing, 181 Call is Being Forwarded, 182 Call Queued, and 183 Session Progress are forwarded to the caller, for the SIP entity associated with the IP Profile. <ul style="list-style-type: none"> ▪ [0] Not Supported = Only the first 18x response is forwarded to the caller. ▪ [1] Supported = (Default) Multiple 18x responses are forwarded to the caller.
Remote Early Media Response Type sbc-rmt-early-media-resp [IpProfile_SBCRemoteEarlyMediaResponseType]	Defines the SIP provisional response type - 180 or 183 - for forwarding early media to the caller, for the SIP entity associated with the IP Profile. <ul style="list-style-type: none"> ▪ [0] Transparent = (Default) All early media response types are supported; the device forwards all responses as is (unchanged). ▪ [1] 180 = Early media is sent as 180 response only. ▪ [2] 183 = Early media is sent as 183 response only.
Remote Multiple Early Dialogs sbc-multi-early-diag [IpProfile_SBCRemoteMultipleEarlyDialogs]	Defines the device's handling of To-header tags in call forking responses (i.e., multiple SDP answers) sent to the SIP entity associated with the IP Profile. When the SIP entity initiates an INVITE that is subsequently forked (for example, by a proxy server) to multiple endpoints, the endpoints respond with a SIP 183 containing an SDP answer. Typically, each endpoint's response has a different To-header tag. For example, a call initiated by the SIP entity (100@A) is forked and two endpoints respond with ringing, each with a different tag: <ul style="list-style-type: none"> ▪ Endpoint "tag 2": SIP/2.0 180 Ringing From: <sip:100@A>;tag=tag1 To: sip:200@B;tag=tag2 Call-ID: c2 ▪ Endpoint "tag 3": SIP/2.0 180 Ringing From: <sip:100@A>;tag=tag1 To: sip:200@B;tag=tag3 Call-ID: c2 In non-standard behavior (when the parameter is configured to Disable), the device forwards all the SDP answers with the same tag. In the example, endpoint "tag 3" is sent with the same tag as endpoint "tag 2" (i.e., To: sip:200@B;tag=tag2).

Parameter	Description
	<ul style="list-style-type: none"> ▪ [-1] According to Operation Mode = (Default) Depends on the setting of the 'Operation Mode' parameter in the IP Group or SRDs table: <ul style="list-style-type: none"> ✓ B2BUA: Device operates as if the parameter is set to Disable [0]. ✓ Call State-full Proxy: Device operates as if the parameter is set to Enable [1]. In addition, the device preserves the From tags and Call-IDs of the endpoints in the SDP answer sent to the SIP entity. ▪ [0] Disable = Device sends the multiple SDP answers with the same To-header tag, to the SIP entity. In other words, this option is relevant if the SIP entity does not support multiple dialogs (and multiple tags). However, non-standard, multiple answer support may still be configured by the SBCRemoteMultipleAnswersMode parameter. ▪ [1] Enable = Device sends the multiple SDP answers with different To-header tags, to the SIP entity. In other words, the SIP entity supports standard multiple SDP answers (with different To-header tags). In this case, the SBCRemoteMultipleAnswersMode parameter is ignored. <p>Note: If the parameter and the SBCRemoteMultipleAnswersMode parameter are disabled, multiple SDP answers are not reflected to the SIP entity (i.e., the device sends the same SDP answer in multiple 18x and 200 responses).</p>
Remote Multiple Answers Mode sbc-multi-answers [IpProfile_SBCRemoteMultipleAnswersMode]	Enables interworking multiple SDP answers within the same SIP dialog (non-standard). The parameter enables the device to forward multiple answers to the SIP entity associated with the IP Profile. The parameter is applicable only when the IpProfile_SBCRemoteMultipleEarlyDialogs parameter is disabled. <ul style="list-style-type: none"> ▪ [0] Disable = (Default) Device always sends the same SDP answer, which is based on the first received answer that it sent to the SIP entity, for all forked responses (even if 'Forking Handling Mode' is Sequential), and thus, may result in transcoding. ▪ [1] Enable = If the 'Forking Handling Mode' parameter is configured to Sequential, the device sends multiple SDP answers.
Remote Early Media RTP Detection Mode sbc-rmt-early-media-rtp [IpProfile_SBCRemoteEarlyMediaRTP]	Defines whether the destination UA sends RTP immediately after it sends a 18x response. <ul style="list-style-type: none"> ▪ [0] By Signaling = (Default) Remote client sends RTP immediately after it sends 18x response with early media. The device forwards 18x and RTP as is. ▪ [1] By Media = After sending 18x response, the remote client waits before sending RTP (e.g., Microsoft Skype for Business environment). For the device's handling of this remote UA support, see Interworking SIP Early Media on page 447.
Remote RFC 3960 Support sbc-rmt-rfc3960-supp	Defines whether the destination UA is capable of receiving 18x messages with delayed RTP.

Parameter	Description
[IpProfile_SBCRemoteSupportsRFC3960]	<ul style="list-style-type: none"> ▪ [0] 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 on page 447. ▪ [1] Supported = UA is capable of receiving 18x messages with delayed RTP.
Remote Can Play Ringback sbc-rmt-can-play-ringback [IpProfile_SBCRemoteCanPlayRingback]	<p>Defines whether the destination UA can play a local ringback tone.</p> <ul style="list-style-type: none"> ▪ [0] No = UA does not support local ringback tone. The device sends 18x with delayed SDP to the UA. ▪ [1] Yes = (Default) UA supports local ringback tone. For the device's handling of this remote UA support, see Interworking SIP Early Media on page 447.
Generate RTP sbc-generate-rtp [IPProfile_SBCGenerateRTP]	<p>Enables the device to generate "silence" RTP packets to the SIP entity until it detects audio RTP packets from the SIP entity. The parameter provides support for interworking with SIP entities that wait for the first incoming packets before sending RTP (e.g., early media used for ringback tone or IVR) during media negotiation.</p> <ul style="list-style-type: none"> ▪ [0] None (Default) = Silence packets are not generated. ▪ [1] Until RTP Detected = The device generates silence RTP packets to the SIP entity upon receipt of a SIP response (183 with SDP) from the SIP entity. In other words, these packets serve as the first incoming packets for the SIP entity. The device stops sending silence packets when it receives RTP packets from the peer side (which it then forwards to the SIP entity). <p>Note: To generate silence packets, DSP resources are required (except for calls using the G.711 coder).</p>
SBC Media	
Transcoding Mode transcoding-mode [IpProfile_TranscodingMode]	<p>Defines the transcoding mode (media negotiation) for the SIP entity associated with the IP Profile.</p> <ul style="list-style-type: none"> ▪ [0] Only if Required = (Default) Transcoding is done only when necessary. Many of the media settings (such as gain control) are not implemented on the voice stream. The device forwards RTP packets transparently (RTP-to-RTP), without processing them. ▪ [1] Force = Transcoding is always done on the outgoing leg. The device interworks the media for the SIP entity (as both legs have different media capabilities), by implementing DSP transcoding. This enables the device to receive capabilities that are not negotiated between the SIP entities. For example, it can enforce gain control to use voice transcoding even though both legs have negotiated without the device's intervention (such as extension coders). <p>For more information on extension coders and transcoding, see Coder Transcoding on page 435,</p> <p>Note:</p> <ul style="list-style-type: none"> ▪ To implement transcoding, you must configure the number of required DSP channels for transcoding (using

Parameter	Description
	<p>the MediaChannels parameter). Each transcoding session uses two DSP resources.</p> <ul style="list-style-type: none"> The corresponding global parameter is TranscodingMode.
Extension Coders Group sbc-ext-coders-group-name [IpProfile_SBCExtensionCodersGroupName]	<p>Assigns a Coder Group used for extension coders, added to the SDP offer in the outgoing leg for the SIP entity associated with the IP Profile. This is used when transcoding is required between two IP entities (i.e., the SDP answer from one doesn't include any coder included in the offer previously sent by the other).</p> <p>For more information on extension coders and transcoding, see Coder Transcoding on page 435, To configure Coder Groups, see Configuring Coder Groups on page 379.</p>
Allowed Audio Coders allowed-audio-coders-group-name [IpProfile_SBCAllowedAudioCodersGroupName]	<p>Assigns an Allowed Audio Coders Group, which defines audio (voice) coders that can be used for the SIP entity associated with the IP Profile.</p> <p>To configure Allowed Audio Coders Groups, see Configuring Allowed Audio Coder Groups on page 384. For a description of the Allowed Coders feature, see "Restricting Coders" on page 434.</p>
Allowed Coders Mode sbc-allowed-coders-mode [IpProfile_SBCAllowedCodersMode]	<p>Defines the mode of the Allowed Coders feature for the SIP entity associated with the IP Profile.</p> <ul style="list-style-type: none"> [0] Restriction = In the incoming SDP offer, the device uses only Allowed coders; the rest are removed from the SDP offer (i.e., only coders common between those in the received SDP offer and the Allowed coders are used). If an Extension Coders Group is also assigned (using the 'Extension Coders Group' parameter, above), these coders are added to the SDP offer if they also appear in Allowed coders. [1] Preference = The device re-arranges the priority (order) of the coders in the incoming SDP offer according to their order of appearance in the Allowed Audio Coders Group or Allowed Video Coders Group. The coders in the original SDP offer are listed after the Allowed coders. [2] Restriction and Preference = Performs both Restriction and Preference. <p>Note:</p> <ul style="list-style-type: none"> The parameter is applicable only if Allowed coders are assigned to the IP Profile (see the 'Allowed Audio Coders' or 'Allowed Video Coders' parameters). For more information on the Allowed Coders feature, see Restricting Coders on page 434.
Allowed Video Coders allowed-video-coders-group-name [IpProfile_SBCAllowedVideoCodersGroupName]	<p>Assigns an Allowed Video Coders Group. This defines permitted video coders when forwarding video streams to the SIP entity associated with the IP Profile. The video coders are listed in the "video" media type in the SDP (i.e., 'm=video' line). For this SIP entity, the device uses only video coders that appear in both the SDP offer and the Allowed Video Coders Group.</p>

Parameter	Description
	<p>By default, no Allowed Video Coders Group is assigned (i.e., all video coders are allowed).</p> <p>To configure Allowed Video Coders Groups, see Configuring Allowed Video Coder Groups on page 387.</p>
<p>Allowed Media Types sbc-allowed-media-types [IpProfile_SBCAllowedMediaTypes]</p>	<p>Defines media types permitted for the SIP entity associated with the IP Profile. The media type appears in the SDP 'm=' line (e.g., 'm=audio'). The device permits only media types that appear in both the SDP offer and this configured list. If no common media types exist between the SDP offer and this list, the device drops the call.</p> <p>The valid value is a string of up to 64 characters. To configure multiple media types, separate the strings with a comma, e.g., " audio, text" (without quotes). By default, no media types are configured (i.e., all media types are permitted).</p>
<p>Direct Media Tag sbc-dm-tag [IPProfile_SBCDirectMediaTag]</p>	<p>Defines an identification tag for enabling direct media (no Media Anchoring) for the SIP entity associated with the IP Profile. Direct media occurs between all endpoints whose IP Profiles have the same tag value (non-empty value). For example, if you set the parameter to "direct-rtp" for two IP Profiles "IP-PBX-1" and "IP-PBX-2", the device employs direct media for calls amongst endpoints associated with IP Profile "IP-PBX-1", for calls amongst endpoints associated with IP Profile "IP-PBX-2", and for calls between endpoints associated with IP Profile "IP-PBX-1" and IP Profile "IP-PBX-2".</p> <p>The valid value is a string of up to 16 characters. By default, no value is defined.</p> <p>For more information on direct media, see Direct Media on page 432.</p> <p>Note: If you enable direct media for the IP Profile, make sure that your Media Realm provides sufficient ports, as media may traverse the device for mid-call services (e.g., call transfer).</p>
<p>RFC 2833 Mode sbc-rfc2833-behavior [IpProfile_SBCRFC2833Behavior]</p>	<p>Defines the handling of RFC 2833 SDP offer-answer negotiation for the SIP entity associated with the IP Profile.</p> <ul style="list-style-type: none"> ▪ [0] As is = (Default) The device does not intervene in the RFC 2833 negotiation. ▪ [1] Extend = Each outgoing offer-answer includes RFC 2833 in the offered SDP. The device adds RFC 2833 only if the incoming offer does not include RFC 2833. ▪ [2] Disallow = The device removes RFC 2833 from the incoming offer. <p>Note: If the device interworks between different DTMF methods and one of the methods is in-band DTMF packets (RFC 2833), detection and generation of DTMF methods requires DSP resources.</p>
<p>RFC 2833 DTMF Payload Type sbc-2833dtmf-payload [IpProfile_SBC2833DTMFPayloadType]</p>	<p>Defines the payload type of DTMF digits for the SIP entity associated with the IP Profile. This enables the interworking of the DTMF payload type for RFC 2833 between different SBC call legs. For example, if two entities</p>

Parameter	Description
	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. The value range is 0 to 200. The default is 0 (i.e., the device forwards the received payload type as is).
Alternative DTMF Method sbc-alternative-dtmf-method [IpProfile_SBCAlternativeDTMFMethod]	The device's first priority for DTMF method at each leg is RFC 2833. Thus, if the device successfully negotiates RFC 2833 for the SIP entity associated with the IP Profile, the chosen DTMF method for this leg is RFC 2833. When RFC 2833 negotiation fails, the device uses the parameter to define the DTMF method for the leg. <ul style="list-style-type: none"> ▪ [0] As Is = (Default) The device does not attempt to interwork any special DTMF method. ▪ [1] In Band ▪ [2] INFO - Cisco ▪ [3] INFO - Nortel ▪ [4] INFO - Lucent = INFO, Korea Note: If the device interworks between different DTMF methods and one of the methods is in-band DTMF packets (RFC 2833), detection and generation of DTMF methods requires DSP resources.
SDP Ptime Answer sbc-sdp-ptime-ans [IpProfile_SBCSDPPtimeAnswer]	Defines the packetization time (ptime) of the coder in RTP packets for the SIP entity associated with the IP Profile. This is useful when implementing transrating. <ul style="list-style-type: none"> ▪ [0] Remote Answer = (Default) Use ptime according to SDP answer. ▪ [1] Original Offer = Use ptime according to SDP offer. ▪ [2] Preferred Value= Use preferred ptime for negotiation, if configured by the 'Preferred Ptime' parameter.
Preferred Ptime sbc-preferred-ptime [IpProfile_SBCPreferredPTime]	Defines the packetization time (in msec) for the SIP entity associated with the IP Profile if the 'SBC SDP Ptime Answer' parameter (see above) is set to Preferred Value. The valid range is 0 to 200. The default is 0 (i.e., preferred ptime is not used).
Use Silence Suppression sbc-use-silence-supp [IpProfile_SBCUseSilenceSupp]	Defines silence suppression support for the SIP entity associated with the IP Profile <ul style="list-style-type: none"> ▪ [0] Transparent = (Default) Forward as is. ▪ [1] Add = Enable silence suppression for each relevant coder listed in the SDP. ▪ [2] Remove = Disable silence suppression for each relevant coder listed in the SDP.
RTP Redundancy Mode sbc-rtp-red-behav [IpProfile_SBCRTPRedundancyBehavior]	Enables interworking RTP redundancy negotiation support between SIP entities in the SDP offer-answer exchange (according to RFC 2198). The parameter defines the device's handling of RTP redundancy for the SIP entity associated with the IP Profile. According to the RTP redundancy SDP offer/answer negotiation, the device uses or discards the RTP redundancy packets. The parameter enables asymmetric RTP redundancy, whereby the device

Parameter	Description
	<p>can transmit and receive RTP redundancy packets to and from a specific SIP entity, while transmitting and receiving regular RTP packets (no redundancy) for the other SIP entity involved in the voice path.</p> <p>The device can identify the RTP redundancy payload type in the SDP for indicating that the RTP packet stream includes redundant packets. RTP redundancy is indicated in SDP using the "red" coder type, for example:</p> <pre>a=rtpmap:<payload type> red/8000/1</pre> <p>RTP redundancy is useful when there is packet loss; the missing information may be reconstructed at the receiver side from the redundant packets.</p> <ul style="list-style-type: none"> ▪ [0] As Is = (Default) The device does not interfere in the RTP redundancy negotiation and forwards the SDP offer/answer (incoming and outgoing calls) as is without interfering in the RTP redundancy negotiation. ▪ [1] Enable = The device always adds RTP redundancy capabilities in the outgoing SDP offer sent to the SIP entity. Whether RTP redundancy is implemented depends on the subsequent incoming SDP answer from the SIP entity. The device does not modify the incoming SDP offer received from the SIP entity, but if RTP redundancy is required, it will be supported. Select the option if the SIP entity requires RTP redundancy. ▪ [2] Disable = The device removes the RTP redundancy payload (if present) from the SDP offer/answer for calls received from or sent to the SIP entity. Select the option if the SIP entity does not support RTP redundancy. <p>Note:</p> <ul style="list-style-type: none"> ▪ To enable the device to generate RFC 2198 redundant packets, use the IPProfile_RTPRedundancyDepth parameter. ▪ To configure the payload type in the SDP offer for RTP redundancy, use the RFC2198PayloadType.
<p>RTCP Mode sbc-rtcp-mode [IPProfile_SBCRTCPMode]</p>	<p>Defines how the device handles RTCP packets during call sessions for the SIP entity associated with the IP Profile. This is useful for interworking RTCP between SIP entities. For example, this may be necessary when incoming RTCP is not compatible with the destination SIP entity's (this IP Profile) RTCP support. In such a scenario, the device can generate the RTCP and send it to the SIP entity.</p> <ul style="list-style-type: none"> ▪ [0] Transparent = (Default) RTCP is forwarded as is (unless transcoding is done, in which case, the device generates RTCP on both legs). ▪ [1] Generate Always = Generates RTCP packets during active and inactive (e.g., during call hold) RTP periods (i.e., media is 'a=recvonly' or 'a=inactive' in the INVITE SDP). ▪ [2] Generate only if RTP Active = Generates RTCP packets only during active RTP periods. In other words, the device does not generate RTCP when there is no RTP traffic (such as when a call is on hold).

Parameter	Description
Jitter Compensation sbc-jitter-compensation [IpProfile_SBCJitterCompensation]	<p>Note: The corresponding global parameter is SBCRTCPMode.</p> <p>Enables the on-demand jitter buffer for SBC calls. The jitter buffer can be used when other functionality such as voice transcoding are not done on the call. The jitter buffer is useful when incoming packets are received at inconsistent intervals (i.e., packet delay variation). The jitter buffer stores the packets and sends them out at a constant rate (according to the coder's settings).</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable <p>Note:</p> <ul style="list-style-type: none"> ▪ The jitter buffer parameters, 'Dynamic Jitter Buffer Minimum Delay' (DJBufMinDelay) and 'Dynamic Jitter Buffer Optimization Factor' (DJBufOptFactor) can be used to configure minimum packet delay only when transcoding is employed. ▪ This functionality may require DSP resources. For more information, contact your AudioCodes sales representative.
ICE Mode ice-mode [IPProfile_SBCIceMode]	<p>Enables Interactive Connectivity Establishment (ICE) Lite for the SIP entity associated with the IP Profile. ICE is a methodology for NAT traversal, employing the Session Traversal Utilities for NAT (STUN) and Traversal Using Relays around NAT (TURN) protocols to provide a peer with a public IP address and port that can be used to connect to a remote peer.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Lite <p>For more information on ICE Lite, see ICE Lite.</p> <p>Note: As ICE has been defined by the WebRTC standard as mandatory, the support is important for deployments implementing WebRTC. For more information on WebRTC, see WebRTC on page 524.</p>
SDP Handle RTCP sbc-sdp-handle-rtcp [IpProfile_SBCSDPHandleRTCPAttribute]	<p>Enables the interworking of the RTCP attribute, 'a=rtcp' (RTCP) in the SDP, for the SIP entity associated with the IP Profile. The RTCP attribute is used to indicate the RTCP port for media when that port is not the next higher port number following the RTP port specified in the media line ('m=').</p> <p>The parameter is useful for SIP entities that either require the attribute or do not support the attribute. For example, Google Chrome and Web RTC do not accept calls without the RTCP attribute in the SDP. In Web RTC, Chrome (SDS) generates the SDP with 'a=rtcp', for example:</p> <pre style="background-color: #f0f0f0; padding: 5px;"> m=audio 49170 RTP/AVP 0 a=rtcp:53020 IN IP6 2001:2345:6789:ABCD:EF01:2345:6789:ABCD </pre> <ul style="list-style-type: none"> ▪ [0] Don't Care = (Default) The device forwards the SDP as is without interfering in the RTCP attribute (regardless if present or not). ▪ [1] Add = The device adds the 'a=rtcp' attribute to the

Parameter	Description
	<p>outgoing SDP offer sent to the SIP entity if the attribute was not present in the original incoming SDP offer.</p> <ul style="list-style-type: none"> ▪ [2] Remove = The device removes the 'a=rtcp' attribute, if present in the incoming SDP offer received from the other SIP entity, before sending the outgoing SDP offer to the SIP entity. <p>Note: As the RTCP attribute has been defined by the WebRTC standard as mandatory, the support is important for deployments implementing WebRTC. For more information on WebRTC, see WebRTC on page 524.</p>
RTCP Mux sbc-rtcp-mux [IPProfile_SBCRTCPMux]	<p>Enables interworking of multiplexing of RTP and RTCP onto a single local port, between SIP entities. The parameter enables multiplexing of RTP and RTCP traffic onto a single local port, for the SIP entity associated with the IP Profile.</p> <p>Multiplexing of RTP data packets and RTCP packets onto a single local UDP port is done for each RTP session (according to RFC 5761). If multiplexing is not enabled, the device uses different (but adjacent) ports for RTP and RTCP packets.</p> <p>With the increased use of NAT and firewalls, maintaining multiple NAT bindings can be costly and also complicate firewall administration since multiple ports must be opened to allow RTP traffic. To reduce these costs and session setup times, support for multiplexing RTP data packets and RTCP packets onto a single port is advantageous.</p> <p>For multiplexing, the initial SDP offer must include the "a=rtcp-mux" attribute to request multiplexing of RTP and RTCP onto a single port. If the SDP answer wishes to multiplex RTP and RTCP, it must also include the "a=rtcp-mux" attribute. If the answer does not include the attribute, the offerer must not multiplex RTP and RTCP packets. If both ICE and multiplexed RTP-RTCP are used, the initial SDP offer must also include the "a=candidate:" attribute for both RTP and RTCP along with the "a=rtcp:" attribute, indicating a fallback port for RTCP in case the answerer does not support RTP and RTCP multiplexing.</p> <ul style="list-style-type: none"> ▪ [0] Not Supported = (Default) RTP and RTCP packets use different ports. ▪ [1] Supported = Device multiplexes RTP and RTCP packets onto a single port. <p>Note: As RTP multiplexing has been defined by the WebRTC standard as mandatory, the support is important for deployments implementing WebRTC. For more information on WebRTC, see WebRTC on page 524.</p>
RTCP Feedback sbc-rtcp-feedback [IPProfile_SBCRTCPFeedback]	<p>Enables RTCP-based feedback indication in outgoing SDPs sent to the SIP entity associated with the IP Profile.</p> <p>The parameter supports indication of RTCP-based feedback, according to RFC 5124, during RTP profile negotiation between two communicating SIP entities. RFC 5124 defines an RTP profile (S)AVPF for (secure) real-time communications to provide timely feedback from the</p>

Parameter	Description
	<p>receivers to a sender. For more information on RFC 5124, see http://tools.ietf.org/html/rfc5124.</p> <p>Some SIP entities may require RTP secure-profile feedback negotiation (AVPF/SAVPF) in the SDP offer/answer exchange, while other SIP entities may not support it. The device indicates whether or not feedback is supported on behalf of the SIP entity. It does this by adding an "F" or removing the "F" from the SDP media line ('m=') for AVP and SAVP. For example, the following shows "AVP" appended with an "F", indicating that the SIP entity is capable of receiving feedback</p> <pre>m=audio 49170 RTP/SAVPF 0 96</pre> <ul style="list-style-type: none"> ▪ [0] Feedback Off = (Default) The device does not send the feedback flag ("F") in SDP offers/answers that are sent to the SIP entity. If the SDP 'm=' attribute of an incoming message that is destined to the SIP entity includes the feedback flag, the device removes it before sending the message to the SIP entity. ▪ [1] Feedback On = The device includes the feedback flag ("F") in the SDP offer sent to the SIP entity. The device includes the feedback flag in the SDP answer sent to the SIP entity only if it was present in the SDP offer received from the other SIP entity. ▪ [2] As Is = The device does not involve itself in the feedback, but simply forwards any feedback indication as is. <p>Note:</p> <ul style="list-style-type: none"> ▪ As RTCP-based feedback has been defined by the WebRTC standard as mandatory, the support is important for deployments implementing WebRTC. For more information on WebRTC, see WebRTC on page 524. ▪ RTCP-based feedback is required for the VoIPerfect feature (see VoIPerfect on page 538).
Voice Quality Enhancement sbc-voice-quality-enhancement [lpProfile_SBCVoiceQualityEnhancement]	<p>Enables the device to detect speech and network quality (packet loss and bandwidth reduction) and triggers the device to overcome adverse conditions to ensure high call quality.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable <p>Note: The parameter is applicable only to the VoIPerfect feature (see VoIPerfect on page 538).</p>
Max Opus Bandwidth sbc-max-opus-bandwidth [lpProfile_SBCMaxOpusBW]	<p>Defines the VoIPerfect mode of operation, which is based on the Opus coder.</p> <ul style="list-style-type: none"> ▪ 0 = (Default) Managed Opus ▪ 80000 = Smart Transcoding <p>Note: The parameter is applicable only to the VoIPerfect feature (see VoIPerfect on page 538).</p>
Quality of Service	
RTP IP DiffServ	Defines the DiffServ value for Premium Media class of service (CoS) content.

Parameter	Description
rtp-ip-diffserv [IpProfile_IPDiffServ]	The valid range is 0 to 63. The default is 46. Note: The corresponding global parameter is PremiumServiceClassMediaDiffServ.
Signaling DiffServ signaling-diffserv [IpProfile_SigIPDiffServ]	Defines the DiffServ value for Premium Control CoS content (Call Control applications). The valid range is 0 to 63. The default is 40. Note: The corresponding global parameter is PremiumServiceClassControlDiffServ.
Jitter Buffer	
Dynamic Jitter Buffer Minimum Delay jitter-buffer-minimum-delay [IpProfile_JitterBufMinDelay]	Defines the minimum delay (in msec) of the device's dynamic Jitter Buffer. The valid range is 0 to 150. The default delay is 10. For more information on Jitter Buffer, see Configuring the Dynamic Jitter Buffer on page 186. Note: The corresponding global parameter is DJBufMinDelay.
Dynamic Jitter Buffer Optimization Factor jitter-buffer-optimization-factor [IpProfile_JitterBufOptFactor]	Defines the Dynamic Jitter Buffer frame error/delay optimization factor. The valid range is 0 to 12. The default factor is 10. For more information on Jitter Buffer, see Configuring the Dynamic Jitter Buffer on page 186. Note: <ul style="list-style-type: none"> ▪ For data (fax and modem) calls, set the parameter to 12. ▪ The corresponding global parameter is DJBufOptFactor.
Silence Suppression [IpProfile_SCE]	Enables the Silence Suppression feature. When enabled, the device, upon detection of silence period during a call does not send packets, thereby conserving bandwidth during the VoIP call. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable = Silence Suppression is enabled. ▪ [2] Enable Without Adaptation = A single silence packet is sent during a silence period (applicable only to G.729). Note: <ul style="list-style-type: none"> ▪ If the coder is G.729, the value of the 'annexb' parameter of the 'a=fmtp' attribute in the SDP is determined by the following: <ul style="list-style-type: none"> ✓ The parameter is set to Disable [0]: 'annexb=no' ✓ The parameter is set to Enable [1]: 'annexb=yes' ✓ The parameter is set to Enable Without Adaptation [2] and IsCiscoSCEMode to [0]: 'annexb=yes' ✓ Enable Without Adaptation is set to Enable Without Adaptation [2] and IsCiscoSCEMode to [1]: 'annexb=no' ▪ The corresponding global parameter is EnableSilenceCompression.

Parameter	Description
Jitter Buffer Max Delay [IpProfile_JitterBufMaxDelay]	Defines the maximum delay and length (in msec) of the Jitter Buffer. The valid range is 150 to 2,000. The default is 250.
Voice	
Echo Canceler echo-canceller [IpProfile_EnableEchoCanceller]	Enables the device's Echo Cancellation feature (i.e., echo from voice calls is removed). <ul style="list-style-type: none"> ▪ [0] Disable ▪ [1] Line (default) ▪ [2] Acoustic For a detailed description of the Echo Cancellation feature, see Configuring Echo Cancellation on page 173. Note: The corresponding global parameter is EnableEchoCanceller.
Input Gain [IpProfile_InputGain]	Defines the pulse-code modulation (PCM) input gain control (in decibels). The valid range is -32 to 31 dB. The default is 0 dB. Note: The corresponding global parameter is InputGain.
Voice Volume [IpProfile_VoiceVolume]	Defines the voice gain control (in decibels). The valid range is -32 to 31 dB. The default is 0 dB. Note: The corresponding global parameter is VoiceVolume.
SBC Signaling	
PRACK Mode sbc-prack-mode [IpProfile_SbcPrackMode]	Defines the device's handling of SIP PRACK messages for the SIP entity associated with the IP Profile. <ul style="list-style-type: none"> ▪ [1] Optional = PRACK is optional. If required, the device performs the PRACK process on behalf of the SIP entity. ▪ [2] Mandatory = PRACK is required for this SIP entity. Calls from endpoints that do not support PRACK are rejected. Calls destined to these endpoints are also required to support PRACK. ▪ [3] Transparent (default) = The device does not intervene with the PRACK process and forwards the request as is.
P-Asserted-Identity Header Mode sbc-assert-identity [IpProfile_SBCAssertIdentity]	Defines the device's handling of the SIP P-Asserted-Identity header for the SIP entity associated with the IP Profile. This header indicates how the outgoing SIP message asserts identity. <ul style="list-style-type: none"> ▪ [0] As Is = (Default) P-Asserted Identity header is not affected and the device uses the same P-Asserted-Identity header (if present) in the incoming message for the outgoing message. ▪ [1] Add = Adds a P-Asserted-Identity header. The header's values are taken from the source URL. ▪ [2] Remove = Removes the P-Asserted-Identity header. Note: <ul style="list-style-type: none"> ▪ The parameter affects only the initial INVITE request.

Parameter	Description
	<ul style="list-style-type: none"> ▪ The corresponding global parameter is SBCAssertIdentity.
Diversion Header Mode sbc-diversion-mode [IpProfile_SBCDiversionMode]	Defines the device's handling of the SIP Diversion header for the SIP entity associated with the IP Profile. <ul style="list-style-type: none"> ▪ [0] As Is = (Default) Diversion header is not handled. ▪ [1] Add = History-Info header is converted to a Diversion header. ▪ [2] Remove = Removes the Diversion header and the conversion to the History-Info header depends on the SBCHistoryInfoMode parameter. For more information on interworking of the History-Info and Diversion headers, see Interworking SIP Diversion and History-Info Headers on page 446. <p>Note: If the Diversion header is used, you can specify the URI type (e.g., "tel:") to use in the header, using the SBCDiversionUriType parameter.</p>
History-Info Header Mode sbc-history-info-mode [IpProfile_SBCHistoryInfoMode]	Defines the device's handling of the SIP History-Info header for the SIP entity associated with the IP Profile. <ul style="list-style-type: none"> ▪ [0] As Is = (Default) History-Info header is not handled. ▪ [1] Add = Diversion header is converted to a History-Info header. ▪ [2] Remove = History-Info header is removed from the SIP dialog and the conversion to the Diversion header depends on the SBCDiversionMode parameter. For more information on interworking of the History-Info and Diversion headers, see Interworking SIP Diversion and History-Info Headers on page 446.
Session Expires Mode sbc-session-expires-mode [IpProfile_SBCSessionExpiresMode]	Defines the required session expires mode for the SIP entity associated with the IP Profile. <ul style="list-style-type: none"> ▪ [0] Transparent = (Default) The device does not interfere with the session expires negotiation. ▪ [1] 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. ▪ [2] Not Supported = The device does not allow a session timer with this SIP entity. ▪ [3] Supported = The device enables the session timer with this SIP 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.
Remote Update Support sbc-rmt-update-supp [IpProfile_SBCRemoteUpdateSupport]	Defines whether the SIP UPDATE message is supported by the SIP entity associated with the IP Profile. <ul style="list-style-type: none"> ▪ [0] Not Supported = UPDATE message is not supported. ▪ [1] Supported Only After Connect = UPDATE message

Parameter	Description
	is supported only after the call is connected. <ul style="list-style-type: none"> ▪ [2] Supported = (Default) UPDATE message is supported during call setup and after call establishment.
Remote re-INVITE sbc-rmt-re-invite-supp [IpProfile_SBCRemoteReinviteSupport]	Defines 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. <ul style="list-style-type: none"> ▪ [0] 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. ▪ [1] Supported only 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. ▪ [2] Supported = (Default) re-INVITE is supported with or without SDP.
Remote Delayed Offer Support sbc-rmt-delayed-offer [IpProfile_SBCRemoteDelayedOfferSupport]	Defines whether the remote endpoint supports delayed offer (i.e., initial INVITEs without an SDP offer). <ul style="list-style-type: none"> ▪ [0] Not Supported = Initial INVITE requests without SDP are not supported. ▪ [1] Supported = (Default) Initial INVITE requests without SDP are supported. <p>Note: For the parameter to function, you need to assign extension coders to the IP Profile of the SIP entity that does not support delayed offer (using the IpProfile_SBCExtensionCodersGroupName parameter).</p>
Remote Representation Mode sbc-rmt-rprsntation [IpProfile_SBCRemoteRepresentationMode]	Enables interworking SIP in-dialog, Contact and Record-Route headers between SIP entities. The parameter defines the device's handling of in-dialog, Contact and Record-Route headers for messages sent to the SIP entity associated with the IP Profile. <ul style="list-style-type: none"> ▪ [-1] According to Operation Mode = (Default) Depends on the setting of the 'Operation Mode' parameter in the IP Group or SRDs table: <ul style="list-style-type: none"> ✓ B2BUA: Device operates as if the parameter is set to Replace Contact [0]. ✓ Call State-full Proxy: Device operates as if the parameter is set to Add Routing Headers [1]. ▪ [0] Replace Contact = Device replaces the address in the Contact header, received in incoming messages from the other side, with its own address in the outgoing message sent to the SIP entity. ▪ [1] Add Routing Headers = Device adds a Record-Route header for itself to outgoing messages (requests/responses) sent to the SIP entity in dialog-setup transactions. The Contact header remains unchanged. ▪ [2] Transparent = Device doesn't change the Contact header and doesn't add a Record-Route header for itself. Instead, it relies on its' own inherent mechanism

Parameter	Description
	to remain in the route of future requests in the dialog (for example, relying on the way the endpoints are set up or on TLS as the transport type).
Keep Incoming Via Headers sbc-keep-via-headers [IpProfile_SBCKeepVIAHeaders]	Enables interworking SIP Via headers between SIP entities. The parameter defines the device's handling of Via headers for messages sent to the SIP entity associated with the IP Profile. <ul style="list-style-type: none"> ▪ [-1] According to Operation Mode = Depends on the setting of the 'Operation Mode' parameter in the IP Groups table or SRDs table: <ul style="list-style-type: none"> ✓ B2BUA: Device operates as if the parameter is set to Disable [0]. ✓ Call State-full Proxy: Device operates as if the parameter is set to Enable [1]. ▪ [0] Disable = Device removes all Via headers received in the incoming SIP request from the other leg and adds a Via header identifying only itself, in the outgoing message sent to the SIP entity. ▪ [1] Enable = Device retains the Via headers received in the incoming SIP request and adds itself as the top-most listed Via header in the outgoing message sent to the SIP entity.
Keep Incoming Routing Headers sbc-keep-routing-headers [IpProfile_SBCKeepRoutingHeaders]	Enables interworking SIP Record-Route headers between SIP entities. The parameter defines the device's handling of Record-Route headers for request/response messages sent to the the SIP entity associated with the IP Profile. <ul style="list-style-type: none"> ▪ [-1] According to Operation Mode = (Default) Depends on the setting of the 'Operation Mode' in the IP Group or SRDs table: <ul style="list-style-type: none"> ✓ B2BUA: Device operates as if the parameter is set to Disable [0]. ✓ Call State-full Proxy: Device operates as if the parameter is set to Enable [1]. ▪ [0] Disable = Device removes the Record-Route headers received in requests and responses from the other side, in the outgoing SIP message sent to the SIP entity. The device creates a route set for that side of the dialog based on these headers, but doesn't send them to the SIP entity. ▪ [1] Enable = Device retains the incoming Record-Route headers received in requests and non-failure responses from the other side, in the following scenarios: <ul style="list-style-type: none"> ✓ The message is part of a SIP dialog-setup transaction. ✓ The messages in the setup and previous transaction didn't include the Record-Route header, and therefore hadn't set the route set. <p>Note: Record-Routes are kept only for SIP INVITE, UPDATE, SUBSCRIBE and REFER messages.</p>
Keep User-Agent Header sbc-keep-user-agent	Enables interworking SIP User-Agent headers between SIP entities. The parameter defines the device's handling of User-Agent headers for response/request messages sent

Parameter	Description
[IpProfile_SBCKeepUserAgentHeader]	to the SIP entity associated with the IP Profile. <ul style="list-style-type: none"> ▪ [-1] According to Operation Mode = (Default) Depends on the setting of the 'Operation Mode' parameter in the IP Group or SRDs table: <ul style="list-style-type: none"> ✓ B2BUA: Device operates as if this parameter is set to Disable [0]. ✓ Call State-full Proxy: Device operates as if this parameter is set to Enable [1]. ▪ [0] Disable = Device removes the User-Agent/Server headers received in the incoming message from the other side, and adds its' own User-Agent header in the outgoing message sent to the SIP entity. ▪ [1] Enable = Device retains the User-Agent/Server headers received in the incoming message and sends the headers as is in the outgoing message to the SIP entity.
Handle X-Detect sbc-handle-xdetect [IpProfile_SBCHandleXDetect]	Enables the detection and notification of events (AMD, CPT, and fax), using the X-Detect SIP header. <ul style="list-style-type: none"> ▪ [0] No (default) ▪ [1] Yes For more information, see Event Detection and Notification using X-Detect Header on page 188.
ISUP Body Handling sbc-isup-body-handling [IpProfile_SBCISUPBodyHandling]	Defines the handling of ISUP data for interworking between SIP and SIP-I endpoints. <ul style="list-style-type: none"> ▪ [0] Transparent = (Default) ISUP data is passed transparently (as is) between endpoints (SIP-I to SIP-I calls). ▪ [1] Remove = ISUP body is removed from INVITE messages. ▪ [2] Create = ISUP body is added to outgoing INVITE messages. For more information on interworking SIP and SIP-I, see Interworking SIP and SIP-I Endpoints on page 522.
ISUP Variant sbc-isup-variant [IpProfile_SBCISUPVariant]	Defines the ISUP variant for interworking SIP and SIP-I endpoints. <ul style="list-style-type: none"> ▪ [0] itu92 = (Default) ITU 92 variant ▪ [1] Spirou = SPIROU (ISUP France)
Max Call Duration sbc-max-call-duration [IpProfile_SBCMaxCallDuration]	Defines the maximum duration (in minutes) per SBC call that is associated with the IP Profile. If the duration is reached, the device terminates the call. The valid range is 0 to 35,791, where 0 is unlimited duration. The default is the value configured for the global parameter, SBCMaxCallDuration.
SBC Registration	
User Registration Time sbc-usr-reg-time [IpProfile_SBCUserRegistrationTime]	Defines the registration time (in seconds) that the device responds to SIP REGISTER requests from users belonging to the SIP entity associated with the IP Profile. The registration time is inserted in the Expires header in the outgoing response sent to the user. The Expires header determines the lifespan of the

Parameter	Description
	<p>registration. For example, a value of 3600 means that the registration will timeout in one hour and at that point, the user will not be able to make or receive calls.</p> <p>The valid range is 0 to 2,000,000. The default is 0. If configured to 0, the Expires header's value received in the user's REGISTER request remains unchanged. If no Expires header is received in the REGISTER message and the parameter is set to 0, the Expires header's value is set to 180 seconds, by default.</p> <p>Note: The corresponding global parameter is SBCUserRegistrationTime.</p>
<p>NAT UDP Registration Time sbc-usr-udp-nat-reg-time [IpProfile_SBCUserBehindUdpNATRegistrationTime]</p>	<p>Defines the registration time (in seconds) that the device includes in register responses, in response to SIP REGISTER requests from users belonging to the SIP entity associated with the IP Profile.</p> <p>The parameter applies only to users that are located behind NAT and whose communication type is UDP. The registration time is inserted in the Expires header in the outgoing response sent to the user.</p> <p>The Expires header determines the lifespan of the registration. For example, a value of 3600 means that the registration will timeout in one hour, unless the user sends a refresh REGISTER before the timeout. Upon timeout, the device removes the user's details from the registration database, and the user will not be able to make or receive calls through the device.</p> <p>The valid value is 0 to 2,000,000. If configured to 0, the Expires header's value received in the user's REGISTER request remains unchanged. By default, no value is defined (-1).</p> <p>Note: If the parameter is not configured, the registration time is according to the global parameter SBCUserRegistrationTime or IP Profile parameter IpProfile_SBCUserRegistrationTime.</p>
<p>NAT TCP Registration Time sbc-usr-tcp-nat-reg-time [IpProfile_SBCUserBehindTcpNATRegistrationTime]</p>	<p>Defines the registration time (in seconds) that the device includes in register responses, in response to SIP REGISTER requests from users belonging to the SIP entity associated with the IP Profile.</p> <p>The parameter applies only to users that are located behind NAT and whose communication type is TCP. The registration time is inserted in the Expires header in the outgoing response sent to the user.</p> <p>The Expires header determines the lifespan of the registration. For example, a value of 3600 means that the registration will timeout in one hour, unless the user sends a refresh REGISTER before the timeout. Upon timeout, the device removes the user's details from the registration database, and the user will not be able to make or receive calls through the device.</p> <p>The valid value is 0 to 2,000,000. If configured to 0, the Expires header's value received in the user's REGISTER request remains unchanged. By default, no value is defined</p>

Parameter	Description
	(-1). Note: If the parameter is not configured, the registration time is according to the global parameter SBCUserRegistrationTime or IP Profile parameter IpProfile_SBCUserRegistrationTime.
SBC Forward and Transfer	
Remote REFER Mode sbc-rmt-refer-behavior [IpProfile_SBCRemoteReferBehavior]	Defines the device's handling of REFER requests for the SIP entity associated with the IP Profile. <ul style="list-style-type: none"> ▪ [0] Regular = (Default) Refer-To header is unchanged and the device forwards the REFER as is. ▪ [1] Database URL = Changes the Refer-To header so that the re-routed INVITE is sent through the SBC: <ol style="list-style-type: none"> a. Before forwarding the REFER request, the device changes the host part to the device's IP address and adds a special prefix ("T-&R_") to the Contact user part. b. The incoming INVITE is identified as a REFER-resultant INVITE according to this special prefix. c. 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. d. The special prefix is removed before the resultant INVITE is sent to the destination. ▪ [2] IP Group Name = Sets the host part in the REFER message to the name defined for the IP Group (in the IP Groups table). ▪ [3] Handle Locally = 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' parameter must be set to REFER). Note: The corresponding global parameter is SBCReferBehavior.
Remote Replaces Mode sbc-rmt-replaces-behavior [IpProfile_SBCRemoteReplacesBehavior]	Enables the device to handle incoming INVITES containing the Replaces header for the SIP entity (which does not support the header) associated with the IP Profile. The Replaces header is used to replace an existing SIP dialog with a new dialog such as in call transfer or call pickup. <ul style="list-style-type: none"> ▪ [0] Standard = (Default) The SIP entity supports INVITE messages containing Replaces headers. The device forwards the INVITE message containing the Replaces header to the SIP entity. The device may change the value of the Replaces header to reflect the call identifiers of the leg. ▪ [1] Handle Locally = The SIP entity does not support INVITE messages containing Replaces headers. The device terminates the received INVITE containing the Replaces header and establishes a new call between the SIP entity and the new call party. It then disconnects the call with the initial call party, by sending it a SIP BYE

Parameter	Description
	<p>request.</p> <ul style="list-style-type: none"> ▪ [2] Keep as is = The SIP entity supports INVITE messages containing Replaces headers. The device forwards the Replaces header as is in incoming REFER and outgoing INVITE messages from/to the SIP entity (i.e., Replaces header's value is unchanged). <p>For example, assume that the device establishes a call between A and B. If B initiates a call transfer to C, the device receives an INVITE with the Replaces header from C. If A supports the Replaces header, the device simply forwards the INVITE as is to A; a new call is established between A and C and the call between A and B is disconnected. However, if A does not support the Replaces header, the device uses this feature to terminate the INVITE with Replaces header and handles the transfer for A. The device does this by connecting A to C, and disconnecting the call between A and B, by sending a SIP BYE request to B. Note that if media transcoding is required, the device sends an INVITE to C on behalf of A with a new SDP offer.</p>
<p>Play RBT To Transferee sbc-play-rbt-to-xferee [IpProfile_SBCPlayRBTTToTransferee]</p>	<p>Enables the device to play a ringback tone to the transferred party (transferee) during a blind call transfer, for the SIP entity associated with the IP Profile (which does not support such a tone generation during call transfer). The ringback tone indicates to the transferee of the ringing of the transfer target (to where the transferee is being transferred).</p> <ul style="list-style-type: none"> ▪ [0] No (Default) ▪ [1] Yes <p>Typically, the transferee hears a ringback tone only if the transfer target sends it early media. However, if the transferee is put on-hold before being transferred, no ringback tone is heard.</p> <p>When this feature is enabled, the device generates a ringback tone to the transferee during call transfer in the following scenarios:</p> <ul style="list-style-type: none"> ▪ Transfer target sends a SIP 180 (Ringing) to the device. ▪ For non-blind transfer, if the call is transferred while the transfer target is ringing and no early media occurs. ▪ The 'Remote Early Media RTP Behavior parameter is set to Delayed (used in the Skype for Business environment), and transfer target sends a 183 Session Progress with SDP offer. If early media from the transfer target has already been detected, the transferee receives RTP stream from the transfer target. If it has not been detected, the device generates a ringback tone to the transferee and stops the tone generation once RTP has been detected from the transfer target. <p>For any of these scenarios, if the transferee is put on-hold by the transferor, the device retrieves the transferee from hold, sends a re-INVITE if necessary, and then plays the ringback tone.</p>

Parameter	Description
	<p>Note: For the device to play the ringback tone, it must be loaded with a Prerecorded Tones (PRT) file. For more information, see Prerecorded Tones File on page 590.</p>
Remote 3xx Mode sbc-rmt-3xx-behavior [IpProfile_SBCRemote3xxBehavior]	<p>Defines the device's handling of SIP 3xx redirect responses for the SIP entity associated with the IP Profile. By default, the device's handling of SIP 3xx responses is to send the Contact header unchanged. However, some SIP entities may support different versions of the SIP 3xx standard while others may not even support SIP 3xx.</p> <p>When enabled, the device handles SIP redirections between different subnets (e.g., between LAN and WAN sides). This is required when 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"> ▪ [0] Transparent = (Default) The device forwards the received SIP 3xx response as is, without changing the Contact header (i.e.,transparent handling). ▪ [1] Database URL = The device changes the Contact header so that the re-route request is sent through 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~&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. ▪ [2] Handle Locally = 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 3xx). <p>Note:</p> <ul style="list-style-type: none"> ▪ When the 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. ▪ 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"> ✓ sip:10.10.10.10:5060;transport=tcp;param=a ✓ sip:10.10.10.10:5060;transport=tcp;param=b ▪ The database entry expires two hours after the last use. ▪ The maximum number of destinations (i.e., database entries) is 50. ▪ The corresponding global parameter is SBC3xxBehavior.

Parameter	Description
SBC Hold	
Remote Hold Format remote-hold-Format [IPProfile_SBCRemoteHoldFormat]	<p>Defines the format of the SDP in the re-INVITE for call hold that the device sends to the held party.</p> <ul style="list-style-type: none"> ▪ [0] Transparent = (Default) Device forwards SDP as is. ▪ [1] Send Only = Device sends SDP with 'a=sendonly'. ▪ [2] Send Only Zero ip = Device sends SDP with 'a=sendonly' and 'c=0.0.0.0'. ▪ [3] Inactive = Device sends SDP with 'a=inactive'. ▪ [4] Inactive Zero ip = Device sends SDP with 'a=inactive' and 'c=0.0.0.0'. ▪ [5] 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.
Reliable Held Tone Source reliable-heldtone-source [IPProfile_ReliableHoldToneSource]	<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"> ▪ [0] 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. ▪ [1] 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). <p>Note: The device plays a held tone only if the 'SBC Play Held Tone' parameter is set to Yes.</p>
Play Held Tone play-held-tone [IpProfile_SBCPlayHeldTone]	<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"> ▪ [0] No (default) ▪ [1] Yes <p>Note: If the 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>
SBC Fax	
Fax Coders Group sbc-fax-coders-group-name [IpProfile_SBCFaxCodersGroupName]	<p>Assigns a Coder Group which defines the supported fax coders for fax negotiation for the SIP entity associated with the IP Profile. To configure Coder Groups, see Configuring Coder Groups on page 379.</p> <p>Note: The parameter is applicable only if you set the IpProfile_SBCFaxBehavior parameter to a value other than [0].</p>
Fax Mode	<p>Enables the device to handle fax offer-answer negotiations for the SIP entity associated with the IP Profile.</p>

Parameter	Description
sbc-fax-behavior [IpProfile_SBCFaxBehavior]	<ul style="list-style-type: none"> ▪ [0] As Is = (Default) Device forwards fax transparently, without interference. ▪ [1] Handle always = Handle fax according to fax settings in the IP Profile for all offer-answer transactions (including the initial INVITE). ▪ [2] Handle on re-INVITE = Handle fax according to fax settings in the IP Profile for all re-INVITE offer-answer transactions (except for initial INVITE). <p>Note: The fax settings in the IP Profile include IpProfile_SBCFaxCodersGroupName, IpProfile_SBCFaxOfferMode, and IpProfile_SBCFaxAnswerMode.</p>
Fax Offer Mode sbc-fax-offer-mode [IpProfile_SBCFaxOfferMode]	Defines the coders included in the outgoing SDP offer (sent to the called "fax") for the SIP entity associated with the IP Profile. <ul style="list-style-type: none"> ▪ [0] All coders = (Default) Use only (and all) the coders of the selected Coder Group configured using the SBCFaxCodersGroupID parameter. ▪ [1] Single coder = Use only one coder. If a coder in the incoming offer (from the calling "fax") matches a coder in the SBCFaxCodersGroupID, the device uses this coder. If no match exists, the device uses the first coder listed in the Coders Group ID (SBCFaxCodersGroupID). <p>Note: The parameter is applicable only if you set the IpProfile_SBCFaxBehavior parameter to a value other than [0].</p>
Fax Answer Mode sbc-fax-answer-mode [IpProfile_SBCFaxAnswerMode]	Defines the coders included in the outgoing SDP answer (sent to the calling "fax") for the SIP entity associated with the IP Profile. <ul style="list-style-type: none"> ▪ [0] All coders = Use matched coders between the incoming offer coders (from the calling "fax") and the coders of the selected Coder Group (configured using the SBCFaxCodersGroupID parameter). ▪ [1] Single coder = (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 Coder Group (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 Coder Group. <p>Note: The parameter is applicable only if you set the IpProfile_SBCFaxBehavior parameter to a value other than [0].</p>
Remote Renegotiate on Fax Detection sbc-rmt-renegotiate-on-fax-detect [IPProfile_SBCRemoteRenegotiateOnFaxDetection]	Enables local handling of fax detection and negotiation by the device on behalf of the SIP entity associated with the IP Profile. This applies to faxes sent immediately upon the establishment of a voice channel (i.e., after 200 OK). The device attempts to detect the fax (CNG tone) from the originating SIP entity within a user-defined interval (see the SBCFaxDetectionTimeout parameter) immediately after the

Parameter	Description
	<p>voice call is established.</p> <p>Once fax is detected, the device can handle the subsequent fax negotiation by sending re-INVITE messages to both SIP entities. The device also negotiates the fax coders between the two SIP entities. The negotiated coders are according to the list of fax coders assigned to each SIP entity, using the IP Profile parameter 'Fax Coders Group'.</p> <ul style="list-style-type: none"> ▪ [0] Transparent = (Default) Device does not interfere in the fax transaction and assumes that the SIP entity fully supports fax renegotiation upon fax detection. ▪ [1] Only on Answer Side = The SIP entity supports fax renegotiation upon fax detection only if it is the terminating (answering) fax, and does not support renegotiation if it is the originating fax. ▪ [2] No = The SIP entity does not support fax renegotiation upon fax detection when it is the originating or terminating fax. <p>Note:</p> <ul style="list-style-type: none"> ▪ This feature is applicable only when both SIP entities do not fully support fax detection (receive or send) and negotiation: one SIP entity must be assigned an IP Profile where the parameter is set to [1] or [2], while the peer SIP entity must be assigned an IP Profile where the parameter is set to [2]. ▪ This feature is supported only if at least one of the SIP entities use the G.711 coder. ▪ This feature utilizes DSP resources. If there are insufficient resources, the fax transaction fails.
Media	
<p>Broken Connection Mode disconnect-on-broken-connection [IpProfile_DisconnectOnBrokenConnection]</p>	<p>Defines the device's handling of calls when RTP packets (media) are not received within a user-defined timeout interval (configured by the BrokenConnectionEventTimeout parameter). The interval can be during call setup (configured by the NoRTPDetectionTimeout parameter) or mid-call when RTP flow suddenly stops (configured by the BrokenConnectionEventTimeout parameter).</p> <ul style="list-style-type: none"> ▪ [0] Ignore = The call is maintained despite no media and is released when signaling ends the call (i.e., SIP BYE). ▪ [1] Disconnect = (Default) The device ends the call. ▪ [2] Reroute = The device ends the call and searches the IP-to-IP Routing table for a matching rule and if found, generates a new INVITE to the corresponding destination (i.e., alternative routing). You can configure a routing rule whose matching characteristics is explicitly for calls with broken RTP connections. This is done using the Call Trigger parameter, as described in Configuring SBC IP-to-IP Routing Rules on page 470. <p>Note:</p> <ul style="list-style-type: none"> ▪ The device can only detect a broken RTP connection if silence compression is disabled for the RTP session.

Parameter	Description
	<ul style="list-style-type: none"> ▪ If during a call the source IP address (from where the RTP packets are received by the device) is changed without notifying the device, the device rejects these RTP packets. To overcome this, configure the DisconnectOnBrokenConnection parameter to 0. By this configuration, the device doesn't detect RTP packets arriving from the original source IP address and switches (after 300 msec) to the RTP packets arriving from the new source IP address. ▪ The corresponding global parameter is DisconnectOnBrokenConnection.
Media IP Version Preference media-ip-version-preference [IpProfile_MediaIPVersionPreference]	<p>Defines the preferred RTP media IP addressing version for outgoing SIP calls (according to RFC 4091 and RFC 4092). The RFCs concern Alternative Network Address Types (ANAT) semantics in the SDP to offer groups of network addresses (IPv4 and IPv6) and the IP address version preference to establish the media stream. The IP address is indicated in the "c=" field (Connection) of the SDP.</p> <ul style="list-style-type: none"> ▪ [0] Only IPv4 = (Default) SDP offer includes only IPv4 media IP addresses. ▪ [1] Only IPv6 = SDP offer includes only IPv6 media IP addresses. ▪ [2] Prefer IPv4 = SDP offer includes IPv4 and IPv6 media IP addresses, but the first (preferred) media is IPv4. ▪ [3] Prefer IPv6 = SDP offer includes IPv4 and IPv6 media IP addresses, but the first (preferred) media is IPv6. <p>To indicate ANAT support, the device uses the SIP Allow header or to enforce ANAT it uses the Require header: Require: sdp-anat</p> <p>In the outgoing SDP, each 'm=' field is associated with an ANAT group. This is done using the 'a=mid:' and 'a=group:ANAT' fields. Each 'm=' field appears under a unique 'a=mid:' number, for example:</p> <pre>a=mid:1 m=audio 63288 RTP/AVP 0 8 18 101 c=IN IP6 3000::290:8fff:fe40:3e21</pre> <p>The 'a=group:ANAT' field shows the 'm=' fields belonging to it, using the number of the 'a=mid:' field. In addition, the ANAT group with the preferred 'm=' fields appears first. For example, the preferred group includes 'm=' fields under 'a=mid:1' and 'a=mid3':</p> <pre>a=group:ANAT 1 3 a=group:ANAT 2 4</pre> <p>If you configure the parameter to a "prefer" option, the outgoing SDP offer contains two medias which are the same except for the "c=" field. The first media is the preferred address type (and this type is also on the session level "c=" field), while the second media has its "c=" field with the other address type. Both medias are grouped by ANAT. For example, if the incoming SDP contains two</p>

Parameter	Description
	<p>medias, one secured and the other non-secured, the device sends the outgoing SDP with four medias:</p> <ul style="list-style-type: none"> ▪ Two secured medias grouped in the first ANAT group, one with IPv4 and the other with IPv6. The first is the preferred type. ▪ Two non-secured medias grouped in the second ANAT group, one with IPv4 and the other with IPv6. The first is the preferred type. <p>Note:</p> <ul style="list-style-type: none"> ▪ The parameter is applicable only when the device offers an SDP. ▪ The IP addressing version is determined according to the first SDP "m=" field. ▪ The feature is applicable to any type of media (e.g., audio and video) that has an IP address. ▪ The corresponding global parameter is <code>MediaIPVersionPreference</code>.
<p>RTP Redundancy Depth <code>rtp-redundancy-depth</code> <code>[IpProfile_RTPTRedundancyDepth]</code></p>	<p>Enables the device to generate RFC 2198 redundant packets. This can be used for packet loss where the missing information (audio) can be reconstructed at the receiver's end from the redundant data that arrives in subsequent packets. This is required, for example, in wireless networks where a high percentage (up to 50%) of packet loss can be experienced.</p> <ul style="list-style-type: none"> ▪ [0] 0 = (Default) Disable. ▪ [1] 1 = Enable - previous voice payload packet is added to current packet. <p>Note:</p> <ul style="list-style-type: none"> ▪ When enabled, you can configure the payload type, using the <code>RFC2198PayloadType</code> parameter. ▪ The corresponding global parameter is <code>RTPTRedundancyDepth</code>.
Gateway Answering Machine	
<p>AMD Sensitivity Parameter Suite <code>amd-sensitivity-parameter-suite</code> <code>[IpProfile_AMDSensitivityParameterSuite]</code></p>	<p>Defines the AMD Parameter Suite to use for the Answering Machine Detection (AMD) feature.</p> <ul style="list-style-type: none"> ▪ [0] 0 = (Default) Parameter Suite 0 based on North American English with standard detection sensitivity resolution (8 sensitivity levels, from 0 to 7). This AMD Parameter Suite is provided by the AMD Sensitivity file, which is shipped pre-installed on the device. ▪ [1] 1 = Parameter Suite based 1 on North American English with high detection sensitivity resolution (16 sensitivity levels, from 0 to 15). This AMD Parameter Suite is provided by the AMD Sensitivity file, which is shipped pre-installed on the device. ▪ [2] 2 to [7]7 = Optional Parameter Suites that you can create based on any language (16 sensitivity levels, from 0 to 15). This requires a customized AMD Sensitivity file that needs to be installed on the device. For more information, contact your AudioCodes sales

Parameter	Description
	representative. Note: <ul style="list-style-type: none"> ▪ To configure the detection sensitivity level, use the 'AMD Sensitivity Level' parameter. ▪ For more information on the AMD feature, see Answering Machine Detection (AMD) on page 192. ▪ The corresponding global parameter is AMDSensitivityParameterSuit.
AMD Sensitivity Level amd-sensitivity-level [lpProfile_AMDSensitivityLevel]	Defines the AMD detection sensitivity level of the selected AMD Parameter Suite (using the 'AMD Sensitivity Parameter Suite' parameter). For Parameter Suite 0, the valid range is 0 to 7, where 0 is for best detection of an answering machine and 7 for best detection of a live call. For any Parameter Suite other than 0, the valid range is 0 to 15, where 0 is for best detection of an answering machine and 15 for best detection of a live call. Note: The corresponding global parameter is AMDSensitivityLevel.
AMD Max Greeting Time amd-max-greeting-time [lpProfile_AMDMaxGreetingTime]	Defines the maximum duration (in 5-msec units) that the device can take to detect a greeting message. The valid range value is 0 to 51132767. The default is 300. Note: The corresponding global parameter is AMDMaxGreetingTime.
AMD Max Post Silence Greeting Time amd-max-post-silence-greeting-time [lpProfile_AMDMaxPostSilenceGreetingTime]	Defines the maximum duration of silence from after the greeting time is over (configured by AMDMaxGreetingTime) until the device's AMD decision. Note: The corresponding global parameter is AMDMaxPostGreetingSilenceTime.

Part V

Session Border Controller Application

22 SBC Overview

This section provides an overview of the device's SBC application.

**Note:**

- For guidelines on how to deploy your SBC device, refer to the *SBC Design Guide* document.
- The SBC feature is available only if the device is installed with a License Key that includes this feature. For installing a License Key, see "License Key" on page 597.
- For the maximum number of supported SBC sessions, and SBC users than can be registered in the device's registration database, see "Technical Specifications" on page 857.

22.1 Feature List

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 and with far-end users located behind NAT on the WAN. The device supports this by:
 - Continually registering far-end users with its users registration database.
 - Maintaining remote NAT binding state by frequent registrations and 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 SDP offer-answer negotiations.
 - ◆ Deep packet inspection of all RTP packets.
 - ◆ Late rogue detection - if a SIP session was gracefully terminated and someone tries to "ride on it" with rogue 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.
- Stateful Proxy Operation Mode: The device can act as a Stateful Proxy by enabling SIP messages to traverse it transparently (with minimal interference) between the inbound and outbound legs.
- B2BUA and 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.
- User-defined manipulation of SIP To, From, and Request-URI host names.
- Generates a new SIP Call-ID header value (different between legs).
- Changes the SIP Contact header and sets it to the device's 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.

22.2 B2BUA and Stateful Proxy Operating Modes

The device can operate in one or both of the following SBC modes:

- **Back-to-Back User Agent (B2BUA):** Maintains independent sessions toward the endpoints, processing an incoming request as a user agent server (UAS) on the inbound leg, and processing the outgoing request as a user agent client (UAC) on the outbound leg. SIP messages are modified regarding headers between the legs and all the device's interworking features may be applied.
- **Stateful Proxy Server:** SIP messages traverse the device transparently (with minimal interference) between the inbound and outbound legs, for connecting SIP endpoints.

By default, the device's B2BUA mode changes SIP dialog identifiers and topology data in SIP messages traversing through it:

- Call identifiers: Replaces the From-header tag and Call-ID header so that they are different for each leg (inbound and outbound).
- Routing headers:
 - Removes all Via headers in incoming requests and sends the outgoing message with its own Via header.
 - Doesn't forward any Record-Route headers from the inbound to outbound leg, and vice versa.

- Replaces the address of the Contact header in the incoming message with its own address in the outgoing message.
- Replaces the User-Agent/ Server header value in the outgoing message, and replaces the original value with itself in the incoming message.

In contrast, when the device operates in Stateful Proxy mode, the device by default forwards SIP messages transparently (unchanged) between SIP endpoints (from inbound to outbound legs). The device retains the SIP dialog identifiers and topology headers received in the incoming message and sends them as is in the outgoing message. The device handles the above mentioned headers transparently (i.e., they remain unchanged) or according to configuration (enabling partial transparency), and only adds itself as the top-most Via header and optionally, to the Record-Route list. To configure the handling of these headers for partial transparency, use the following IP Profile parameters (see "Configuring IP Profiles" on page 388):

- IpProfile_SBCRemoteRepresentationMode: Contact and Record-Route headers
- IpProfile_SBCKeepVIAHeaders: Via headers
- IpProfile_SBCKeepUserAgentHeader: User-Agent headers
- IpProfile_SBCKeepRoutingHeaders: Record-Route headers
- IpProfile_SBCRemoteMultipleEarlyDialogs: To-header tags

Thus, the Stateful Proxy mode provides full SIP transparency (no topology hiding) or asymmetric topology hiding. Below is an example of a SIP dialog-initiating request when operating in Stateful Proxy mode for full transparency, showing all the incoming SIP headers retained in the outgoing INVITE message.

Figure 22-1: Example of SIP Message Handling in Stateful Proxy Mode

Incoming INVITE	Outgoing INVITE
<pre> INVITE sip:bob@domain.com SIP/2.0 To: Bob <sip:bob@domain.com> From: Alice <sip:alice@caller.com>;tag=100 Call-ID: callid1@caller.com Contact: <sip:alice@pc1.caller.com> Via: SIP/2.0/UDP pc2.com;branch=brancn2 Via: SIP/2.0/UDP pc1.com;branch=brancn1 Record-Route: <pc2.com;lr> Record-Route: <pc1.com;lr> CSeq: 666 INVITE User-Agent: IPPv3.1 Max-Forwards: 70 Content-Type: application/sdp Content-Length: 142 v=0 ... </pre>	<pre> INVITE sip:bob@domain.com SIP/2.0 To: Bob <sip:bob@domain.com> From: Alice <sip:alice@caller.com>;tag=100 Call-ID: callid1@caller.com Contact: <sip:alice@pc1.caller.com> Via: SIP/2.0/UDP Proxy-IP;branch=brancn3 Via: SIP/2.0/UDP pc2.com;branch=brancn2 Via: SIP/2.0/UDP pc1.com;branch=brancn1 Record-Route: <Proxy-IP;lr> Record-Route: <pc2.com;lr> Record-Route: <pc1.com;lr> CSeq: 666 INVITE User-Agent: IPPv3.1 Max-Forwards: 70 Content-Type: application/sdp Content-Length: 142 v=0 ... </pre>

Some of the reasons for implementing Stateful Proxy mode include:

- B2BUA typically hides certain SIP headers for topology hiding. In specific setups, some SIP servers require the inclusion of these headers to know the history of the SIP request. In such setups, the requirement may be asymmetric topology hiding, whereby SIP traffic toward the SIP server must expose these headers whereas SIP traffic toward the users must not expose these headers.
- B2BUA changes the call identifiers between the inbound and outbound SBC legs and therefore, call parties may indicate call identifiers that are not relayed to the other leg. Some SIP functionalities are achieved by conveying the SIP call identifiers either in SIP specific headers (e.g., Replaces) or in the message bodies (e.g. Dialog Info in an XML body).

- In some setups, the SIP client authenticates using a hash that is performed on one or more of the headers that B2BUA changes (removes). Therefore, implementing B2BUA would cause authentication to fail.
- For facilitating debugging procedures, some administrators require that the value in the Call-ID header remains unchanged between the inbound and outbound SBC legs. As B2BUA changes the Call-ID header, such debugging requirements would fail.

The operating mode can be configured per the following configuration entities:

- SRDs in the SRDs table (see "Configuring SRDs" on page 311)
- IP Groups in the IP Groups table (see "Configuring IP Groups" on page 329)

If the operation mode is configured in both tables, the operation mode of the IP Group is applied. Once configured, the device uses default settings in the IP Profiles table for handling the SIP headers, as mentioned previously. However, you can change the default settings to enable partial transparency.

Note:

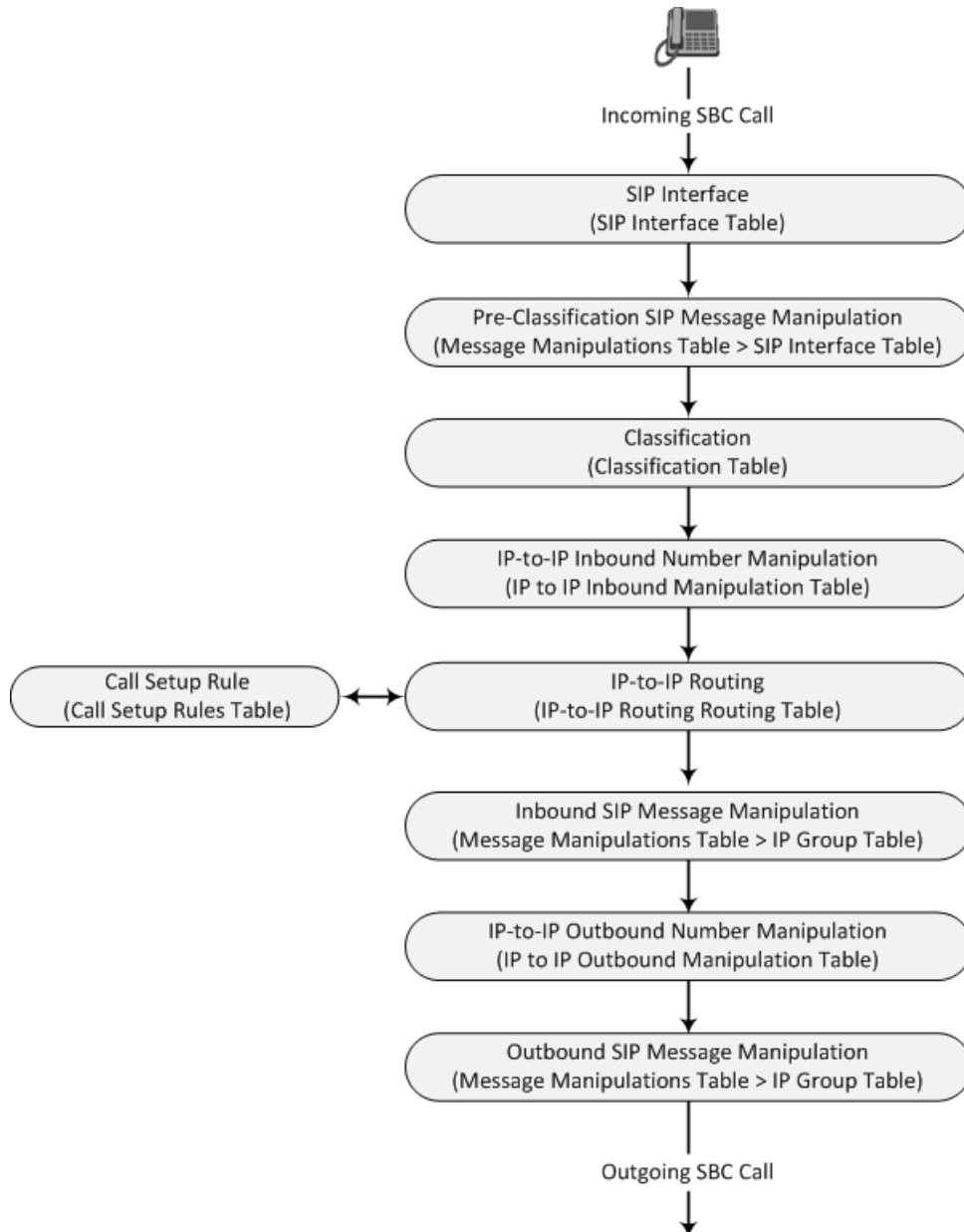
- The To-header tag remains the same for inbound and outbound legs of the dialog, regardless of operation mode.
- If the Operation Mode of the SRD\IP Group of one leg of the dialog is set to 'Call Stateful Proxy', the device also operates in this mode on the other leg with regards to the dialog identifiers (Call-ID header, tags, CSeq header).
- It is recommended to implement the B2BUA mode, unless one of the reasons mentioned previously is required. B2BUA supports all the device's feature-rich offerings, while Stateful Proxy may offer only limited support. The following features are not supported when in Stateful Proxy mode:
 - ✓ Alternative routing
 - ✓ Call forking
 - ✓ Terminating REFER/3xx
- If Stateful Proxy mode is enabled and any one of the unsupported features is enabled, the device disables the Stateful Proxy mode and operates in B2BUA mode.
- You can configure the device to operate in both B2BUA and Stateful Proxy modes for the same users. This is typically implemented when users need to communicate with different SIP entities (IP Groups). For example, B2BUA mode for calls destined to a SIP Trunk and Stateful Proxy mode for calls destined to an IP PBX. The configuration is done using IP Groups and SRDs.
- If Stateful Proxy mode is used only due to the debugging benefits, it is recommended to configure the device to only forward the Call-ID header unchanged



22.3 Call Processing of SIP Dialog Requests

The device processes incoming SIP dialog requests (SIP methods) such as INVITE, SUBSCRIBE, OPTIONS, REFER, INFO, UNSOLICITED NOTIFY, MESSAGE, and REGISTER. The process is summarized in the following figure and subsequently described:

Figure 22-2: SBC Call Processing



The SIP dialog-initiating process consists of the following stages:

- 1. Determining Source and Destination URL:** The SIP protocol has more than one URL in a dialog-initiating request that may represent the source and destination URLs. The device obtains the source and destination URLs from certain SIP headers. Once the URLs are determined, the user and host parts of the URLs can be used as matching rule characteristics for classification, message manipulation, and call routing.

- **All SIP requests (e.g., INVITE) except REGISTER:**
 - ◆ Source URL: 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: Obtained from the Request-URI.
- **REGISTER dialogs:**
 - ◆ Source URL: Obtained from the To header.
 - ◆ Destination URL: Obtained from the Request-URI.



Note: You can specify the SIP header from where you want the device to obtain the source URL in the incoming dialog request. This is configured in the IP Groups table using the 'Source URI Input' parameter (see "Configuring IP Groups" on page 329).

2. **Determining SIP Interface:** The device checks the SIP Interface on which the SIP dialog is received. The SIP Interface defines the local SIP "listening" port and IP network interface. For more information, see "Configuring SIP Interfaces" on page 321.
3. **Applying SIP Message Manipulation:** Depending on configuration, the device can apply a SIP message manipulation rule (assigned to the SIP Interface) on the incoming SIP message. A SIP Message Manipulation rule defines a matching characteristics (*condition*) of the incoming SIP message and the corresponding manipulation operation (e.g., remove the P-Asserted-Identity header), which can apply to almost any aspect of the message (add, remove or modify SIP headers and parameters). For more information, see "Configuring SIP Message Manipulation" on page 362.
4. **Classifying to an IP Group:** Classification identifies the incoming SIP dialog request as belonging to a specific IP Group (i.e., from where the SIP dialog request originated). The classification process is based on the SRD to which the dialog belongs (the SRD is determined according to the SIP Interface). For more information, see "Configuring Classification Rules" on page 461.
5. **Applying Inbound Manipulation:** Depending on configuration, the device can apply an Inbound Manipulation rule to the incoming dialog. This manipulates the user part of the SIP URI for source (e.g., in the SIP From header) and destination (e.g., in the Request-URI line). The manipulation rule is associated with the incoming dialog, by configuring the rule with incoming matching characteristics such as source IP Group and destination host name. The manipulation rules are also assigned a Routing Policy, which in turn, is assigned to IP-to-IP routing rules. As most deployments require only one Routing Policy, the default Routing Policy is automatically assigned to manipulation and routing rules. For more information, see "Configuring IP-to-IP Inbound Manipulations" on page 493.
6. **SBC IP-to-IP Routing:** The device searches the IP-to-IP Routing table for a routing rule that matches the characteristics of the incoming call. If found, the device routes the call to the configured destination which can be, for example, an IP Group, the Request-URI if the user is registered with the device, and a specified IP address. For more information, see "Configuring SBC IP-to-IP Routing Rules" on page 470.
7. **Applying Inbound SIP Message Manipulation:** Depending on configuration, the device can apply a SIP message manipulation rule (assigned to the IP Group) on the incoming dialog. For more information, see Stage 3.
8. **Applying Outbound Manipulation:** Depending on configuration, the device can apply an Outbound Manipulation rule to the outbound dialog. This manipulates the user part of the Request-URI for source (e.g., in the SIP From header) or destination (e.g., in the SIP To header) or calling name in the outbound SIP dialog. The

manipulation rule is associated with the dialog, by configuring the rule with incoming matching characteristics such as source IP Group and destination host name. The manipulation rules are also assigned a Routing Policy, which in turn, is assigned to IP-to-IP routing rules. As most deployments require only one Routing Policy, the default Routing Policy is automatically assigned to manipulation rules and routing rules. For more information, see "Configuring IP-to-IP Outbound Manipulations" on page 497.

9. **Applying Outbound SIP Message Manipulation:** Depending on configuration, the device can apply a SIP message manipulation rule (assigned to the IP Group) on the outbound dialog. For more information, see Stage 3.
10. The call is sent to the configured destination.

22.4 User Registration

The device provides a registration database for registering users. Only users belonging to a User-type IP Group can register with the device. User-type IP Groups represent a group of SIP user agents that share the following characteristics:

- Perform registrations and share the same serving proxy\registrar
- Same SIP and media behavior
- Same IP Profile
- Same SIP handling configuration
- Same Call Admission Control (CAC)

Typically, the device is configured as the user's outbound proxy, routing requests (using the IP-to-IP Routing table) from the user's User-type IP Group to the serving proxy, and vice versa. Survivability can be achieved using the alternative routing feature.

The device forwards registration requests (REGISTER messages) from a Server-type IP Group, but does not save the registration binding in its' registration database.

22.4.1 Initial Registration Request Processing

A summary of the device's handling of registration requests (REGISTER messages) is as follows:

- The URL in the To header of the REGISTER message constitutes the primary Address of Record (AOR) for registration (according to standard). The device can save other AORs in its registration database as well. When the device searches for a user in its' registration database, any of the user's AORs can result in a match.
- The device's Classification process for initial REGISTER messages is slightly different than for other SIP messages. Unlike other requests, initial REGISTER requests can't be classified according to the registration database.
- If registration succeeds (replied with 200 OK by the destination server), the device adds a record to its' registration database, which identifies the specific contact of the specific user (AOR). The device uses this record to route subsequent SIP requests to the specific user (in normal or survivability modes).
- The records in the device's registration database include the Contact header. The device adds every REGISTER request to the registration database before manipulation, allowing correct user identification in the Classification process for the next received request.
- You can configure Call Admission Control (CAC) rules for incoming and outgoing REGISTER messages. For example, you can limit REGISTER requests from a specific IP Group or SRD. Note that this applies only to concurrent REGISTER dialogs and not concurrent registrations in the device's registration database.

The device provides a dynamic registration database that it updates according to registration requests traversing it. Each database entry for a user represents a binding between an AOR (obtained from the SIP To header), optional additional AORs, and one or more contacts (obtained from the SIP Contact headers). Database bindings are added upon successful registration responses from the proxy server (SIP 200 OK). The device removes database bindings 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 UA did not send a refresh registration request).



Note:

- 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 message is not supported.
- One database is shared between all User-type IP Groups.

22.4.2 Classification and Routing of Registered Users

The device can classify incoming SIP dialog requests (e.g., INVITE) from registered users to an IP Group, by searching for the sender's details in the registration database. The device uses the AOR from the From header and the URL in the Contact header of the request to locate a matching registration binding. The found registration binding contains information regarding the registered user, including the IP Group to which it belongs. (Upon initial registration, the Classification table is used to classify the user to a User-type IP Group and this information is then added with the user in the registration database.)

The destination of a dialog request can be a registered user and the device thus uses its registration database to route the call. This can be achieved by various ways such as configuring a rule in the IP-to-IP Routing table where the destination is a User-type IP Group or any matching user registered in the database ('Destination Type' is configured to **All Users**). The device searches the registration database for a user that matches the incoming Request-URI (listed in chronological order):

1. Unique Contact generated by the device and sent in the initial registration request to the serving proxy.
2. AOR. The AOR is originally obtained from the incoming REGISTER request and must either match both user part and host part of the Request-URI, or only user part.
3. Contact. The Contact is originally obtained from 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 a SIP 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.

You can configure (using the SBCDBRoutingSearchMode parameter) for which part of the destination Request-URI in the INVITE message the device must search in the registration database:

- Only by entire Request-URI (user@host), for example, "4709@joe.company.com".
- By entire Request-URI, but if not found, by the user part of the Request-URI, for example, "4709".

When an incoming INVITE is received for routing to a user and the user is located in the registration database, the device sends the call to the user's corresponding contact address specified in the database.



Note: If the Request-URI contains the "tel:" URI or "user=phone" parameter, the device searches only for the user part.

22.4.3 General Registration Request Processing

The device's general handling of registration requests (REGISTER messages) for unregistered users is as follows:

- The device routes REGISTER requests according to the IP-to-IP Routing table. If the destination is a User-type IP Group, the device does not forward the registration; instead, it accepts (replies with a SIP 200 OK response) or rejects (replies with a SIP 4xx) the request according to the user's IP Group configuration.
- Alternative routing can be configured for REGISTER requests, in the IP-to-IP Routing table.
- By default, the Expires header has the same value in incoming and outgoing REGISTER messages. However, you can modify the Expires value using the following parameters: `SBCUserRegistrationTime`, `SBCProxyRegistrationTime`, `SBCRandomizeExpires`, and `SBCSurvivabilityRegistrationTime`. You can also modify the Expires value of REGISTER requests received from users located behind NAT, using the IP Profile parameters `IpProfile_SBCUserBehindUdpNATRegistrationTime` and `IpProfile_SBCUserBehindTcpNATRegistrationTime`.
- By default, the Contact header in outgoing REGISTER message is different than the Contact header in the incoming REGISTER. The user part of the Contact is populated with a unique contact generated by the device and associated with the specific registration. The IP address in the host part is changed to the address of the device. Alternatively, the original user can be retained in the Contact header and used in the outgoing REGISTER request (using the `SBCKeepContactUserinRegister` parameter).

22.4.4 Registration Refreshes

Registration refreshes are incoming REGISTER requests from users that are registered in the device's registration database. The device sends these refreshes to the serving proxy only if the serving proxy's Expires time is about to expire; otherwise, the device responds with a 200 OK to the user, without routing the REGISTER. Each such refreshes also refresh the internal timer set on the device for this specific registration.

The device automatically notifies SIP proxy / registrar servers of users that are registered in its registration database and whose registration timeout has expired. When a user's registration timer expires, the device removes the user's record from the database and sends an un-register notification (REGISTER message with the Expires header set to 0) to the proxy/registrar. This occurs only if a REGISTER message is sent to an IP Group destination type (in the IP-to-IP Routing table).

You can also apply a graceful period to unregistered requests, using the 'User Registration Grace Time' parameter (`SBCUserRegistrationGraceTime`):

- You can configure the device to add extra time (grace period) to the expiration timer of registered users in the database. If you configure this grace period, the device keeps the user in the database (and does not send an un-register to the registrar server), allowing the user to send a "late" re-registration to the device. The device removes the

user from the database only when this additional time expires.

- The graceful period is also used before removing a user from the registration database when the device receives a successful unregister response (200 OK) from the registrar/proxy server. This is useful in scenarios, for example, in which users (SIP user agents) such as IP Phones erroneously send unregister requests. Instead of immediately removing the user from the registration database upon receipt of a successful unregister response, the device waits until it receives a successful unregister response from the registrar server, waits the user-defined graceful time and if no register refresh request is received from the user agent, removes the contact (or AOR) from the database.

The device keeps registered users in its' registration database even if connectivity with the proxy is lost (i.e., proxy does not respond to users' registration refresh requests). The device removes users from the database only when their registration expiry time is reached (with the additional grace period, if configured).

22.4.5 Registration Restriction Control

The device provides flexibility in controlling user registrations:

- **Limiting Number of Registrations:** You can limit the number of users that can register with the device per IP Group, SIP Interface, and/or SRD, in the IP Group, SIP Interface and SRDs tables respectively. By default, no limitation exists.
- **Blocking Incoming Calls from Unregistered Users:** You can block incoming calls (INVITE requests) from unregistered users belonging to User-type IP Groups. By default, calls from unregistered users are not blocked. This is configured per SIP Interface or SRD. When the call is rejected, the device sends a SIP 500 (Server Internal Error) response to the remote end.

22.4.6 Deleting Registered Users

You can remove registered users from the device's registration database through CLI:

- To delete a specific registered user:

```
# clear voip register db sbc user <AOR of user - user part or user@host>
```

For example:

```
# clear voip register db sbc user John@10.33.2.22
# clear voip register db sbc user John
```

- To delete all registered users belonging to a specific IP Group:

```
# clear voip register db sbc ip-group <ID or name>
```

22.5 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 multiple media sessions of different types (e.g. audio and fax). In a SIP dialog, multiple offer-answer transactions may occur and each may change the media session 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 (e.g., audio, secure audio, video, fax, and 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

Typically, the device does not change the negotiated media capabilities (mainly performed by the remote user agents). However, it does examine and may take an active role in the SDP offer-answer mechanism. This is done mainly to anchor the media to the device (default) and also to change the negotiated media type, if configured. Some of the media handling features, which are described later in this section, include the following:

- Media anchoring (default)
- Direct media
- Audio coders restrictions
- Audio coders transcoding
- RTP-SRTP transcoding
- DTMF translations
- Fax translations and detection
- Early media and ringback tone handling
- Call hold translations and held tone generation
- NAT traversal
- RTP broken connections
- Media firewall
 - 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.

22.5.1 Media Anchoring

By default, the device anchors the media (RTP) traffic. In other words, the media between SIP endpoints traverses the device. You can change this default mode by enabling direct media between SIP endpoints. Media anchoring may be required, for example, to resolve NAT problems, enforce media security policies, perform media transcoding, and media monitoring.

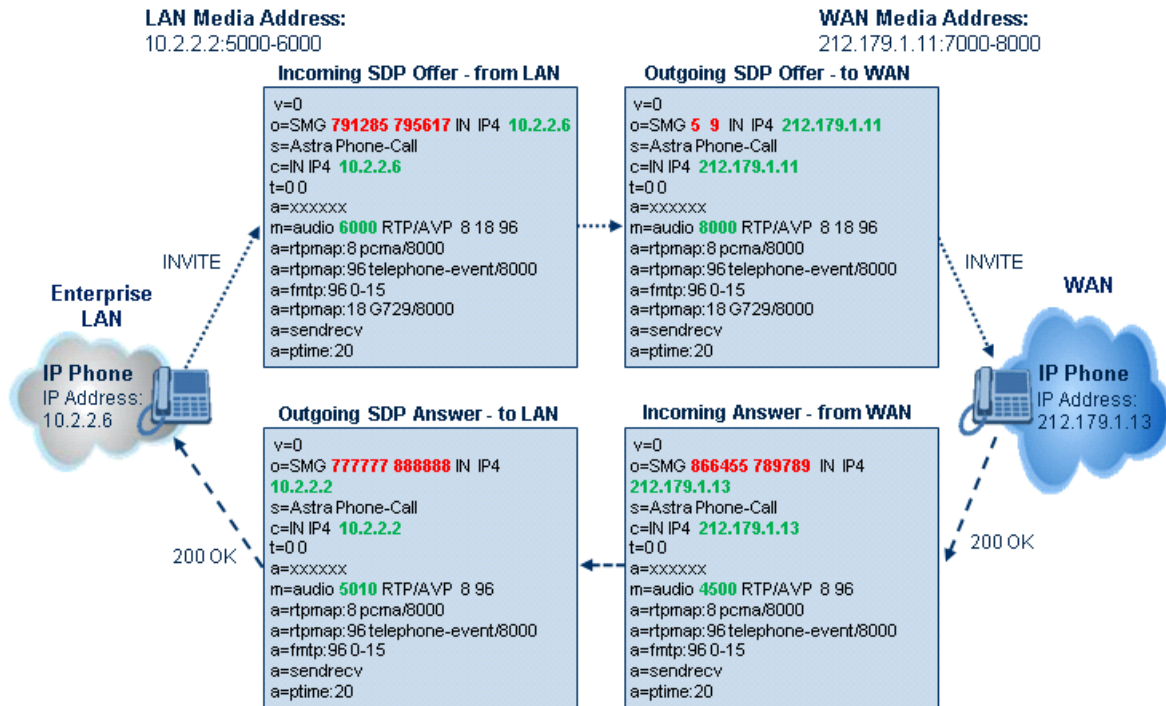
To enforce RTP traffic to flow through the device, the device modifies all IP address fields in the SDP:

- 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

The device uses different local ports (e.g., for RTP, RTCP and fax) for each leg (inbound and outbound). The local ports are allocated from the Media Realm associated with each

leg. The Media Realm assigned to the leg's IP Group (in the IP Groups table) is used. If not assigned to the IP Group, the Media Realm assigned to the leg's SIP Interface (in the SIP Interfaces table) is used. The following figure provides 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 22-3: SDP Offer/Answer Example



22.5.2 Direct Media

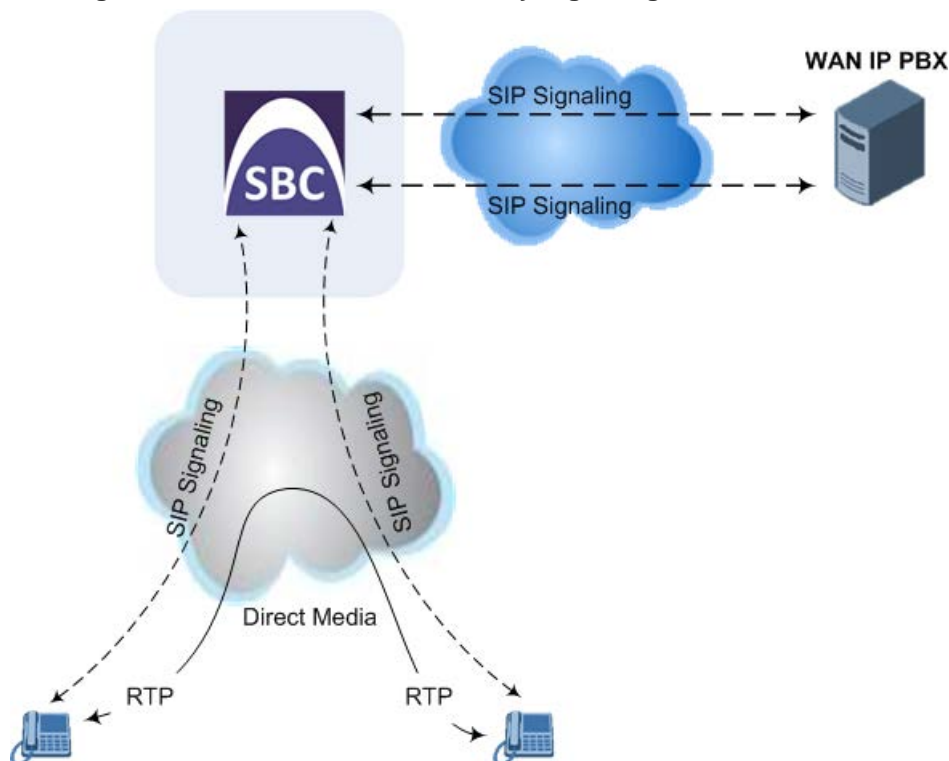
You can configure the device to allow the media (RTP/SRTP) session to flow directly between the SIP endpoints, without traversing the device. This is referred to as No Media Anchoring (also known as Anti-Tromboning or Direct Media). SIP signaling continues to traverse the device, with minimal intermediation and involvement, to enable certain SBC capabilities such as routing. By default, the device employs media anchoring, whereby the media session traverses the device, as described in "Media Anchoring" on page 431.

Direct media offers the following benefits:

- Saves network bandwidth
- Reduces the device's CPU usage (as there is no media handling)
- Avoids interference in SDP negotiation and header manipulation on RTP/SRTP

Direct media is typically implemented for calls between users located in the same LAN or domain, and where NAT traversal is not required and other media handling features such as media transcoding is not required. The following figure provides an example of direct media between LAN IP phones, while SIP signaling continues to traverse the device between LAN IP phones and the hosted WAN IP-PBX.

Figure 22-4: Direct Media where only Signaling Traverses Device



➤ **To enable direct media:**

- **For all calls:** Use the global parameter, `SBCDirectMedia` (overrides all other direct media configuration).
- **For specific calls:**
 - **SIP Interface:** You can enable direct media per SIP Interface (in the SIP Interfaces table), whereby calls (source and destination) associated with **this same** SIP Interface are handled as direct media calls. The SIP Interface can also enable direct media for users located behind the same NAT. For more information, see "Configuring SIP Interfaces" on page 321.
 - **Direct Media Tag:** You can enable direct media between users that are configured with the same Direct Media tag value. The tag is configured using the IP Profiles table's `IPProfile_SBCDirectMediaTag` parameter (see "Configuring IP Profiles" on page 388).

The device employs direct media between endpoints under the following configuration conditions (listed in chronological order):

1. Direct media is enabled by the global parameter (`SBCDirectMedia`).
2. IP Groups of the endpoints are associated with IP Profiles whose 'Direct Media Tag' parameter has the same value (non-empty value).
3. IP Groups of the endpoints have the 'SBC Operation Mode' parameter set to **Microsoft Server** (direct media is required in the Skype for Business environment). For more information, see "Configuring IP Groups" on page 329.
4. IP Groups of the endpoints use the same SIP Interface and the SIP Interface's 'SBC

Direct Media' parameter is set to **Enable** (SIPInterface_SBCDirectMedia = 1).

5. IP Groups of the endpoints use the same SIP Interface and the SIP Interface's 'SBC Direct Media' parameter is set to Enable When Single NAT (SIPInterface_SBCDirectMedia = 2), and the endpoints are located behind the same NAT.

Note:

- If you enable direct media by the SBCDirectMedia parameter, direct media is applied to all calls even if direct media is disabled per SIP Interface.
- If you configure direct media for all calls (using the SBCDirectMedia parameter), the device does not open voice channels nor allocate media ports for the calls, as the media always bypasses the device. In contrast, if you configure direct media for specific calls, the device allocates ports for these calls. The reason is that the ports may be required for mid-call services (e.g., early media, call forwarding, call transfer, and playing on-hold tones) handled by the server (IP PBX), which traverse the device. Therefore, make sure that you have allocated sufficient media ports (Media Realm) for such calls.
- Direct media cannot operate with the following features:
 - ✓ Manipulation of SDP data (offer-answer transaction) such as ports, IP address, coders
 - ✓ Force transcoding
 - ✓ Extension Coders
 - ✓ Extension of RFC 2833 / out-of-band DTMF / in-band DTMF
 - ✓ Extension of SRTP/RTP
- All restriction features (Allowed Coders, restrict SRTP/RTP, restrict RFC 2833) can operate with direct media. Restricted coders are removed from the SDP offer message.
- For two users belonging to the same SIP Interface that is enabled for direct media and one of the users is defined as a foreign user (example, "follow me service") located in the WAN while the other is located in the LAN: calls between these two users cannot be established until direct media is disabled for the SIP Interface. The reason for this is that the device does not interfere in the SIP signaling. In other words, parameters such as IP addresses are not manipulated for calls between LAN and WAN (although required).



22.5.3 Restricting Audio Coders

You can configure a list of permitted (allowed) voice coders that can be used for a specific SIP entity (leg). In other words, you can enforce the use of specific coders. If the SDP offer in the incoming SIP message does not contain any coder that is configured as an allowed coder, the device rejects the calls (unless transcoding is implemented whereby Extension coders are added to the SDP, as described in Coder Transcoding on page 435). If the SDP offer contains some coders that are configured as allowed coders, the device manipulates the SDP offer by removing the coders that are not configured as allowed coders, before routing the SIP message to its destination. The device also re-orders (prioritizes) the coder list in the SDP according to the listed order of configured allowed coders.

For example, assume the following:

- The SDP offer in the incoming SIP message contains the G.729, G.711, and G.723 coders.
- The allowed coders configured for the SIP entity include G.711 and G.729.

The device removes the G.723 coder from the SDP offer, re-orders the coder list so that G.711 is listed first, and sends the SIP message containing only the G.711 and G.729 coders in the SDP.

The allowed coders are configured in the Allowed Audio Coders Groups table. For more information, see "Configuring Allowed Audio Coder Groups" on page 384.



Note: If you assign the SIP entity an Allowed Audio Coders Group for coder restriction and a Coders Group for extension coders (i.e., voice transcoding), the allowed coders take precedence over the extension coders. In other words, if an extension coder is not listed as an allowed coder, the device does not add the extension coder to the SDP offer.

22.5.4 Coder Transcoding

By default, the device forwards media packets transparently (i.e., no media negotiation) between SIP endpoints. However, when there are no common coders between two SIP entities that need to establish voice communication (i.e., the SDP answer from one SIP entity doesn't include any coder included in the SDP offer previously sent by the other), you can configure the device to perform audio coder transcoding between the inbound and outbound legs in order to enable media flow between them.

Transcoding may also be performed in scenarios where the same coder has been chosen between the legs, but where coder transrating is required. For example, the coders may use different coder settings such as rate and packetization time (G.729 at 20 ms to G.729 at 30 ms).

The coders that the device adds to the SDP offer on the outbound leg is referred to as *extension coders*. The extension coders are configured using Coder Groups (see "Configuring Coder Groups" on page 379), which you need to then assign to the IP Profile associated with the SIP entity.

The figure below illustrates transcoding between two SIP entities (IP Groups) where one uses G.711 (LAN IP phone) and the other G.729 (WAN IP phone). The initial SDP offer received on the inbound leg from the LAN IP phone includes coder G.711 as the supported coder. In the outgoing SDP offer on the outbound leg to the WAN IP phone, the device adds extension coder G.729 to the SDP, which is supported by the WAN IP phone. The subsequent incoming SDP answer from the WAN IP phone includes the G.729 coder as the chosen coder. Since this coder was not included in the original incoming SDP offer from the LAN IP phone, the device performs G.729-G.711 transcoding between the inbound and outbound legs.


Note:

- If you assign a SIP entity an Allowed Audio Coders Group for coder restriction (allowed coders) and a Coders Group for extension coders, the allowed coders take precedence over the extension coders. In other words, if an extension coder is not listed as an allowed coder, the device does not add the extension coder to the SDP offer.
- If none of the coders in the incoming SDP offer on the inbound leg appear in the associated Allowed Audio Coders Group for coder restriction, the device rejects the call (sends a SIP 488 to the SIP entity that initiated the SDP offer).
- If none of the coders (including extension coders) in the outgoing SDP offer on the outbound leg appear in the associated Allowed Audio Coders Group for coder restriction, the device rejects the call (sends a SIP 488 to the SIP entity that initiated the SDP offer).
- For coder transcoding, the following prerequisites must be met (otherwise, the extension coders are not added to the SDP offer):
 - ✓ The device must support at least one of the coders listed in the incoming SDP offer.
 - ✓ The device must have available DSPs for both legs (inbound and outbound).
 - ✓ The incoming SDP offer must have at least one media line that is audio ('m=audio').
- The device adds the extension coders below the coder list received in the original SDP offer. This increases the chance of media flow without requiring transcoding.
- The device does not add extension coders that also appear in the original SDP offer.

As an example for using allowed and extension coders, assume the following:

■ Inbound leg:

- Incoming SDP offer includes the G.729, G.711, and G.723 coders.

```
m=audio 6050 RTP/AVP 18 0 8 4 96
a=rtpmap:18 G729/8000
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:4 G723/8000
a=fmtp:4 annexa=no
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
a=ptime:20
a=sendrecv
```

The SDP "m=audio 6010 RTP/AVP 18 0 8 4 96" line shows the coder priority, where "18" (G.729) is highest and "4" (G.723) is lowest.

- Allowed Audio Coders Group for coder restriction includes the G.711 and G.729 coders (listed in order of appearance).

■ Outbound leg:

- Allowed Audio Coders Group for coder restriction includes the G.723, G.726, and G.729 coders (listed in order of appearance).
 - Allowed Audio Coders Group for coder extension (transcoding) includes the G.726 coder.
1. On the inbound leg for the incoming SDP offer: The device allows and keeps the coders in the SDP that also appear in the Allowed Audio Coders Group for coder restriction (i.e., G.711 and G.729). It changes the order of listed coders in the SDP so that G.711 is listed first. The device removes the coders (i.e., G.723) from the SDP that do not appear in the Allowed Audio Coders Group for coder restriction.

```
m=audio 6050 RTP/AVP 0 8 18 96
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=fmtp:4 annexa=no
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
aptime:20
a=sendrecv
```

2. On the outbound leg for the outgoing SDP offer: The SDP offer now includes only the G.711 and G.729 coders due to the coder restriction process on the incoming SDP offer (see Step 1).

- a. The device adds the extension coder to the SDP offer and therefore, the SDP offer now includes the G.711, G.729 and G.726 coders.

```
m=audio 6050 RTP/AVP 0 8 18 96 96
a=rtpmap:0 PCMU/8000
a=rtpmap:8 PCMA/8000
a=rtpmap:18 G729/8000
a=rtpmap:96 G726-32/8000
a=fmtp:4 annexa=no
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
aptime:20
a=sendrecv
```

- b. The device applies coder restriction to the SDP offer. As the Allowed Audio Coders Group for coder restriction includes the G.723, G.726, and G.729 coders, the device allows and keeps the G.729 and G.726, but removes the G.711 coder as it does not appear in the Allowed Audio Coders Group for coder restriction.

```
m=audio 6050 RTP/AVP 18 96 96
a=rtpmap:18 G729/8000
a=rtpmap:96 G726-32/8000
a=fmtp:4 annexa=no
a=rtpmap:96 telephone-event/8000
a=fmtp:96 0-15
aptime:20
a=sendrecv
```

3. The device includes only the G.729 and G.726 coders in the SDP offer that it sends from the outgoing leg to the outbound SIP entity. The G.729 is listed first as the Allowed Audio Coders Group for coder restriction takes precedence over the extension coder.

➤ **To configure coder transcoding:**

1. In the Coder Groups table, configure a Coders Group for extension coders. For more information, see "Configuring Coder Groups" on page 379.
2. In the IP Profiles table, configure the IP Profile associated with the SIP entity:
 - a. Assign the Coders Group to the IP Profile, using the 'Extension Coders Group' parameter (SBCExtensionCodersGroupName).
 - b. Enable extension coders by configuring the 'Allowed Coders Mode' parameter to **Restriction** or **Restriction and Preference**.


Note:

- To implement transcoding, you must configure the number of required DSP channels for transcoding (for example, MediaChannels = 120). Each transcoding session uses two DSP resources.
- The transcoding mode can be configured globally, using the TranscodingMode parameter or for specific calls, using the IP Profiles table.
-

22.5.5 Transcoding Mode

By default, the device performs transcoding only if required. This refers to all types of transcoding (interworking) that require DSPs such as voice coder transcoding, DTMF negotiations, and fax negotiations. Transcoding is required, for example, when two SIP entities use different coders. In such a scenario, you would need to configure transcoding (i.e., extension coders), the device performs coder transcoding between the legs (inbound and outbound). If the SIP entities use the same coder, the device does not perform transcoding.

Alternatively, you can configure the device to always perform transcoding, regardless whether it is required or not. This is referred to as *forced* transcoding. For example, if the SIP entities use the same coder, the device performs transcoding of the same coder (e.g., G.711 and G.711) between the two legs.

The transcoding mode can be configured globally (TranscodingMode parameter) or per SIP entity using IP Profiles (IpProfile_TranscodingMode parameter).



Note: If the transcoding mode is configured to **Force** (i.e., always performs transcoding) for an IP Profile associated with a specific SIP entity, the device also applies forced transcoding for the SIP entity communicating with this SIP entity, regardless of its IP Profile settings.

22.5.6 Prioritizing Coder List in SDP Offer

In addition to restricting the use of coders using Allowed Audio Coders Groups (see "Configuring Allowed Audio Coder Groups" on page 384), you can also prioritize the coders listed in the SDP offer. This feature is referred to as *Coder Preference* and applies to both SBC legs:

- **Incoming SDP offer:** The device arranges the coder list in the incoming SDP offer according to the order of appearance of the Allowed Audio Coders Group that is associated with the incoming dialog. The coders listed higher up in the group take preference over ones listed lower down. To configure this, configure the 'Allowed Coders Mode' parameter (IpProfile_SBCAllowedCodersMode) in the associated IP Profile to **Preference** or **Restriction and Preference**. If you configure the parameter to **Preference**, the coders in the SDP offer that also appear in the Allowed Audio Coders Group are listed first in the SDP offer, and the coders in the SDP offer that do not appear in the Allowed Audio Coders Group are listed after the Allowed coders in the SDP offer. Therefore, this setting does not restrict coder use to Allowed coders, but uses (prefers) the Allowed coders whenever possible.
- **Outgoing SDP offer:** If only Allowed coders are used, the device arranges the coders in the SDP offer as described above.

However, if Extension coders are also used, the coder list is arranged according to the SBCPreferencesMode parameter. Depending on the parameter's settings, the

Extension coders are added after the Allowed coders according to their order in the Allowed Audio Coders Group, or the Allowed and Extension coders are arranged according to their position in the Allowed Audio Coders Group.

22.5.7 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, 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.

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.

DSP resources are not required for RTP-SRTP transcoding.

22.5.8 Multiple RTP Media Streams per Call Session

The device's SBC application supports multiple RTP media streams per SBC call session. It supports the negotiation of up to five media streams ('m=' line) in the SDP offer/answer model per session. The media can include a combination of any of the following types:

- Audio, indicated in the SDP as 'm=audio'
- Video, indicated in the SDP as 'm=video'
- Text, indicated in the SDP as 'm=text'
- Fax, indicated in the SDP as 'm=image'
- Binary Floor Control Protocol (BFCP), indicated in the SDP as 'm=application <port> UDP/BFCP'

Therefore, the device supports 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 (e.g., does not support the coder), it relays the SBC dialog transparently.

The device transparently forwards Binary Floor Control Protocol (BFCP) signaling over UDP between IP entities (RFC 4582). BFCP is a signaling protocol used by some third-party conferencing servers to share content (such as video conferencing, presentations or documents) between conference participants (SIP clients supporting BFCP). The SDP offer/answer exchange model is used to establish (negotiate) BFCP streams between clients. The BFCP stream is identified in the SDP as 'm=application <port> UDP/BFCP' and a dedicated UDP port is used for the BFCP streams.

22.5.9 Interworking Miscellaneous Media Handling

This section describes various interworking features relating to media handling.

22.5.9.1 Interworking DTMF Methods

The device supports interworking between various DTMF methods such as RFC 2833, In-Band DTMF's, and SIP INFO (Cisco\Nortel\Korea). By default, the device allows the remote user agents to negotiate (in case of RFC 2833) and passes DTMF without intervention. However, if two user agents (UA) support different DTMF methods, the device can interwork these different DTMF methods at each leg.

This DTMF interworking feature is enabled using IP Profiles (*ini* file parameter `IPProfile`):

- `SBCRFC2833Behavior` - affects the RFC 2833 SDP offer-answer negotiation:
 - [0]: (default) the device does not intervene in the RFC 2833 negotiation.
 - [1]: each outgoing offer-answer includes RFC 2833 in the offered SDP (the device adds RFC 2833 only if the incoming offer does not include RFC 2833).
 - [2]: the device removes RFC 2833 from the incoming offer.
- `SBCAlternativeDTMFMethod` – the device's first priority for DTMF method at each leg is RFC 2833. Therefore, if a specific leg negotiates RFC 2833 successfully, then the chosen DTMF method for this leg is RFC 2833. For legs where RFC 2833 is not negotiated successfully, the device uses the parameter to determine the DTMF method for the leg.

The chosen DTMF method determines (for each leg) which DTMF method is used for sending DTMF's. If the device interworks between different DTMF methods and one of the methods is In-band\RFC 2833, detection and generation of DTMF methods requires DSP allocation.

22.5.9.2 Interworking RTP Redundancy

The device supports interworking of RTP redundancy (according to RFC 2198) between SIP entities. Employing IP Profiles, you can configure RTP redundancy handling per SIP entity:

- Generate RFC 2198 redundant packets (`IpProfile_RTPRedundancyDepth` parameter).
- Determine RTP redundancy support in the RTP redundancy negotiation in SDP offer/answer (`IpProfile_SBCRTPRedundancyBehavior` parameter). If not supported, the device discards RTP redundancy packets (if present) received from or sent to the SIP entity.

For more information, see the above parameters in "Configuring IP Profiles" on page 388.

22.5.9.3 Interworking RTP-RTCP Multiplexing

The device supports interworking of RTP-RTCP multiplexing onto a single, local UDP port (according to RFC 5761) between SIP entities. Employing IP Profiles, you can configure RTP multiplexing per SIP entity, using the `IPProfile_SBCRTCPMux` parameter (see "Configuring IP Profiles" on page 388).

22.5.9.4 Interworking RTCP Attribute in SDP

The device supports interworking the RTCP attribute 'a=rtcp' in the SDP between SIP entities. Employing IP Profiles, you can configure RTCP attribute handling (add, remove or transparent) per SIP entity, using the `IpProfile_SBCSDPHandleRTCPAttribute` parameter (see "Configuring IP Profiles" on page 388).

22.5.9.5 Interworking Crypto Lifetime Field

The device supports interworking the lifetime field in the 'a=crypto' attribute of the SDP, between SIP entities. Employing IP Profiles, you can configure the lifetime field handling (remove or retain) per SIP entity, using the `IpProfile_SBCRemoveCryptoLifetimeInSDP` parameter (see "Configuring IP Profiles" on page 388).

22.5.9.6 Interworking Media Security Protocols

The device supports interworking media security protocols for SRTP, between SIP entities. Employing IP Profiles, you can configure the security protocol (SDES, DTLS or both) per SIP entity, using the `IPProfile_SBCMediaSecurityMethod` parameter (see "Configuring IP Profiles" on page 388). For more information on SDES and DTLS, see "Configuring Media (SRTP) Security" on page 196.

22.5.9.7 Interworking ICE Lite for NAT Traversal

The device supports interworking ICE for NAT traversal, between SIP entities. Employing IP Profiles, you can enable ICE Lite per SIP entity, using the `IPProfile_SBCIceMode` parameter (see "Configuring IP Profiles" on page 388).

22.6 Fax Negotiation and Transcoding

The device can allow fax transmissions to traverse transparently without transcoding or it can handle the fax as follows:

- Allow interoperability between different fax machines, supporting fax transcoding if required.
- Restrict usage of specific fax coders to save bandwidth, enhance performance, or comply with supported coders. These coders include G.711 (A-Law or Mu-Law), VBD (G.711 A-Law or G.711 Mu-Law), and T38.

Fax configuration is done in the Coder Groups table and IP Profiles table. The Coder Groups table defines the supported coders, which is assigned to the IP Profile associated with the SIP entity. The IP Profiles table also defines the negotiation method used between the incoming and outgoing fax legs, using the following fax-related parameters:

- `IPProfile_SBCFaxBehavior`: defines the offer negotiation method - pass fax transparently, negotiate fax according to fax settings in IP Profile, or enforce remote UA to first establish a voice channel before fax negotiation.
- `IPProfile_SBCFaxCodersGroupName`: defines the supported fax coders (from the Coder Groups table).
- `IPProfile_SBCFaxOfferMode`: determines the fax coders sent in the outgoing SDP offer.
- `IPProfile_SBCFaxAnswerMode`: determines the fax coders sent in the outgoing SDP answer.
- `IPProfile_SBCRemoteRenegotiateOnFaxDetection`: You can also configure the device to detect for faxes (CNG tone) immediately after the establishment of a voice channel (i.e., after 200 OK) and within a user-defined interval. If detected, it can then handle the subsequent fax renegotiation by sending re-INVITE messages to both SIP entities (originating and terminating faxes). For more information, see the parameter in "Configuring IP Profiles" on page 388.



Note: The voice-related coder configuration (Allowed and Extension coders) is independent of the fax-related coder configuration, with the exception of the G.711 coder. If the G.711 coder is restricted by the Allowed Audio Coders Groups table, it is not used for fax processing even if it is listed in the Coder Groups table for faxes. However, support for G.711 coders for voice is not dependent upon which fax coders are listed in the Coder Groups table.

22.7 Limiting SBC Call Duration

You can configure the maximum allowed call duration (in minutes) per SBC call. If an established call reaches this user-defined limit, the device terminates the call. The feature ensures that calls are properly terminated, allowing available resources for new calls. The following procedure describes how to configure the feature for all calls (globally). To configure the feature per specific calls, use IP Profiles (IpProfile_SBCMaxCallDuration).

➤ **To configure maximum call duration:**

1. Open the SBC General Settings page (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **SBC General Settings**).
2. In the 'Max Call Duration' field (SBCMaxCallDuration), enter the maximum call duration per SBC call:

Figure 22-5: Configuring Maximum Call Duration

Max Call Duration [min]

3. Click **Apply**.

22.8 SBC Authentication

The device can authenticate SIP servers and SBC users (clients). The different authentication methods are described in the subsequent subsections.

22.8.1 SIP Authentication Server Functionality

The device can function as an Authentication server for authenticating received SIP 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, the device can authenticate the following SIP entities:

- **SIP servers:** This is applicable to Server-type IP Groups. This provides protection from rogue SIP servers, preventing unauthorized usage of device resources and functionality. To authenticate remote servers, the device challenges the server with a user-defined username and password that is shared with the remote server. When the device receives an INVITE request from the remote server, it challenges the server by replying with a SIP 401 Unauthorized response containing the WWW-Authenticate header. The remote server then re-sends the INVITE containing an Authorization header with authentication information based on this username-password combination to confirm its identity. The device uses the username and password to authenticate the message prior to processing it.
- **SIP clients:** These are clients belonging to a User-type IP Group. This support prevents unauthorized usage of the device's resources by rogue SIP clients. 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 challenges the received SIP message only if it is configured as a SIP method (e.g., INVITE) for authorization. This is configured in the IP Groups table, using the 'Authentication Method List' parameter.
2. If the message is received without a SIP Authorization header, the device "challenges" the client by sending a SIP 401 or 407 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 AuthNonceDuration, AuthChallengeMethod and AuthQOP parameters.
 - ◆ If validation fails, the device rejects the message and sends a 403 (Forbidden) response to the client.
 - ◆ If validation succeeds, the device verifies client identification. It checks that the username and password received from the client is the same username and password in the device's User Information table / database (see "SBC User Information for SBC User Database" on page 593). If the client is not successfully authenticated after three attempts, the device sends a SIP 403 (Forbidden) response to the client. If the user is successfully identified, the device accepts the SIP message request.

The device's Authentication server functionality is configured per IP Group, using the 'Authentication Mode' parameter in the IP Groups table (see "Configuring IP Groups" on page 329).

22.8.2 User Authentication based on RADIUS

The device can authenticate SIP clients (users) using a remote RADIUS server. The device supports the RADIUS extension for digest authentication of SIP clients, according to draft-sterman-aaa-sip-01. Based on this standard, the device generates the nonce (in contrast to RFC 5090, where it is done by the RADIUS server).

RADIUS based on draft-sterman-aaa-sip-01 operates as follows:

1. The device receives a SIP request without an Authorization header from the SIP client.
2. The device generates the nonce and sends it to the client in a SIP 407 (Proxy Authentication Required) response.
3. The SIP client sends the SIP request with the Authorization header to the device.
4. The device sends an Access-Request message to the RADIUS server.
5. The RADIUS server verifies the client's credentials and sends an Access-Accept (or Access-Reject) response to the device.
6. The device accepts the SIP client's request (sends a SIP 200 OK or forwards the authenticated request) or rejects it (sends another SIP 407 to the SIP client).

To configure this feature, set the SBCServerAuthMode ini file parameter to 2.

22.9 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.

22.9.1 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. To configure different SIP 3xx handling options for different UAs (i.e., per IP Group), use the IP Profiles table parameter, 'SBC Remote 3xx Mode'.

22.9.1.1 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:

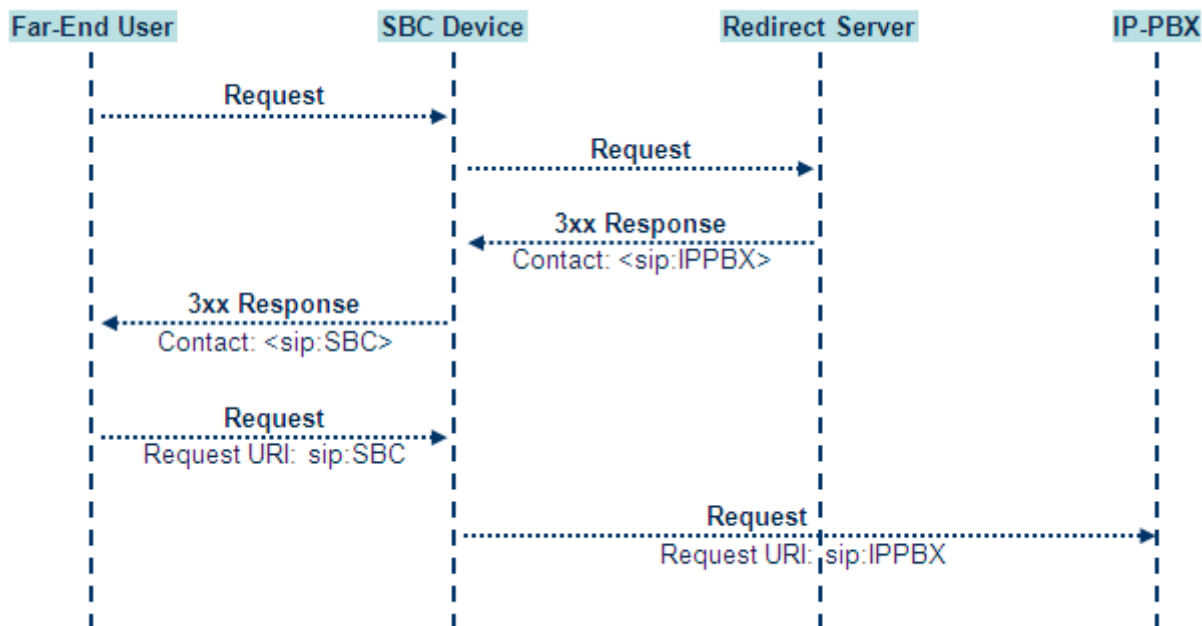
- Changes the host part to the device's IP address – this change causes the remote user agent to send the INVITE to the device.
- Adds a special prefix ("T~&R_") to the Contact user part – to identify the new INVITE as a 3xx resultant INVITE.

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 22-6: 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`).

22.9.1.2 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).

22.9.2 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. If the Diversion header is used, you can specify the URI type (e.g., "tel:") to use in the header, using the SBCDiversionUriType parameter.

This feature is configured in the IP Profiles table (IPProfile parameter) using the following 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 22-1: Handling of SIP Diversion and History-Info Headers

Parameter Value	SIP Header Present in Received SIP Message		
	Diversion	History-Info	Diversion and History-Info
HistoryInfoMode = Add DiversionMode = Remove	Diversion converted to History-Info. Diversion removed.	Not present	Diversion removed.
HistoryInfoMode = Remove DiversionMode = Add	Not present.	History-Info converted to Diversion. History-Info removed.	History-Info added to Diversion. History-Info removed.
HistoryInfoMode = Disable DiversionMode = Add	Diversion converted to History-Info.	Not present.	Diversion added to History-Info.
HistoryInfoMode = Disable DiversionMode = Add	Not present.	History-Info converted to Diversion.	History-Info added to Diversion.
HistoryInfoMode = Add DiversionMode = Add	Diversion converted to History-Info.	History-Info converted to Diversion.	Headers are synced and sent.
HistoryInfoMode = Remove DiversionMode = Remove	Diversion removed.	History-Info removed.	Both removed.

22.9.3 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`. To configure different REFER handling options for different UAs (i.e., IP Groups), use the IP Profiles table parameter, 'Remote REFER Mode'.

- **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 Groups table.

22.9.4 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.

22.9.5 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.

To configure the handling of session expires, use the IP Profile parameter, 'SBC Session Expires Mode'.

22.9.6 Interworking SIP Early Media

The device supports early media. Early media is when the media flow starts before the SIP call is established (i.e., before the 200 OK response). This occurs when the first SDP offer-

answer transaction completes. The offer-answer options can be included in the following SIP messages:

- Offer in first INVITE, answer on 180, and no or same answer in the 200 OK
- Offer in first INVITE, answer on 180, and a different answer in the 200 OK (not standard)
- INVITE without SDP, offer in 180, and answer in PRACK
- PRACK and UPDATE transactions can also be used for initiating subsequent offer-answer transactions before the INVITE 200 OK response.
- In a SIP dialog life time, media characteristics after originally determined by the first offer-answer transaction can be changed by using subsequent offer-answer transactions. These transactions may be carried either in UPDATE or re-INVITE transactions. The media handling is similar to the original offer-answer handling. If the offer is rejected by the remote party, no media changes occur (e.g., INVITE without SDP, then 200 OK and ACK, offer-answer within an offer-answer, and Hold re-INVITE with IP address of 0.0.0.0 - IP address is unchanged).

The device supports various interworking modes for 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 the 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, 'Remote Early Media RTP Detection Mode', 'SBC Remote Supports RFC 3960', and 'SBC Remote Can Play Ringback'. See the flowcharts below for the device's handling of such scenarios:

Figure 22-7: SBC Early Media RTP 18x without SDP

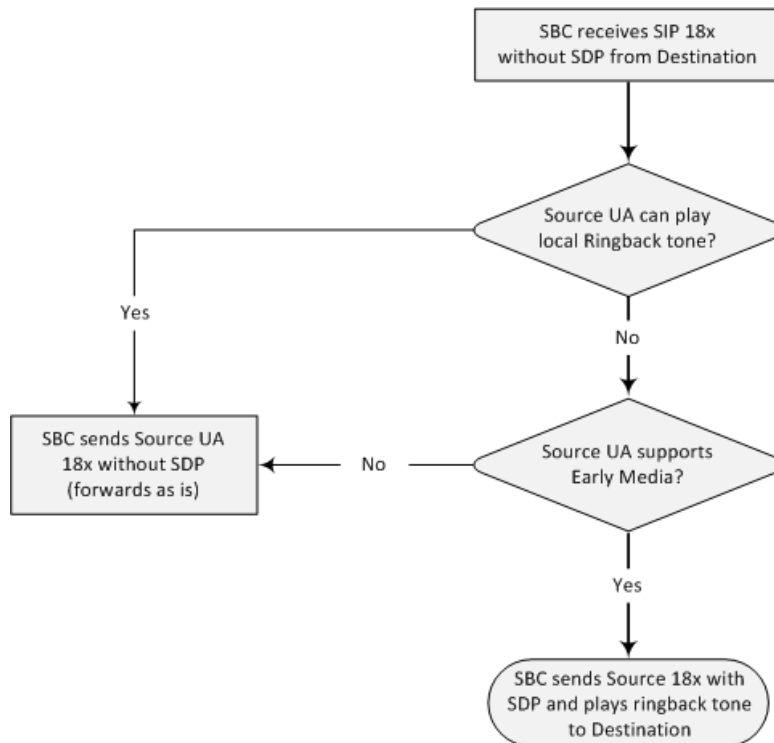
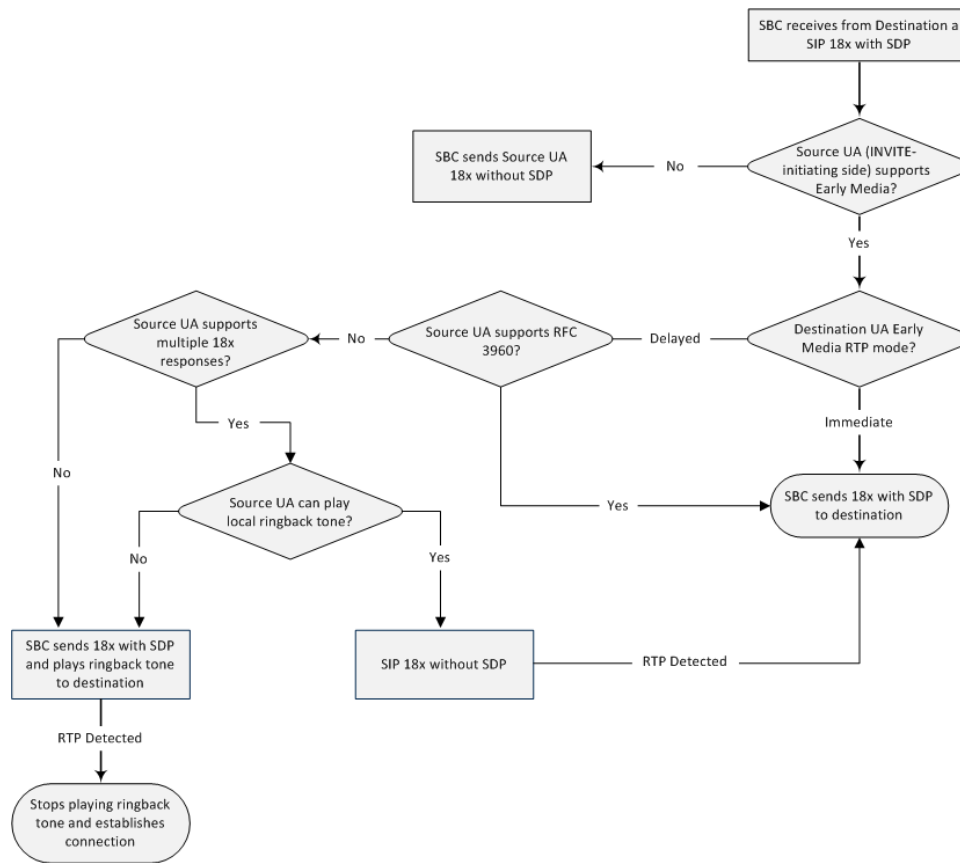


Figure 22-8: Early Media RTP - SIP 18x with SDP



22.9.7 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'.

22.9.8 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'.

22.9.9 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.

22.9.10 Interworking Delayed Offer

The device supports interworking of INVITE messages with and without SDP between SIP entities. 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. This intervention in the SDP offer-answer process may require transcoding. Delayed offer is also supported when early media is present.

Employing IP Profiles, you can configure this interworking feature per SIP entity, using the 'SBC Remote Delayed Offer Support' parameter (see "Configuring IP Profiles" on page 388).



Note: For SIP entities that do not support delayed offer, you must assign extension coders to its IP Profile (using the 'Extension Coders' parameter).

22.9.11 Interworking Call Hold

The device supports the interworking of call hold / retrieve requests between SIP 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'.

To configure IP Profiles, see "Configuring IP Profiles" on page 388.

22.9.12 Interworking SIP Via Headers

The device supports the interworking of SIP Via headers between SIP entities. For the outgoing message sent to a SIP entity, the device can remove or retain all the Via headers received in the incoming SIP request from the other side. Employing IP Profiles, you can

configure this interworking feature per SIP entity, using the `IpProfile_SBCKeepVIAHeaders` parameter (see "Configuring IP Profiles" on page 388).

22.9.13 Interworking SIP User-Agent Headers

The device supports the interworking of SIP User-Agent headers between SIP entities. For the outgoing message sent to a SIP entity, the device can remove or retain all the User-Agent headers received in the incoming SIP request/response from the other side. Employing IP Profiles, you can configure this interworking feature per SIP entity, using the `IpProfile_SBCKeepUserAgentHeader` parameter (see "Configuring IP Profiles" on page 388).

22.9.14 Interworking SIP Record-Route Headers

The device supports the interworking of SIP Record-Route headers between IP entities. For the outgoing message sent to a SIP entity, the device can remove or retain all the Record-Route headers received in the incoming SIP request/response from the other side. Employing IP Profiles, you can configure this interworking feature per SIP entity, using the `IpProfile_SBCKeepRoutingHeaders` parameter (see "Configuring IP Profiles" on page 388).

22.9.15 Interworking SIP To-Header Tags in Multiple SDP Answers

The device supports the interworking of SIP To-header tags in call forking responses (i.e., multiple SDP answers) between IP entities. The device can either use the same To-header tag value for all SDP answers sent to the SIP entity, or send each SDP answer with its original tag. Employing IP Profiles, you can configure this interworking feature per SIP entity, using the `IpProfile_SBCRemoteMultipleEarlyDialogs` parameter (see "Configuring IP Profiles" on page 388).

22.9.16 Interworking In-dialog SIP Contact and Record-Route Headers

The device supports the interworking of in-dialog, SIP Contact and Record-Route headers between SIP entities. Employing IP Profiles, you can configure this interworking feature per SIP entity, using the `IpProfile_SBCRemoteRepresentationMode` parameter (see "Configuring IP Profiles" on page 388).

23 Enabling the SBC Application

Before you can start configuring the SBC, you must first enable the SBC application. Once enabled, the Web interface displays the menus and parameter fields relevant to the SBC application.



Note: The SBC feature is available only if the device is installed with a License Key that includes this feature. For installing a License Key, see "License Key" on page 597.

➤ **To enable the SBC application:**

1. Open the Applications Enabling page (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Applications Enabling**).
2. From the 'SBC Application' drop-down list, select **Enable**:

GENERAL

SBC Application • Enable

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

This page is intentionally left blank.

24 Configuring General SBC Settings

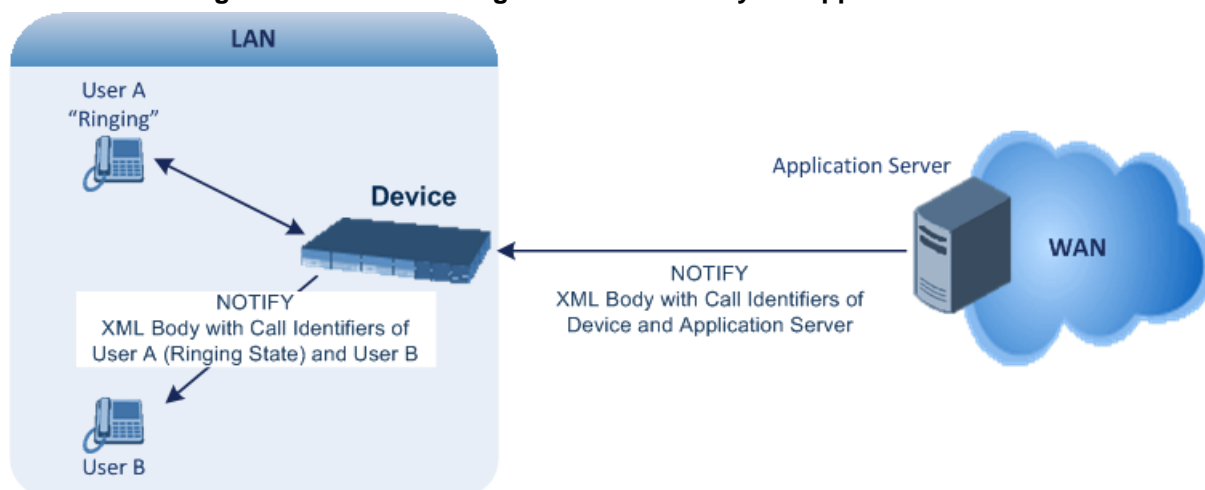
This section describes configuration of various SBC features.

24.1 Interworking Dialog Information in SIP NOTIFY Messages

You can enable the device to interwork dialog information (XML body) received in SIP NOTIFY messages from a remote (WAN) application server. The NOTIFY message is sent by application servers to notify a SIP client, subscribed to a service and located behind the device (LAN), of the status of another SIP client in the LAN. For example, user B can subscribe to an application server for call pick-up service, whereby if user A's phone rings, the application server notifies user B. User B can then press a pre-configured key sequence to answer the call.

The NOTIFY message contains the XML body with call identifiers (call-id and tags). However, as the application server is located in the external network WAN and the SIP clients behind the device, the call dialog information sent by the application server reflects only the dialog between the device and itself; not that of the involved SIP clients. This is due to, for example, the device's topology hiding (e.g., IP address) of its LAN elements. The device resolves this by replacing the call identifiers received from the application server with the correct call identifiers (e.g., user A and user B). Thus, users subscribed to the service can receive relevant NOTIFY messages from the device and use the service.

Figure 24-1: Interworking NOTIFY XML Body for Application Server



➤ **To enable the feature:**

- Configure the 'SBC Dialog-Info Interworking' (EnableSBCDialogInfoInterworking) parameter to **Enable**.

When the feature is disabled, the device forwards the NOTIFY message as is, without modifying its XML body.

Below is an example of an XML body where the call-id, tags, and URIs have been replaced by the device:

```
<?xml version="1.0"?>
<dialog-info xmlns="urn:ietf:params:xml:ns:dialog-info"
version="10" state="partial"
entity="sip:alice@example.com">
<dialog id="zxcvbnm3" call-id="67402270@10.132.10.150"
local-tag="1c137249965"
```

```
remote-tag="CCDORRTDRKIKWVBRWYM" direction="initiator">
<state event="replaced">terminated</state>
</dialog>
<dialog id="sfhjsjk12" call-id="67402270@10.132.10.150"
local-tag="1c137249965"
remote-tag="CCDORRTDRKIKWVBRWYM" direction="receiver">
<state reason="replaced">confirmed</state>
<replaces
call-id="67402270@10.132.10.150"
local-tag="1c137249965"
remote-tag="CCDORRTDRKIKWVBRWYM" />
<referred-by>
sip:bob-is-not-here@vm.example.net
</referred-by>
<local>
<identity display="Jason Forster">
sip:jforsters@home.net
</identity>
<target uri="sip:alice@pc33.example.com">
<param pname="+sip.rendering" pval="yes"/>
</target>
</local>
<remote>
<identity display="Cathy Jones">
sip:cjones@example.net
</identity>
<target uri="sip:line3@host3.example.net">
<param pname="actor" pval="attendant"/>
<param pname="automaton" pval="false"/>
</target>
</remote>
</dialog>
</dialog-info>
```


25 Configuring Admission Control

The Admission Control table lets you configure up to 1,500 Call Admission Control rules (CAC). CAC rules define the maximum number of concurrent calls (SIP dialogs) permitted per IP Group, SIP Interface or SRD, and per user (identified by its registered contact). CAC rules also define a guaranteed (*reserved*) number of concurrent calls. Thus, CAC rules can be useful for implementing Service Level Agreements (SLA) policies.

CAC rules can be applied per SIP request type and SIP dialog direction (inbound and/or outbound). 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 INVITE, REGISTER, and/or SUBSCRIBE messages, 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. Thus, 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.

Reserved capacity is especially useful when the device operates with multiple SIP entities such as in a contact center environment handling multiple customers. For example, if the total call capacity of the device is 200 call sessions, a scenario may arise where one SIP entity may reach the maximum configured call capacity of 200 and thereby, leaving no available call resources for the other SIP entities. Thus, reserved capacity guarantees a minimum capacity for each SIP entity. If the reserved call capacity of a SIP entity is threatened by a new call for a different SIP entity, the device rejects the call to safeguard the reserved capacity.

Reserved call capacity can be configured for an SRD and each of its associated IP Groups, by configuring multiple CAC rules. In such a setup, the SRD's reserved call capacity must be greater or equal to the summation of the reserved call capacity of all these IP Groups. In other words, the SRD serves as the "parent" reserved call capacity. If the SRD's reserved call capacity is greater, the extra call capacity can be used as a shared pool between the IP Groups for unreserved calls when they exceed their reserved capacity. For example, assume that the reserved capacities for an SRD and its associated IP Groups are as follows:

- SRD reserved call capacity: 40
- IP Group ID 1 reserved call capacity: 10
- IP Group ID 2 reserved call capacity: 20

In this setup, the SRD offers a shared pool for unreserved call capacity of 10 [i.e., 40 – (10 + 20)]. If IP Group ID 1 needs to handle 15 calls, it is guaranteed 10 calls and the remaining 5 is provided from the SRD's shared pool. If the SDR's shared pool is currently empty and resources for new calls are required, the quota is taken from the device's total capacity, if available. For example, if IP Group ID 1 needs to handle 21 calls, it's guaranteed 10, the SRD's shared pool provides another 10, and the last call is provided from the device's total call capacity support (e.g., of 200).

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. If no alternative

routing rule exists, the device rejects the SIP request with a SIP 480 "Temporarily Unavailable" response.



Note: The device applies the CAC rule for the incoming leg 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 following procedure describes how to configure CAC rules through the Web interface. You can also configure it through ini file (SBCAdmissionControl) or CLI (configure voip > sbc sbc-admission-control).

➤ **To configure a CAC rule:**

1. Open the Admission Control table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Admission Control**).
2. Click **New**; the following dialog box appears:

Figure 25-1: Admission Control Table - Add Dialog Box

3. Configure an Admission Control rule according to the parameters described in the table below.
4. Click **Apply**.

Table 25-1: Admission Control Table Parameter Description

Parameter	Description
SRD srd-name [SBCAdmissionControl_SRDName]	Assigns an SRD to the rule. By default, no value is defined. For all SRDs, configure the parameter to Any . Note: The parameter is applicable only if 'Limit Type' is configured to SRD .
General	
Index [SBCAdmissionControl_Index]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.

Parameter	Description
Name admission-name [SBCAdmissionControl_AdmissionControlName]	Defines an arbitrary name to easily identify the row. The valid value is a string of up to 20 characters. By default, no value is defined.
Limit Type limit-type [SBCAdmissionControl_LimitType]	Defines the entity to which the rule applies. <ul style="list-style-type: none"> ▪ [0] IP Group (default) ▪ [1] SRD ▪ [2] SIP Interface
IP Group ip-group-name [SBCAdmissionControl_IPGroupName]	Assigns an IP Group to the rule if the rule is applied to an IP Group. By default, no value is defined. For all IP Groups, configure the parameter to Any . Note: The parameter is applicable only if 'Limit Type' is configured to IP Group .
SIP Interface sip-interface-name [SBCAdmissionControl_SIPInterfaceName]	Assigns a SIP Interface to the rule if the rule is applied to a SIP Interface. By default, no value is defined. For all SIP Interfaces, configure the parameter to Any . Note: The parameter is applicable only if 'Limit Type' is configured to SIP Interface .
Request Type 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"> ▪ [0] All = (Default) Includes the total number of all dialogs. ▪ [1] INVITE ▪ [2] SUBSCRIBE ▪ [3] Other = All SIP request types except INVITEs and SUBSCRIBEs (e.g., REGISTER).
Request Direction request-direction [SBCAdmissionControl_RequestDirection]	Defines the call direction of the SIP request to which the rule applies. <ul style="list-style-type: none"> ▪ [0] Both = (Default) Rule applies to inbound and outbound SIP dialogs. ▪ [1] Inbound = Rule applies only to inbound SIP dialogs. ▪ [2] Outbound = Rule applies only to outbound SIP dialogs.
Limit	
Reserved Capacity reservation [SBCAdmissionControl_Reservation]	Defines the guaranteed (minimum) call capacity. The default is 0 (i.e., no reserved capacity). Note: <ul style="list-style-type: none"> ▪ Reserved call capacity is applicable only to IP Groups and SRDs (i.e., 'Limit Type' parameter configured to IP Group or SRD). If you configure the 'Limit Type' parameter to SIP Interface, leave the 'Reserved Capacity' parameter at its default (i.e., 0). ▪ Reserved call capacity is applicable only to INVITE and SUBSCRIBE messages. ▪ Reserved call capacity must be less than the maximum

Parameter	Description
	capacity (limit) configured for the CAC rule (see the 'Limit' parameter below). <ul style="list-style-type: none"> ▪ The total reserved call capacity configured for all CAC rules must be within the device's total call capacity support.
Limit limit [SBCAdmissionControl_Limit]	Defines the maximum number of concurrent SIP dialogs per IP Group, SIP Interface or SRD. You can also use the following special values: <ul style="list-style-type: none"> ▪ [0] 0 = Block all these dialogs. ▪ [-1] -1 = (Default) Unlimited.
Limit Per User limit-per-user [SBCAdmissionControl_LimitPer User]	Defines the maximum number of concurrent SIP dialogs per user belonging to the specified IP Group, SIP Interface or SRD. You can also use the following special values: <ul style="list-style-type: none"> ▪ [-1] -1 = (Default) Unlimited. ▪ [0] 0 = Block all these dialogs.
Rate rate [SBCAdmissionControl_Rate]	Defines the rate (in seconds) at which tokens are added to the token bucket per second (i.e., token rate). The default is 0 (i.e., unlimited rate). Note: <ul style="list-style-type: none"> ▪ You must first configure the 'Maximum Burst' parameter (see below) before configuring the 'Rate' parameter. ▪ The token bucket feature is per IP Group, SIP Interface, SRD, SIP request type, and SIP request direction.
Maximum Burst max-burst [SBCAdmissionControl_MaxBurst]	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, 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 configured in the 'Rate' field), the device accepts the first 100 SIP dialogs and rejects the last one. The device sends a SIP 480 "Temporarily Unavailable" response when it rejects requests. Dropped requests are not counted in the bucket. The default is 0 (i.e., unlimited SIP dialogs). Note: The token bucket feature is per IP Group, SIP Interface, SRD, SIP request type, and SIP request direction.

26 Routing SBC

This section describes the configuration of the call routing entities for the SBC application.

26.1 Configuring Classification Rules

The Classification table lets you configure up to 1,500 Classification rules. A Classification rule classifies incoming SIP dialog-initiating requests (e.g., INVITE messages) to a "source" IP Group. The source IP Group is the SIP entity that sent the SIP dialog request. Once classified, the device uses the IP Group to process the call (manipulation and routing).

You can also use the Classification table for employing SIP-level access control for successfully classified calls, by configuring Classification rules with whitelist and blacklist settings. If a Classification rule is configured as a whitelist ("Allow"), the device accepts the SIP dialog and processes the call. If the Classification rule is configured as a blacklist ("Deny"), the device rejects the SIP dialog.

Configuration of Classification rules includes two areas:

- **Match:** Defines the matching characteristics of the incoming IP call (e.g, source SIP Interface and IP address). Classification is primarily based on the SIP Interface (as the matching characteristics) on which the incoming dialog is received. As Classification rules must first be assigned with an SRD, the SIP Interface is one that belongs to the SRD. Therefore, Classification rules are configured per SRD, where multiple SIP Interfaces can be used as matching characteristics. However, as multiple SRDs are relevant only for multi-tenant deployments, for most deployments only a single SRD is required. As the device provides a default SRD ("Default_SRD"), when only one SRD is required, the device automatically assigns it to the Classification rule.
- **Action:** Defines the action that is done if the incoming call matches the characteristics of the rule (i.e., classifies the call to the specified IP Group).

The device searches the table from **top to bottom** for the **first** rule that matches the characteristics of the incoming call. If it finds a matching rule, it classifies the call to the IP Group configured for that rule.



Note: Configure stricter classification rules higher up in the table than less strict rules to ensure incoming dialogs are classified to the desired IP Group. *Strict* refers to the number of matching characteristics configured for the rule. For example, a rule configured with source host name and destination host name as matching characteristics is stricter than a rule configured with only source host name. If the rule configured with only source host name appears higher up in the table, the device ("erroneously") uses the rule to classify incoming dialogs matching this source host name (even if they also match the rule appearing lower down in the table configured with the destination host name as well).

If the device doesn't find a matching rule (i.e., classification fails), the device rejects or allows the call depending on the following configuration:

- **To configure the action for unclassified calls:**
- 1. Open the SBC General Settings (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **SBC General Settings**).

- From the 'Unclassified Calls' drop-down list, select **Reject** to reject unclassified calls or **Allow** to accept unclassified calls:

Figure 26-1: Configuring Action for Classification Failure



- Click **Apply**.

If you configure the parameter to **Allow**, the incoming SIP dialog is assigned to an IP Group as follows:

- The device determines on which SIP listening port (e.g., 5061) the incoming SIP dialog request was received and the SIP Interface configured with this port (in the SIP Interfaces table).
- The device determines the SRD associated with this SIP Interface (in the SIP Interfaces table) and then classifies the SIP dialog to the first IP Group in the IP Groups table that is associated with the SRD. For example, if IP Groups 3 and 4 belong to the same SRD, the device classifies the call to IP Group 3.



Note: If classification of a SIP request fails and you configure the device to reject unclassified calls, the device can send a specific SIP response code per SIP Interface. To configure this, use the 'Classification Failure Response Type' parameter in the SIP Interfaces table (see "Configuring SIP Interfaces" on page 321).

The Classification table is used to classify incoming SIP dialog requests **only if** the following classification stages fail:

- Classification Stage 1 - Based on User Registration Database:** The device searches its users registration database to check whether the incoming SIP dialog arrived from a registered user. The device searches the database for a user that matches the address-of-record (AOR) and Contact of the incoming SIP message:
 - Compares the SIP Contact header to the contact value in the database.
 - Compares the URL in the SIP P-Asserted-Identity/From header to the registered AOR in the database.

If the device finds a matching registered user, it classifies the user to the IP Group associated with the user in the database. If this classification stage fails, the device proceeds to classification based on Proxy Set.

- Classification Stage 2 - Based on Proxy Set:** If the database search fails, the device performs classification based on Proxy Set. This classification is applicable only to Server-type IP Groups and is done only if classification based on Proxy Set is enabled (see the 'Classify By Proxy Set' parameter in the IP Groups table in "Configuring IP Groups" on page 329). The device checks whether the incoming INVITE's IP address (if host name, then according to the dynamically resolved IP address list) is configured for a Proxy Set (in the Proxy Sets table). If such a Proxy Set exists, the device classifies the INVITE to the IP Group that is associated with the Proxy Set. The Proxy Set is assigned to the IP Group in the IP Groups table.

If more than one Proxy Set is configured with the same IP address and associated with the same SIP Interface, the device may classify and route the SIP dialog to an incorrect IP Group. In such a scenario, a warning is generated in the Syslog message. However, if some Proxy Sets are configured with the same IP address but different ports (e.g., 10.1.1.1:5060 and 10.1.1.1:5070) and the 'Classification Input' parameter is configured to **IP Address, Port & Transport Type**, classification (based on IP address and port combination) to the correct IP Group is achieved. Therefore, when classification is by Proxy Set, pay attention to the configured IP addresses and the 'Classification Input' parameter of your Proxy Sets. When more than one Proxy Set is configured with the same IP address, the device selects the matching Proxy Set in the following precedence order:

- a. Selects the Proxy Set whose IP address, port, and transport type match the source of the incoming dialog.
- b. If no match is found for a), it selects the Proxy Set whose IP address and transport type match the source of the incoming dialog (if the 'Classification Input' parameter is configured to **IP Address Only**).
- c. If no match is found for b), it selects the Proxy Set whose IP address match the source of the incoming dialog (if the 'Classification Input' parameter is configured to **IP Address Only**).

If classification based on Proxy Set fails (or classification based on Proxy Set is disabled), the device proceeds to classification based on the Classification table.

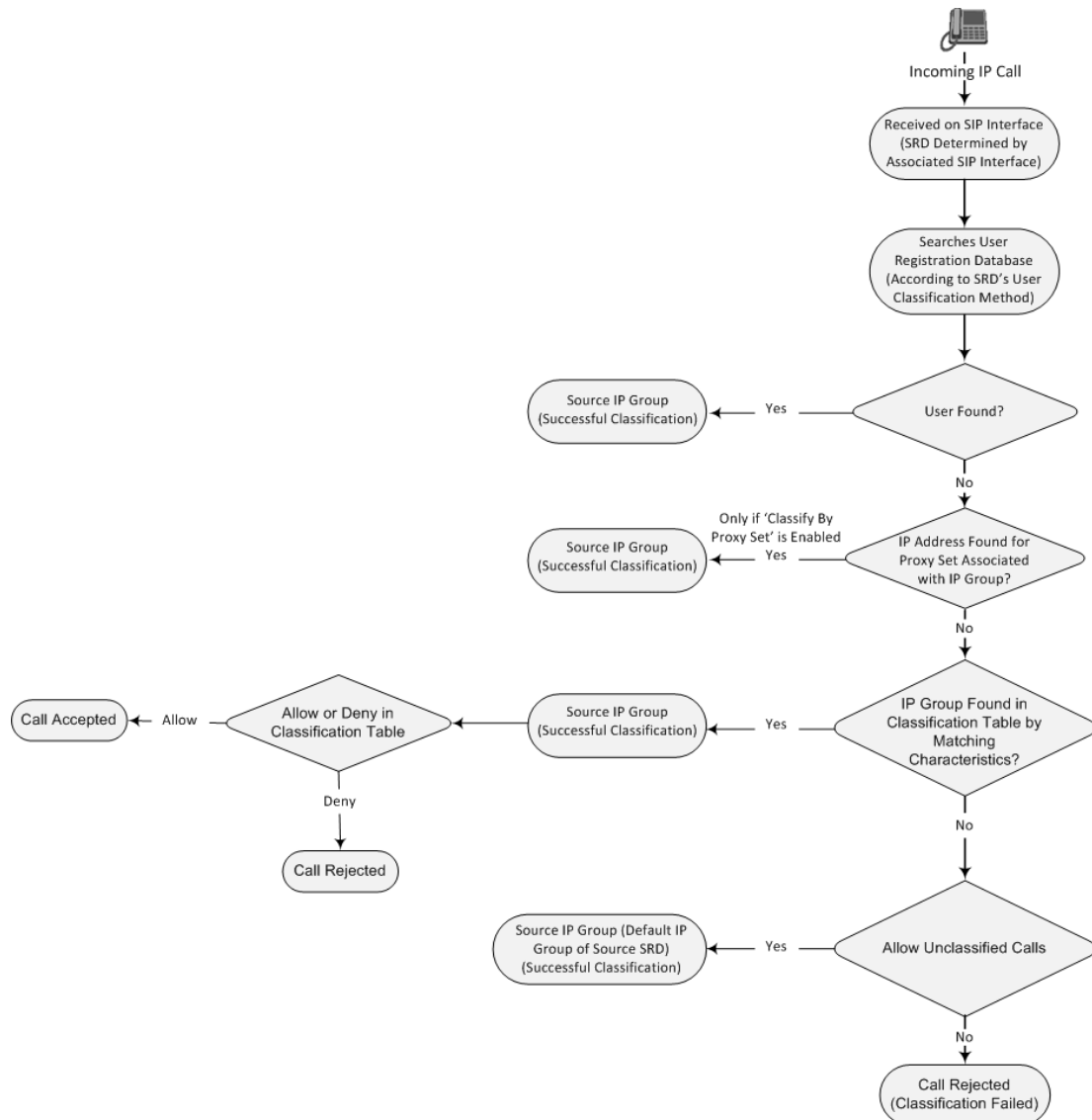


Note:

- For security, it is recommended to classify SIP dialogs based on Proxy Set only if the IP address of the Server-type IP Group is **unknown**. In other words, if the Proxy Set associated with the IP Group is configured with an FQDN. In such cases, the device classifies incoming SIP dialogs to the IP Group based on the DNS-resolved IP address. If the IP address is known, it is recommended to use a Classification rule instead (and disable the Classify by Proxy Set feature), where the rule is configured with not only the **IP address, but also with SIP message characteristics** to increase the strictness of the classification process. The reason for preferring classification based on Proxy Set when the IP address is unknown is that IP address forgery (commonly known as IP spoofing) is more difficult than malicious SIP message tampering and therefore, using a Classification rule without an IP address offers a weaker form of security. When classification is based on Proxy Set, the Classification table for the specific IP Group is ignored.
- If multiple IP Groups are associated with the same Proxy Set, use Classification rules to classify the incoming dialogs to the IP Groups (do **not** use the Classify by Proxy Set feature).
- The device saves incoming SIP REGISTER messages in its registration database. If the REGISTER message is received from a User-type IP Group, the device sends the message to the configured destination.

The flowchart below illustrates the classification process:

Figure 26-2: Classification Process (Identifying IP Group or Rejecting Call)



The following procedure describes how to configure Classification rules through the Web interface. You can also configure it through ini file (Classification) or CLI (configure voip > sbc classification).

➤ **To configure a Classification rule:**

1. Open the Classification table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Classification Table**).

- Click **New**; the following dialog box appears:

Figure 26-3: Classification Table - Add Dialog Box

The screenshot shows a dialog box titled "Classification" with a window control bar (minimize, maximize, close). At the top, there is a dropdown menu for "SRD" with the value "#0 [DefaultSRD]". Below this are two main sections: "MATCH" and "ACTION".

MATCH Section:

- Index: 0
- Name: (empty)
- Source SIP Interface: Any (dropdown) with a "View" link
- Source IP Address: (empty)
- Source Transport Type: Any (dropdown)
- Source Port: 0
- Source Username Prefix: *
- Source Host: *
- Destination Username Prefix: *
- Destination Host: *
- Message Condition: -- (dropdown) with a "View" link

ACTION Section:

- Action Type: Allow (dropdown)
- Destination Routing Policy: -- (dropdown) with a "View" link
- Source IP Group: -- (dropdown) with a "View" link
- IP Profile: -- (dropdown) with a "View" link

- Configure the Classification rule according to the parameters described in the table below.
- Click **Apply**.

Table 26-1: Classification Table Parameter Descriptions

Parameter	Description
SRD srd-name [Classification_SRDName]	Assigns an SRD to the rule as a matching characteristic for the incoming SIP dialog. If only one SRD is configured in the SRDs table, the SRD is assigned to the rule by default. If multiple SRDs are configured in the SRDs table, no value is assigned. To configure SRDs, see "Configuring SRDs" on page 311. Note: The parameter is mandatory.
Match	
Index [Classification_Index]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
Name classification-name [Classification_ClassificationName]	Defines an arbitrary name to easily identify the row. The valid value is a string of up to 20 characters. By default, no name is defined. Note: Each row must be configured with a unique name.
Source SIP Interface src-sip-interface-name [Classification_SrcSIPInterfaceName]	Assigns a SIP Interface to the rule as a matching characteristic for the incoming SIP dialog. The default is Any (i.e., all SIP Interfaces belonging to the SRD assigned to the rule). Note: The SIP Interface must belong to the SRD assigned to the

Parameter	Description
	rule (see the 'SRD' parameter in the table).
Source IP Address src-ip-address [Classification_SrcAddress]	Defines a source IP address as a matching characteristic for the incoming SIP dialog. The valid value is an IP address in dotted-decimal notation. In addition, the following wildcards can be used: <ul style="list-style-type: none"> ▪ "x" wildcard: represents single digits. For example, 10.8.8.xx represents all addresses between 10.8.8.10 and 10.8.8.99. ▪ Asterisk (*) wildcard: represents any number between 0 and 255. For example, 10.8.8.* represents all addresses between 10.8.8.0 and 10.8.8.255. By default, no value is defined (i.e., any source IP address is accepted). Note: <ul style="list-style-type: none"> ▪ The parameter is applicable only to Server-type IP Groups. ▪ If the IP address is unknown (i.e., configured for the associated Proxy Set as an FQDN), it is recommended to classify incoming dialogs based on Proxy Set (instead of using a Classification rule). For more information on classification by Proxy Set or by Classification rule, see the note bulletin in the beginning of this section.
Source Transport Type src-transport-type [Classification_SrcTransportType]	Defines the source transport type as a matching characteristic for the incoming SIP dialog. <ul style="list-style-type: none"> ▪ [-1] Any = (Default) All transport types ▪ [0] UDP ▪ [1] TCP ▪ [2] TLS
Source Port src-port [Classification_SrcPort]	Defines the source port number as a matching characteristic for the incoming SIP dialog. By default, no value is defined.
Source Username Prefix src-user-name-prefix [Classification_SrcUsernamePrefix]	Defines the prefix of the source URI user part as a matching characteristic for 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, in the IP Groups table ('Source URI Input' parameter). For more information on how the device obtains the URI, see "SIP Dialog Initiation Process" on page 425. The default is the asterisk (*) symbol, which represents any source username prefix. 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 729. Note: For REGISTER requests, the source URI is obtained from the To header.
Source Host src-host [Classification_SrcHost]	Defines the prefix of the source URI host name as a matching characteristic for 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, in the IP Groups table ('Source URI Input' parameter). For more information on how the device obtains this URI, see "Call Processing of SIP Dialog Requests" on page 425.

Parameter	Description
	The default is the asterisk (*) symbol, which represents any source host prefix. Note: For REGISTER requests, the source URI is obtained from the To header.
Destination Username Prefix dst-user-name-prefix [Classification_DestUsernamePrefix]	Defines the prefix of the destination Request-URI user part as a matching characteristic for the incoming SIP dialog. The default is the asterisk (*) symbol, which represents any destination username. 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 729.
Destination Host dst-host [Classification_DestHost]	Defines the prefix of the destination Request-URI host name as a matching characteristic for the incoming SIP dialog. The default is the asterisk (*) symbol, which represents any destination host prefix.
Message Condition message-condition-name [Classification_MessageConditionName]	Assigns a Message Condition rule to the Classification rule as a matching characteristic for the incoming SIP dialog. By default, no value is defined. To configure Message Condition rules, see "Configuring Message Condition Rules" on page 469.
Action	
Action Type action-type [Classification_ActionType]	Defines a whitelist or blacklist for the matched incoming SIP dialog. <ul style="list-style-type: none"> ▪ [0] Deny = Blocks incoming SIP dialogs that match the characteristics of the rule (blacklist). ▪ [1] Allow = (Default) Allows incoming SIP dialogs that match the characteristics of the rule (whitelist) and assigns it to the associated IP Group.
Destination Routing Policy dest-routing-policy [Classification_DestRoutingPolicy]	Assigns a Routing Policy to the matched incoming SIP dialog. The assigned Routing Policy overrides the Routing Policy assigned to the SRD (in the SRDs table). The option to assign Routing Policies to Classification rules is useful in deployments requiring different routing and manipulation rules for specific calls pertaining to the same SRD. In such scenarios, you need to configure multiple Classification rules for the same SRD, where for some rules no Routing Policy is assigned (i.e., the SRD's assigned Routing Policy is used) while for others a different Routing Policy is specified to override the SRD's assigned Routing Policy. By default, no value is defined. To configure Routing Policies, see "Configuring SBC Routing Policy Rules" on page 484.
Source IP Group src-ip-group-name [Classification_SrcIPGroupName]	Assigns an IP Group to the matched incoming SIP dialog. By default, no value is defined. To configure IP Groups, see "Configuring IP Groups" on page 329. Note: The IP Group must be associated with the assigned SRD (see the 'SRD' parameter in the table).
IP Profile ip-profile-id	Assigns an IP Profile to the matched incoming SIP dialog. The assigned IP Profile overrides the IP Profile assigned to the IP Group (in the IP Groups table) to which the SIP dialog is classified.

Parameter	Description
[Classification_IpProfileName]	<p>Therefore, assigning an IP Profile during classification allows you to assign different IP Profiles to specific users (calls) that belong to the same IP Group (User or Server type).</p> <p>For example, you can configure two Classification rules to classify incoming calls to the same IP Group. However, one Classification rule is a regular rule that doesn't specify any IP Profile (IP Profile assigned to IP Group is used), while the second rule is configured with an additional matching characteristic for the source hostname prefix (e.g., "abcd.com") and with an additional action that assigns a different IP Profile.</p> <p>By default, no value is defined.</p> <p>Note: For User-type IP Groups, if a user is already registered with the device (from a previous, initial classification process), the device classifies subsequent INVITE requests from the user according to the device's users database instead of the Classification table. In such a scenario, the same IP Profile that was previously assigned to the user by the Classification table is also used (in other words, the device's users database stores the associated IP Profile).</p>

26.1.1 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. The 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=z9hG4bKVEBTDHAHSUYRTEXEDEGJY
From: <sip:100@10.33.4.226>;tag=YSQQKXXREVDPYPTNFMWG
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-Called-Party-ID: <sip:1111@10.33.38.1>
User-Agent: Sip Message Generator V1.0.0.5
Content-Length: 0
```

1. In the Classification table, add the following classification rules:

Index	Source Username Prefix	Destination Username Prefix	Destination Host	Source IP Group
0	333	-	-	1
1	1111	2000	10.10.10.10	2

2. In the IP Groups table, add the following IP Groups:

Index	Source URI Input	Destination URI Input
1	-	-

Index	Source URI Input	Destination URI Input
2	P-Called-Party-ID	Route

In the 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 2.

26.2 Configuring Message Condition Rules

The Message Conditions table lets you configure up to 1,200 Message Condition rules. A Message Condition defines special conditions (requisites) for incoming SIP messages. These rules can be used as additional matching criteria for the following:

- Classification rules in the Classification table (see "Configuring Classification Rules" on page 461)
- IP-to-IP routing rules in the IP-to-IP Routing table (see "Configuring SBC IP-to-IP Routing Rules" on page 470)
- Outbound Manipulation rules in the Outbound Manipulations table (see "Configuring IP-to-IP Outbound Manipulations" on page 497)

Message Condition rules are configured using the same syntax as that used for Conditions when configuring Message Manipulation rules in the Message Manipulations table (see "Configuring SIP Message Manipulation" on page 362). You can configure simple Message Condition rules, for example, "header.to.host contains company", meaning SIP messages whose To header has a host part containing the string "company". You can configure complex rules using the "AND" or "OR" Boolean operands and 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.



Note: For a description on SIP message manipulation syntax, refer to the *SIP Message Manipulations Quick Reference Guide*.

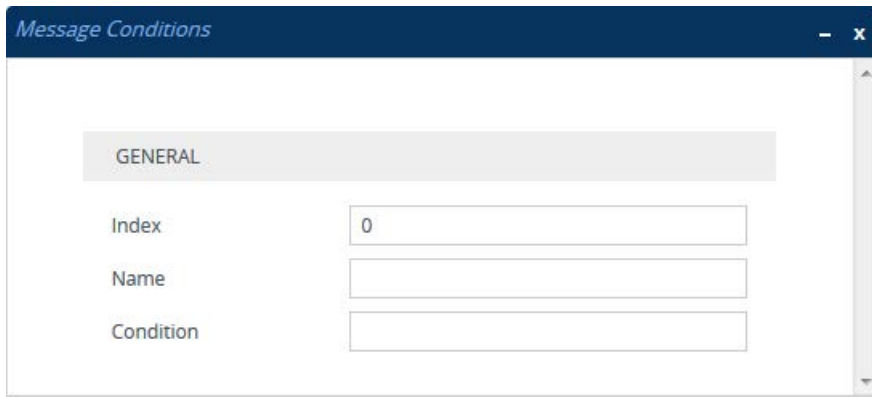
The following procedure describes how to configure Message Condition rules through the Web interface. You can also configure it through ini file (ConditionTable) or CLI (configure voip > sbc routing condition-table).

➤ To configure a Message Condition rule:

1. Open the Message Conditions table (**Setup** menu > **Signaling & Media** tab > **Message Manipulation** folder > **Message Conditions**).

- Click **New**; the following dialog box appears:

Figure 26-4: Message Conditions Table - Add Dialog Box



- Configure a Message Condition rule according to the parameters described in the table below.
- Click **Apply**.

An example of configured Message Condition rules is shown in the figure below:

Figure 26-5: Example of Configured SIP Message Conditions

INDEX ↕	NAME	CONDITION
0	IP Group user	param.ipg.src.type==user
1	Contains SIP Via Header	header.via.exists
2	"101" user part in From header	header.from.url.user=="101"

- **Index 0:** Incoming SIP dialog that is classified as belonging to a User-type IP Group.
- **Index 1:** Incoming SIP dialog that contains a SIP Via header.
- **Index 2:** Incoming SIP dialog with "101" as the user part in the SIP From header.

Table 26-2: Message Conditions Table Parameter Descriptions

Parameter	Description
Index [ConditionTable_Index]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
Name name [ConditionTable_Name]	Defines a brief description of the Condition rule. The valid value is a string of up to 59 characters.
Condition condition [ConditionTable_Condition]	Defines the Condition rule of the SIP message. The valid value is a string. Note: User and host parts must be enclosed in single quotes.

26.3 Configuring SBC IP-to-IP Routing

The IP-to-IP Routing table lets you configure up to 9,000 SBC IP-to-IP routing rules. Configuration of IP-to-IP routing rules includes two areas:

- **Match:** Defines the characteristics of the incoming SIP dialog message (e.g., IP Group from which the message is received).
- **Action:** Defines the action that is done if the incoming call matches the characteristics of the rule (i.e., routes the call to the specified destination).

The device searches the table from **top to bottom** for the **first** rule that matches the characteristics of the incoming call. If it finds a matching rule, it sends the call to the destination configured for that rule. If it doesn't find a matching rule, it rejects the call.

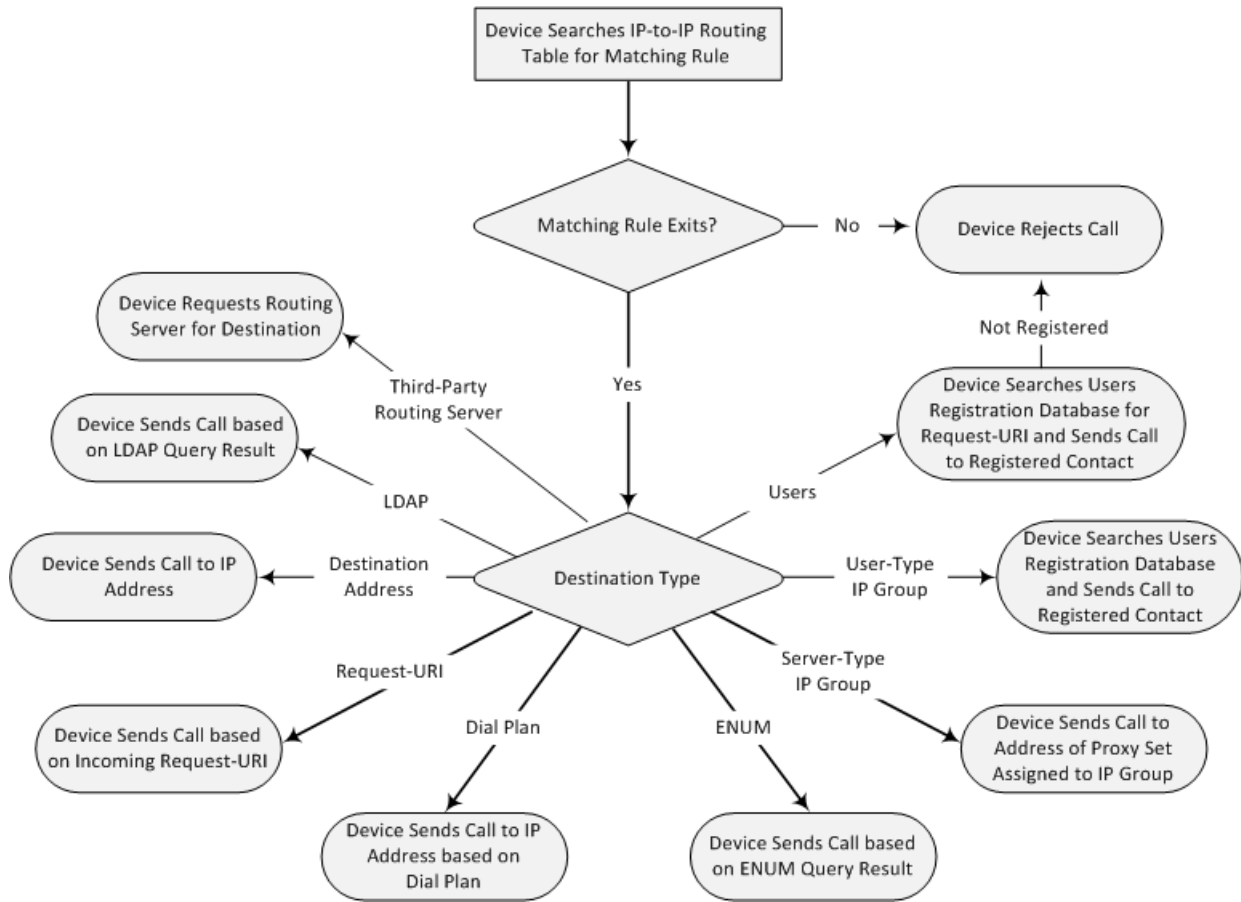


Note: Configure stricter rules higher up in the table than less strict rules to ensure the desired rule is used to route the call. *Strict* refers to the number of matching characteristics configured for the rule. For example, a rule configured with source host name and source IP Group as matching characteristics is stricter than a rule configured with only source host name. If the rule configured with only source host name appears higher up in the table, the device ("erroneously") uses the rule to route calls matching this source host name (even if they also match the rule appearing lower down in the table configured with the source IP Group as well).

You can route incoming SIP dialog messages (e.g., INVITE) to any of the following IP destinations:

- According to registered user Contact listed in the device's registration database (only for User-type IP Groups).
- IP Group - the destination is the address configured for the Proxy Set associated with the IP Group.
- IP address in dotted-decimal notation or FQDN. Routing to a host name can be resolved using NAPTR/SRV/A-Record.
- Request-URI of incoming SIP dialog-initiating requests.
- Any registered user in the registration database. If the Request-URI of the incoming INVITE exists in the database, the call is sent to the corresponding contact address specified in the database.
- According to result of an ENUM query.
- Hunt Group - used for call survivability of call centers (see "Configuring Call Survivability for Call Centers" on page 535).
- According to result of LDAP query (for more information on LDAP-based routing, see "Routing Based on LDAP Active Directory Queries" on page 226).
- Third-party routing server, which determines the destination (next hop) of the call (IP Group). The IP Group represents the next device in the routing path to the final destination. For more information, see "Centralized Third-Party Routing Server" on page 266.

Figure 26-6: IP-to-IP Routing Destination Types



To configure and apply an IP-to-IP Routing rule, the rule must be associated with a Routing Policy. The Routing Policy associates the routing rule with an SRD(s). Therefore, the Routing Policy lets you configure routing rules for calls belonging to specific SRD(s). However, as multiple Routing Policies are relevant only for multi-tenant deployments (if needed), for most deployments, only a single Routing Policy is required. As the device provides a default Routing Policy ("Default_SBCRoutingPolicy"), when only one Routing Policy is required, the device automatically assigns the default Routing Policy to the routing rule. If you are implementing LDAP-based routing (with or without Call Setup Rules) and/or Least Cost Routing (LCR), you need to configure these settings for the Routing Policy (regardless of the number of Routing Policies employed). For more information on Routing Policies, see "Configuring SBC Routing Policy Rules" on page 484.

The IP-to-IP Routing table also provides the following features:

- **Alternative Routing:** 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 Alternative Routing Reasons table (see "Configuring SIP Response Codes for Alternative Routing Reasons" on page 482).
 - ◆ 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 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).
- **Load Balancing:** You can implement load balancing of calls, belonging to the same source, between a set of destination IP Groups known as an **IP Group Set**. The IP Group Set can include up to five IP Groups (Server-type and/or Gateway-type only) and the chosen IP Group depends on the configured load-balancing policy (e.g., Round Robin). To configure the feature, you need to first configure an IP Group Set (see Configuring IP Group Sets on page 487), and then assign it to a routing rule with 'Destination Type' configured to **IP Group Set**.
- **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. To configure Cost Groups, see "Least Cost Routing" on page 254. 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 that are assigned Cost Groups, according to the default LCR settings configured for the assigned Routing Policy (see "Configuring SBC Routing Policy Rules" on page 484).
- **Call Forking:** The IP-to-IP Routing table can be configured to route an incoming IP call to multiple destinations (call forking). The incoming call can be routed to multiple destinations of any type such as an IP Group or IP address. The device forks the call by sending simultaneous INVITE messages to all the specified destinations. It handles the multiple SIP dialogs until one of the calls is answered and then terminates the other SIP dialogs.

Call forking is configured by creating a Forking group. A Forking group consists of a main routing rule ('Alternative Route Options' set to **Route Row**) whose 'Group Policy' is set to **Forking**, and one or more associated routing rules ('Alternative Route Options' set to **Group Member Ignore Inputs** or **Group Member Consider Inputs**). The group members must be configured in contiguous table rows to the main routing rule. If an incoming call matches the input characteristics of the main routing rule, the device routes the call to its destination and all those of the group members.

An alternative routing rule can also be configured for the Forking group. The alternative route is used if the call fails for the Forking group (i.e., main route and all its group members). The alternative routing rule must be configured in the table row immediately below the last member of the Forking group. The 'Alternative Route Options' of this alternative route must be set to **Alt Route Ignore Inputs** or **Alt Route Consider Inputs**. The alternative route can also be configured with its own forking group members, where if the device uses the alternative route, the call is also sent to its group members. In this case, instead of setting the alternative route's 'Group Policy' to **None**, you must set it to **Forking**. The group members of the alternative route must be configured in the rows immediately below it.

The LCR feature can also be employed with call forking. The device calculates a maximum call cost for each Forking group and routes the call to the Forking group with the lowest cost. Thus, even if the call can successfully be routed to the main routing rule, a different routing rule can be chosen (even an alternative route, if configured) based on LCR. If routing to one Forking group fails, the device tries to route the call to the Forking group with the next lowest cost (main or alternative route), and so on. The prerequisite for this functionality is that the incoming call must successfully match the input characteristics of the main routing rule.

- Dial Plan Tags for Representing Source / Destination Numbers:** If your deployment includes calls of many different called (source URI user name) and/or calling (destination URI user name) numbers that need to be routed to the same destination, you can employ user-defined tags to represent these numbers. Thus, instead of configuring many routing rules, you can configure only one routing rule using the tag as the source and destination number matching characteristics, and a destination for the calls. For more information on tags, see "Configuring Dial Plans" on page 503.



Note: Call forking is not applicable to LDAP-based IP-to-IP routing rules.

The following procedure describes how to configure IP-to-IP routing rules through the Web interface. You can also configure it through ini file (IP2IPRouting) or CLI (configure voip > sbc routing ip2ip-routing).

➤ **To configure an IP-to-IP routing rule:**

- Open the IP-to-IP Routing table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **IP-to-IP Routing**).
- Click **New**; the following dialog box appears:

Figure 26-7: IP-to-IP Routing Table - Add Dialog Box

- Configure an IP-to-IP routing rule according to the parameters described in the table below.
- Click **Apply**.

Table 26-3: IP-to-IP Routing Table Parameter Descriptions

Parameter	Description
Routing Policy	Assigns a Routing Policy to the rule. The Routing Policy associates the rule with an SRD(s). The Routing Policy also

Parameter	Description
sbc-routing-policy-name [IP2IPRouting_RoutingPolicyName]	defines default LCR settings as well as the LDAP servers used if the routing rule is based on LDAP routing (and Call Setup Rules). If only one Routing Policy is configured in the Routing Policies table, the Routing Policy is automatically assigned. If multiple Routing Policies are configured, no value is assigned. To configure Routing Policies, see "Configuring SBC Routing Policy Rules" on page 484. Note: The parameter is mandatory.
General	
Index [IP2IPRouting_Index]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
Name route-name [IP2IPRouting_RouteName]	Defines an arbitrary name to easily identify the row. The valid value is a string of up to 20 characters. By default, no value is defined.
Alternative Route Options alt-route-options [IP2IPRouting_AltRouteOptions]	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). <ul style="list-style-type: none"> ▪ [0] 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. ▪ [1] Alternative 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. ▪ [2] Alternative 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. ▪ [3] Group Member Ignore Inputs = This routing rule is a member of the Forking routing rule. The incoming call is also forked to the destination of this routing rule. The matching input characteristics of the routing rule are ignored. ▪ [4] Group Member Consider Inputs = This routing rule is a member of the Forking routing rule. The incoming call is also forked to the destination of this routing rule only if the incoming call matches this rule's input characteristics. Note: <ul style="list-style-type: none"> ▪ The alternative routing entry ([1] or [2]) 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. ▪ The Forking Group members must be configured in a table row that is immediately below the main Forking routing rule, or below an alternative routing rule for the main rule, if configured. ▪ For IP-to-IP alternative routing, configure alternative routing reasons upon receipt of 4xx, 5xx, and 6xx SIP responses (see "Configuring SIP Response Codes for Alternative

Parameter	Description
	Routing Reasons" on page 482). 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 Alternative Routing Reasons table. <ul style="list-style-type: none"> ▪ 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).
Match	
Source IP Group src-ip-group-name [IP2IPRouting_SrcIPGroupName]	Defines the IP Group from where the IP call is received (i.e., the IP Group that sent the SIP dialog). Typically, the IP Group of an incoming SIP dialog is determined (or classified) using the Classification table (see "Configuring Classification Rules" on page 461). The default is Any (i.e., any IP Group). Note: The selectable IP Group for the parameter depends on the assigned Routing Policy (in the 'Routing Policy' parameter in this table). For more information, see "Configuring SBC Routing Policy Rules" on page 484.
Request Type request-type [IP2IPRouting_RequestType]	Defines the SIP dialog request type (SIP Method) of the incoming SIP dialog. <ul style="list-style-type: none"> ▪ [0] All (default) ▪ [1] INVITE ▪ [2] REGISTER ▪ [3] SUBSCRIBE ▪ [4] INVITE and REGISTER ▪ [5] INVITE and SUBSCRIBE ▪ [6] OPTIONS
Source Username Prefix src-user-name-prefix [IP2IPRouting_SrcUsernamePrefix]	Defines the prefix of the user part of the incoming SIP dialog's source URI (usually the From URI). You can use special notations for denoting the prefix. To denote calls without a user part in the URI, use the \$ sign. For available notations, see "Dialing Plan Notation for Routing and Manipulation" on page 729. The default is the asterisk (*) symbol (i.e., any prefix). If this rule is not required, leave this field empty. Note: If you need to route calls of many different source URI user names to the same destination, you can use tags (see 'Source Tags' parameter below) instead of this parameter.
Source Host src-host [IP2IPRouting_SrcHost]	Defines the host part of the incoming SIP dialog's source URI (usually the From URI). The default is the asterisk (*) symbol (i.e., any host name). If this rule is not required, leave this field empty.
Source Tags src-tags [IP2IPRouting_SrcTags]	Assigns a tag to denote source URI user names corresponding to the tag configured in the associated Dial Plan. The valid value is a string of up to 20 characters. The tag is case insensitive. To configure tags, see "Configuring Dial Plans" on page 503. Note: <ul style="list-style-type: none"> ▪ Make sure that you assign the Dial Plan in which you have

Parameter	Description
	<p>configured the tag, to the related IP Group or SRD.</p> <ul style="list-style-type: none"> Instead of using tags and configuring the parameter, you can use the 'Source Username Prefix' parameter to specify a specific URI source user or all source users.
<p>Destination Username Prefix dst-user-name-prefix [IP2IPRouting_DestUsernamePrefix]</p>	<p>Defines the prefix of the incoming SIP dialog's destination URI (usually the Request URI) user part. You can use special notations for denoting the prefix. To denote calls without a user part in the URI, use the \$ sign. For available notations, see "Dialing Plan Notation for Routing and Manipulation" on page 729.</p> <p>The default is the asterisk (*) symbol (i.e., any prefix). If this rule is not required, leave this field empty.</p> <p>Note: If you need to route calls of many different destination URI user names to the same destination, you can use tags (see 'Source Tags' parameter below) instead of this parameter.</p>
<p>Destination Host dst-host [IP2IPRouting_DestHost]</p>	<p>Defines the host part of the incoming SIP dialog's destination URI (usually the Request-URI).</p> <p>The default is the asterisk (*) symbol (i.e., any destination host). If this rule is not required, leave this field empty.</p>
<p>Destination Tags dest-tags [IP2IPRouting_DestTags]</p>	<p>Assigns a prefix tag to denote destination URI user names corresponding to the tag configured in the associated Dial Plan.</p> <p>The valid value is a string of up to 20 characters. The tag is case insensitive.</p> <p>To configure prefix tags, see "Configuring Dial Plans" on page 503.</p> <p>Note:</p> <ul style="list-style-type: none"> Make sure that you assign the Dial Plan in which you have configured the prefix tag, to the related IP Group or SRD. Instead of using tags and configuring the parameter, you can use the 'Destination Username Prefix' parameter to specify a specific URI destination user or all destinations users.
<p>Message Condition message-condition-name [IP2IPRouting_MessageConditionName]</p>	<p>Assigns a SIP Message Condition rule to the IP-to-IP Routing rule.</p> <p>To configure Message Condition rules, see "Configuring Message Condition Rules" on page 469.</p>
<p>Call Trigger trigger [IP2IPRouting_Trigger]</p>	<p>Defines the reason (i.e., trigger) for re-routing (i.e., alternative routing) the SIP request:</p> <ul style="list-style-type: none"> [0] Any = (Default) This routing rule is used for all scenarios (re-routes and non-re-routes). [1] 3xx = Re-routes the request if it was triggered as a result of a SIP 3xx response. [2] REFER = Re-routes the INVITE if it was triggered as a result of a REFER request. [3] 3xx or REFER = Applies to options [1] and [2]. [4] Initial only = This routing rule is used for regular requests that the device forwards to the destination. This rule is not used for re-routing of requests triggered by the receipt of REFER or 3xx. [5] Broken Connection = If the device detects a broken RTP

Parameter	Description
	connection during the call and the Broken RTP Connection feature is enabled (IpProfile_DisconnectOnBrokenConnection parameter is configured to [2]), you can use this option as an explicit matching characteristics to route the call to an alternative destination. Therefore, for alternative routing upon broken RTP detection, position the routing rule configured with this option above the regular routing rule associated with the call. Such a configuration setup ensures that the device uses this alternative routing rule only when RTP broken connection is detected.
ReRoute IP Group re-route-ip-group-id [IP2IPRouting_ReRouteIPGroupName]	Defines the IP Group that initiated (sent) the SIP redirect response (e.g., 3xx) or REFER message. This parameter is typically used for re-routing requests (e.g., INVITEs) when interworking is required for SIP 3xx redirect responses or REFER messages. For more information, see "Interworking SIP 3xx Redirect Responses" on page 444 and "Interworking SIP REFER Messages" on page 446, respectively. The parameter functions together with the 'Call Trigger' parameter (in the table). The default is Any (i.e., any IP Group). Note: The selectable IP Group for the parameter depends on the assigned Routing Policy (in the 'Routing Policy' parameter in this table). For more information, see "Configuring SBC Routing Policy Rules" on page 484.
Action	
Destination Type dst-type [IP2IPRouting_DestType]	Determines the destination type to which the outgoing SIP dialog is sent. <ul style="list-style-type: none"> ▪ [0] IP Group = (Default) The SIP dialog is sent to the IP Group as defined in the 'Destination IP Group' (IP2IPRouting_DestIPGroupName) parameter. For more information on the actual address, see the 'Destination IP Group' parameter. ▪ [1] Dest Address = The SIP dialog is sent to the address configured in the following parameters: 'Destination Address', 'Destination Port' and 'Destination Transport Type'. ▪ [2] Request URI = The SIP dialog is sent to the address indicated in the incoming Request-URI. If the parameters 'Destination Port' and 'Destination Transport Type' are configured, the incoming Request-URI parameters are overridden and these parameters take precedence. ▪ [3] ENUM = An ENUM query is sent to include the destination address. If the parameters 'Destination Port' and 'Destination Transport Type' are configured, the incoming Request-URI parameters are overridden and these parameters take precedence. ▪ [4] Hunt Group = Used for call center survivability. For more information, see "Configuring Call Survivability for Call Centers" on page 535. ▪ [5] Dial Plan = (For Backward Compatibility Only - see Note below) The IP destination is determined by a Dial Plan index of the loaded Dial Plan file. The syntax of the Dial Plan index in the Dial Plan file is as follows: <destination / called prefix number>,0,<IP destination>

Parameter	Description
	<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 data-bbox="687 392 1390 571">[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"> ▪ [7] LDAP = LDAP-based routing. Make sure that the Routing Policy assigned to the routing rule is configured with the LDAP Server Group for defining the LDAP server(s) to query. ▪ [9] Routing Server = Device sends a request to a third-party routing server for an appropriate destination (next hop) for the matching call. ▪ [10] All Users = Device checks whether the Request-URI (i.e., destination user) in the incoming INVITE is registered in its' users' database, and if yes, it sends the INVITE to the address of the corresponding contact specified in the database. If the Request-URI is not registered, the call is rejected. ▪ [11] IP Group Set = The device employs load balancing and routes the call to one of the IP Groups in the IP Group Set, assigned using the 'IP Group Set' parameter (below). <p>Note: Use option [5] Dial Plan only for backward compatibility purposes; otherwise, use prefix tags as described in "Configuring Dial Plans" on page 503.</p>
Destination IP Group dst-ip-group-name [IP2IPRouting_DestIPGroupName]	<p>Defines the IP Group to where you want to route the call. The actual destination of the SIP dialog message depends on the IP Group type (as defined in the 'Type' parameter):</p> <ul style="list-style-type: none"> ▪ Server-type IP Group: The SIP dialog is sent to the IP address configured for the Proxy Set that is associated with the IP Group. ▪ User-type IP Group: The device checks if the SIP dialog is from a registered user, by searching for a match between the Request-URI of the received SIP dialog and an AOR registration record in the device's database. If found, the device sends the SIP dialog to the IP address specified in the database for the registered contact. <p>By default, no value is defined.</p> <p>Note:</p> <ul style="list-style-type: none"> ▪ The parameter is applicable only if the 'Destination Type' parameter is configured to IP Group. ▪ The selectable IP Group for the parameter depends on the assigned Routing Policy (in the 'Routing Policy' parameter in this table). For more information, see "Configuring SBC Routing Policy Rules" on page 484.

Parameter	Description
Destination SIP Interface dst-srd-id [IP2IPRouting_DestSIPInterfaceName]	Defines the destination SIP Interface to where the call is sent. By default, no value is defined. To configure SIP Interfaces, see "Configuring SIP Interfaces" on page 321. Note: <ul style="list-style-type: none"> ▪ The parameter is applicable only if the 'Destination Type' parameter is configured to any value other than IP Group. If the 'Destination Type' parameter is configured to IP Group, the following SIP Interface is used: <ul style="list-style-type: none"> ✓ Server-type IP Groups: SIP Interface that is assigned to the Proxy Set associated with the IP Group. ✓ User-type IP Groups: SIP Interface is determined during user registration with the device. ▪ For multi-tenancy, if the assigned Routing Policy is not shared (i.e., the Routing Policy is associated with an Isolated SRD), the SIP Interface must be one that is associated with the Routing Policy or with a shared Routing Policy (i.e., the Routing Policy is associated with one or more Shared SRDs). If the Routing Policy is shared, the SIP Interface can be one that is associated with any SRD or Routing Policy (but it's recommended that it belong to the same SRD/Routing Policy or to shared SRD/Routing Policy to avoid "bleeding").
Destination Address dst-address [IP2IPRouting_DestAddress]	Defines the destination address to where the call is sent. The address can be an IP address or a domain name (e.g., domain.com). If ENUM-based routing is used (i.e., the 'Destination Type' parameter is set to ENUM) the parameter defines the IP address or domain name (FQDN) of the ENUM service, for example, e164.arpa, e164.customer.net or NREnum.net. The device sends the ENUM query containing the destination phone number to an external DNS server, configured in the IP Interfaces table. The ENUM reply includes a SIP URI (user@host) which is used as the destination Request-URI in this routing table. The valid value is a string of up to 50 characters (IP address or FQDN). By default, no value is defined. Note: <ul style="list-style-type: none"> ▪ The parameter is applicable only if the 'Destination Type' parameter is set to Dest Address [1] or ENUM [3]; otherwise, the parameter is ignored. ▪ 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 153). ▪ To terminate SIP OPTIONS messages at the device (i.e., to handle them locally), set the parameter to "internal".
Destination Port dst-port [IP2IPRouting_DestPort]	Defines the destination port to where the call is sent.
Destination Transport Type dst-transport-type	Defines the transport layer type for sending the call: <ul style="list-style-type: none"> ▪ [-1] = (Default) Not configured - the transport type is

Parameter	Description
[IP2IPRouting_DestTransportType]	<p>determined by the SIPTransportType global parameter.</p> <ul style="list-style-type: none"> ▪ [0] UDP ▪ [1] TCP ▪ [2] TLS
IP Group Set ipgroupset-name [IP2IPRouting_IPGroupSetName]	<p>Assigns an IP Group Set to the routing rule. The device routes the call to one of the IP Groups in the IP Group Set according to the load-balancing policy configured for the IP Group Set. For more information, see Configuring IP Group Sets on page 487.</p> <p>Note: The parameter is applicable only if you configure the 'Destination Type' parameter to IP Group Set (above).</p>
Call Setup Rules Set ID call-setup-rules-set-id [IP2IPRouting_CallSetupRulesSetId]	<p>Assigns a Call Setup Rule Set ID to the routing rule. The device performs the Call Setup rules of this Set ID if the incoming call matches the characteristics of this routing rule. The device routes the call to the destination according to the routing rule's configured action, only after it has performed the Call Setup rules.</p> <p>To configure Call Setup rules, see "Configuring Call Setup Rules" on page 370.</p>
Group Policy group-policy [IP2IPRouting_GroupPolicy]	<p>Defines whether the routing rule includes call forking.</p> <ul style="list-style-type: none"> ▪ [0] None = (Default) Call uses only this route (even if Forking Group members are configured in the rows below it). ▪ [1] Forking = Call uses this route and the routes of Forking Group members, if configured (in the rows below it). <p>Note: Each Forking Group can contain up to 20 members. In other words, up to 20 routing rules can be configured for the same Forking Group.</p>
Cost Group cost-group [IP2IPRouting_CostGroup]	<p>Assigns a Cost Group to the routing rule for determining the cost of the call.</p> <p>By default, no value is defined.</p> <p>To configure Cost Groups, see "Configuring Cost Groups" on page 256.</p> <p>Note:</p> <ul style="list-style-type: none"> ▪ To implement LCR and its Cost Groups, you must enable LCR for the Routing Policy assigned to the routing rule (see "Configuring SBC Routing Policy Rules" on page 484). If LCR is disabled, the device ignores the parameter. ▪ The Routing Policy also determines whether matched routing rules that are not assigned Cost Groups are considered as a higher or lower cost route compared to matching routing rules that are assigned Cost Groups. For example, if the 'Default Call Cost' parameter in the Routing Policy is configured to Lowest Cost, even if the device locates matching routing rules that are assigned Cost Groups, the first-matched routing rule without an assigned Cost Group is considered as the lowest cost route and thus, chosen as the preferred route.

26.4 Configuring SIP Response Codes for Alternative Routing Reasons

The Alternative Routing Reasons table lets you configure up to 20 SIP response codes for call release (termination) reasons. If a call (outgoing SIP dialog-initiating methods, e.g., INVITE, OPTIONS, and SUBSCRIBE messages) is released as a result of a configured SIP code (e.g., SIP 406), the device searches for an alternative routing rule for the call in the IP-to-IP Routing table (see "Configuring SBC IP-to-IP Routing Rules" on page 470).

Typically, the device performs alternative routing when there is no response at all to an INVITE message. This is done after a user-defined number of INVITE re-transmissions, configured by the SIPMaxRtx parameter. In such a scenario, the device issues itself the SIP response code 408 (Request Timeout). Alternative routing is only done if you have configured the response code in the Alternative Routing Reasons table.

You can also configure alternative routing for the following proprietary response codes, if configured in the table, that are issued by the device itself:

- **805 IP Profile Call Limit:** The device generates the response code when Call Admission Control (CAC) limits (e.g., maximum concurrent calls) are exceeded for an IP Group (or SRD). The CAC rules are configured in the Admission Control table (see "Configuring Admission Control" on page 457). When this occurs, the device sends a SIP 480 (Temporarily Unavailable) response to the SIP entity. In such a scenario, an alternative route configured in the IP-to-IP Routing table can be used.
- **806 Media Limits Exceeded:** The device generates the response code when the call is terminated due to crossed user-defined thresholds of QoE metrics such as MOS, packet delay, and packet loss (see "Configuring Quality of Experience Profiles" on page 291) and/or media bandwidth (see "Configuring Bandwidth Profiles" on page 296). When this occurs, the device sends a SIP 480 (Temporarily Unavailable) response to the SIP entity. This is configured by 1) assigning an IP Group a QoE and/or Bandwidth profile that rejects calls if the threshold is crossed, 2) configuring 806 in the Alternative Routing Reasons table and 3) configuring an alternative routing rule.

The device also generates the response code when it rejects a call based on Quality of Service rules due to crossed Voice Quality and Bandwidth thresholds (see "Configuring Quality of Service Rules" on page 300). If the response code is configured in the table and the device rejects a call due to threshold crossing, it searches in the IP-to-IP Routing table for an alternative routing rule.

- **818 Signalling Limits Exceeded:** The device generates the response code when it rejects a call based on Quality of Service rules due to crossed ASR, NER or ACD thresholds (see "Configuring Quality of Service Rules" on page 300). If the response code is configured in the table and the device rejects a call due to threshold crossing, it searches in the IP-to-IP Routing table for an alternative routing rule.



Note:

- If the device receives a SIP 408 response, an ICMP message, or no response, alternative routing is still performed even if the code is not configured in the Alternative Routing Reasons table.
- SIP requests belonging to an SRD or IP Group that have reached the call limit (maximum concurrent calls and/or call rate) as configured 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 480 (Temporarily Unavailable) response.

The following procedure describes how to configure the Alternative Routing Reasons table through the Web interface. You can also configure it through ini file (SBCAlternativeRoutingReasons) or CLI (configure voip > sbc routing sbc-alt-routing-reasons).

➤ **To configure SIP reason codes for alternative IP routing:**

1. Open the Alternative Routing Reasons table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **Alternative Reasons**).
2. Click **New**; the following dialog box appears:

Figure 26-8: Alternative Routing Reasons Table - Dialog Box

3. Configure a SIP response code for alternative routing according to the parameters described in the table below.
4. Click **Apply**.

Table 26-4: Alternative Routing Reasons Table Parameter Descriptions

Parameter	Description
Index [SBCAlternativeRoutingReasons_Index]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
Release Cause rel-cause [SBCAlternativeRoutingReasons_ReleaseCause]	Defines a SIP response code for triggering the device's alternative routing mechanism. [4] 4xx; [5] 5xx; [6] 6xx; [400] Bad Request; [402] 402 Payment Required; [403] Forbidden; [404] Not Found; [405] Method Not Allowed; [406] Not Acceptable; [408] Request Timeout (Default); [409] Conflict; [410] Gone; [413] Request Too Large; [414] Request URI Too Long; [415] Unsupported Media; [420] Bad Extension; [421] Extension Required; [423] Session Interval Too Small; [480] Unavailable; [481] Transaction Not Exist; [482] Loop Detected; [483] Too Many Hops; [484] Address Incomplete; [485] Ambiguous; [486] Busy; [487] Request Terminated; [488] Not Acceptable Here; [491] Request Pending; [493] Undecipherable; [500] Internal Error; [501] Not Implemented; [502] Bad Gateway; [503] Service Unavailable; [504] Server Timeout; [505] Version Not Supported; [513] Message Too Large; [600] Busy Everywhere; [603] Decline; [604] Does Not Exist Anywhere; [606] Not Acceptable; [805] Admission Failure; [806] Media Limits Exceeded; [818] Signalling Limits Exceeded.

26.5 Configuring SBC Routing Policy Rules

The Routing Policies table lets you configure up to 600 Routing Policy rules. A Routing Policy determines the routing and manipulation (inbound and outbound) rules per SRD in a multiple SRD configuration topology. The Routing Policy also configures the following:

- Enables Least Cost Routing (LCR), and configures default call cost (highest or lowest) and average call duration for routing rules that are not assigned LCR Cost Groups. The default call cost determines whether matched routing rules that are not assigned Cost Groups are considered as a higher or lower cost route compared to other matching routing rules that are assigned Cost Groups. If you disable LCR, the device ignores the Cost Groups assigned to the routing rules in the IP-to-IP Routing table.
- Assigns LDAP servers (LDAP Server Group) for LDAP-based routing. IP-to-IP routing rules configured for LDAP or CSR (Call Setup Rules) queries use the LDAP server(s) that is assigned to the routing rule's associated Routing Policy. You can configure a Routing Policy per SRD or alternatively, configure a single Routing Policy that is shared between all SRDs.

The implementation of Routing Policies is intended for the following deployments **only**:

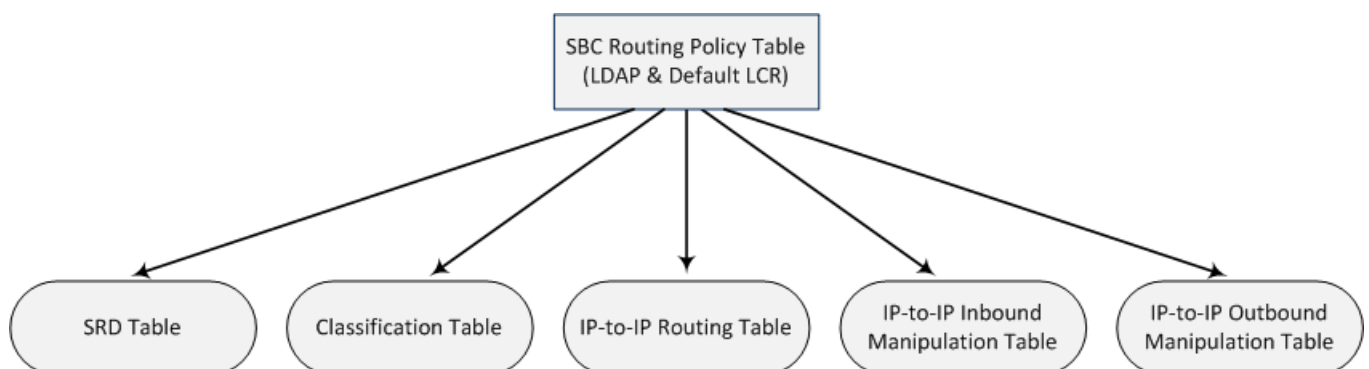
- Deployments requiring LCR and/or LDAP-based routing.
- Multi-tenant deployments that require multiple, logical routing tables where each tenant has its own dedicated ("separated") routing (and manipulation) table. In such scenarios, each SRD (tenant) is configured as an Isolated SRD and assigned its own unique Routing Policy, implementing an almost isolated, non-bleeding routing configuration topology.

For all other deployment scenarios, the Routing Policy is irrelevant and the handling of the configuration entity is not required as a default Routing Policy ("Default_SBCRoutingPolicy" at Index 0) is provided. When only one Routing Policy is required, the device automatically associates the default Routing Policy with newly added configuration entities that can be associated with the Routing Policy (as mentioned later in this section, except for Classification rules). This facilitates configuration, eliminating the need to handle the Routing Policy configuration entity (except if you need to enable LCR and/or assign an LDAP server to the Routing Policy). In such a setup, where only one Routing Policy is used, single routing and manipulation tables are employed for all SRDs.



Note: If possible, it is recommended to use only **one** Routing Policy for all SRDs (tenants), unless deployment requires otherwise (i.e., a dedicated Routing Policy per SRD).

Once configured, you need to associate the Routing Policy with an SRD(s) in the SRDs table. To determine the routing and manipulation rules for the SRD, you need to assign the Routing Policy to routing and manipulation rules. The figure below shows the configuration entities to which Routing Policies can be assigned:



Typically, assigning a Routing Policy to a Classification rule is not required, as when an incoming call is classified it uses the Routing Policy associated with the SRD to which it belongs. However, if a Routing Policy is assigned to a Classification rule, it overrides the Routing Policy assigned to the SRD. The option to assign Routing Policies to Classification rules is useful in deployments requiring different routing and manipulation rules for specific calls pertaining to the **same** SRD. In such scenarios, you need to configure multiple Classification rules for the same SRD, where for some rules no Routing Policy is assigned (i.e., the SRD's assigned Routing Policy is used) while for others a different Routing Policy is specified to override the SRD's assigned Routing Policy.

In multi-tenant environments employing multiple SRDs and Routing Policies, the IP Groups that can be used in routing rules (in the IP-to-IP Routing table) are as follows:

- If the Routing Policy is assigned to only one SRD and the SRD is an Isolated SRD, the routing rules of the Routing Policy can be configured with IP Groups belonging to the Isolated SRD and IP Groups belonging to all Shared SRDs.
- If the Routing Policy is assigned to a Shared SRD, the routing rules of the Routing Policy can be configured with any IP Group (i.e., belonging to Shared and Isolated SRDs). In effect, the Routing Policy can include routing rules for call routing between Isolated SRDs.
- If the Routing Policy is assigned to multiple SRDs (Shared and/or Isolated), the routing rules of the Routing Policy can be configured with IP Groups belonging to all Shared SRDs as well as IP Groups belonging to Isolated SRDs that are assigned the Routing Policy.

To facilitate the configuration of routing rules in the IP-to-IP Routing table through the Web interface, only the permitted IP Groups (according to the above) are displayed as optional values.

The general flow for processing the call for multi-tenant deployments and Routing Policies is as follows:

1. Using the Classification table, the device classifies the incoming call to an IP Group, based on the SIP Interface on which the call is received. Based on the SIP Interface, the device associates the call to the SRD that is assigned to the SIP Interface.
2. Once the call has been successfully classified to an IP Group, the Routing Policy assigned to the associated SRD is used. However, if a Routing Policy is configured in the Classification table, it overrides the Routing Policy assigned to the SRD.
3. The regular manipulation (inbound and outbound) and routing processes are done according to the associated Routing Policy.



Note:

- The Classification table is used only if classification by registered user in the device's users registration database or by Proxy Set fails.
- If the device receives incoming calls (e.g., INVITE) from users that have already been classified and registered in the device's registration database, the device ignores the Classification table and uses the Routing Policy that was determined for the user during the initial classification process.

The following procedure describes how to configure Routing Policies rules through the Web interface. You can also configure it through ini file (SBCRoutingPolicy) or CLI (configure voip > sbc routing sbc-routing-policy).

➤ **To configure a Routing Policy rule:**

1. Open the Routing Policies table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **Routing Policies**).

- Click **New**; the following dialog box appears:

Figure 26-9: Routing Policies Table - Add Dialog Box

- Configure the Routing Policy rule according to the parameters described in the table below.
- Click **Apply**.

Table 26-5: Routing Policies table Parameter Descriptions

Parameter	Description
General	
Index	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
Name name [SBCRoutingPolicy_Name]	Defines an arbitrary name to easily identify the row. The valid value is a string of up to 41 characters. By default, no name is defined. If you don't configure a name, the device automatically assigns a name in the following format: "SBCRoutingPolicy_<Index>", for example, "SBCRoutingPolicy_2". Note: Each row must be configured with a unique name.
LDAP Servers Group Name ldap-srv-group-name [SBCRoutingPolicy_LdapServersGroupName]	Assigns an LDAP Server Group to the Routing Policy. Routing rules in the IP-to-IP Routing table that are associated with the Routing Policy and that are configured with LDAP and/or Call Setup Rules, use the LDAP server(s) configured for this LDAP Server Group. By default, no value is defined. For more information on LDAP Server Groups, see "Configuring LDAP Server Groups" on page 228. Note: The default Routing Policy is assigned the default LDAP Server Group ("DefaultCTRLServersGroup").
Least Cost Routing	

Parameter	Description
LCR Feature lcr-enable [SBCRoutingPolicy_LCREnable]	<p>Enables the Least Cost Routing (LCR) feature for the Routing Policy.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable <p>For more information on LCR, see "Least Cost Routing" on page 254.</p>
Default Call Cost lcr-default-cost [SBCRoutingPolicy_LCRDefaultCost]	<p>Defines whether routing rules in the IP-to-IP Routing table that are not assigned a 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"> ▪ [0] Lowest Cost = (Default) The device considers a matched routing rule (belonging to the Routing Policy) that is not assigned a Cost Group as the lowest cost route. Therefore, it uses the routing rule. ▪ [1] Highest Cost = The device considers a matched routing rule (belonging to the Routing Policy) that is not assigned a Cost Group as the highest cost route. Therefore, it is only used if the other matched routing rules that are assigned Cost Groups are unavailable. <p>Note: If multiple matched routing rules without an assigned Cost Group exist, the device selects the first matched rule in the table.</p>
LCR Call Duration lcr-call-length [SBCRoutingPolicy_LCRAverageCallLength]	<p>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).</p> <p>The valid value is 0-65533. The default is 1.</p> <p>For example, assume the following Cost Groups:</p> <ul style="list-style-type: none"> ▪ "Weekend A": call connection cost is 1 and charge per minute is 6. Therefore, a call of 1 minute cost 7 units. ▪ "Weekend B": call connection cost is 6 and charge per minute is 1. Therefore, a call of 1 minute cost 7 units. <p>Therefore, for calls under one minute, "Weekend A" carries the lower cost. However, if the average call duration is more than one minute, "Weekend B" carries the lower cost.</p>

26.6 Configuring IP Group Sets

The IP Group Set table lets you configure up to 51 IP Group Sets. An IP Group Set is a group of IP Groups used for load balancing of calls, belonging to the same source, to a call destination (i.e., IP Group). Each IP Group Set can include up to five IP Groups (Server-type and/or Gateway-type only). The chosen destination IP Group for each call depends on the configured load-balancing policy, which can be Round Robin, Random Weights, or Homing (for more information, see the table's description, later in this section).

Alternative routing within the IP Group Set is also supported, whereby if a chosen destination IP Group responds with a reject response that is configured as a reason for alternative routing (see Configuring SIP Response Codes for Alternative Routing Reasons

on page 482) or doesn't respond at all (i.e., keep-alive with its' associated Proxy Set fails), the device attempts to send the call to another IP Group in the IP Group Set (according to the load-balancing policy). For enabling Proxy Set keep-alive, see Configuring Proxy Sets on page 341.

An example of round-robin load-balancing and alternative routing: The first call is sent to IP Group #1 in the IP Group Set, the second call to IP Group #2, and the third call to IP Group #3. If the call sent to IP Group #1 is rejected, the device employs alternative routing and sends it to IP Group #4.

To implement call load-balancing by IP Groups, you need to assign the IP Group Sets to the desired routing rules in the IP-to-IP Routing table. The 'Destination Type' of these routing rules must also be configured to **IP Group Set**. For more information, see Configuring SBC IP-to-IP Routing Rules on page 470.

IP Group Sets are configured using two tables with parent-child type relationship:

- **Parent table:** IP Group Set table, which defines the name and load-balancing policy of the IP Group Set.
- **Child table:** IP Group Set Member table, which assigns IP Groups to IP Group Sets. You can assign up to five IP Groups per IP Group Set.

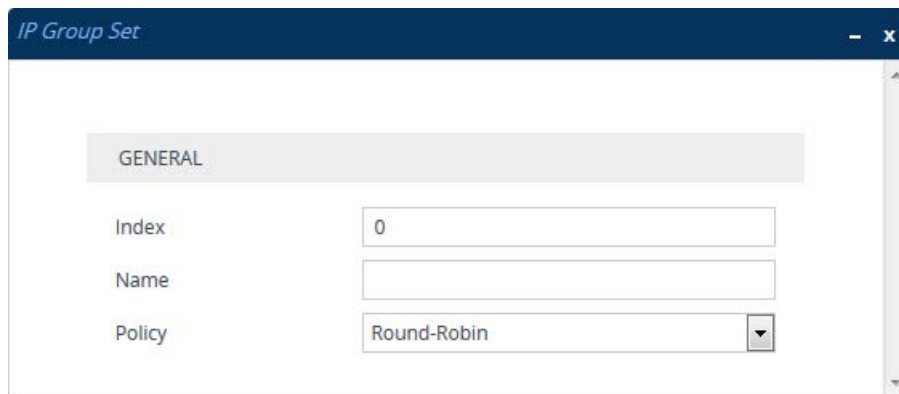
The following procedure describes how to configure IP Group Sets through the Web interface. You can also configure it through other management platforms:

- **IP Group Set Table:** *ini* file (IPGroupSet) or CLI (configure voip >)
- **IP Group Set Member Table:** *ini* file (IPGroupSetMember) or CLI (configure voip >)

➤ **To configure an IP Group Set:**

1. Open the IP Group Set table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Routing** > **IP Group Set**).
2. Click **New**; the following dialog box appears:

Figure 26-10: IP Group Set Table - Dialog Box



3. Configure the IP Group Set according to the parameters described in the table below.
4. Click **Apply**.

Table 26-6: IP Group Set Table Parameter Descriptions

Parameter	Description
General	
Index [IPGroupSet_Index]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.

Parameter	Description
Name [IPGroupSet_Name]	<p>Defines an arbitrary name to easily identify the row.</p> <p>The valid value is a string of up to 41 characters. By default, no name is defined. If you don't configure a name, the device automatically assigns a name in the following format: "IPGroupSet_<index>". For example, if you add a new row to Index 0, the following name is assigned: "IPGroupSet_0"</p> <p>Note: Each row must be configured with a unique name.</p>
Policy [IPGroupSet_Policy]	<p>Defines the load-balancing policy.</p> <ul style="list-style-type: none"> ▪ [0] Round-Robin = (Default) The device selects the next consecutive, available IP Group for each call. The device selects the first IP Group in the table (i.e., lowest index) for the first call and the next consecutive IP Groups for the next calls. For example, first call to IP Group at Index 0, second call to IP Group at Index 2, third call to IP Group at Index 3, and so on. If an IP Group is offline, the device selects the next consecutive IP Group. Once the last IP Group in the IP Group Set list is selected for a call, the device goes to the beginning of the list and sends the next call to the first IP Group, and so on. ▪ [1] Random Weight = The device selects IP Groups at random and their weights determine their probability of getting chosen over others. The higher the weight, the more chance of the IP Group being chosen. ▪ [2] Homing = The device always attempts to send all calls to the first IP Group in the table (i.e., lowest index). If unavailable, it sends the calls to the next consecutive, available IP Group. However, if the first IP Group comes online again, the device selects it. <p>Note: For the Random Weight optional value, use the 'Weight' parameter in the IP Group Set Member table (below) to configure weight value per IP Group.</p>

5. Select the IP Group Set row for which you want to assign IP Groups, and then click the **IP Group Set Member** link located below the table; the IP Group Set Member table appears.
6. Click **New**; the following dialog box appears:

Figure 26-11: IP Group Set Member Table - Dialog Box

7. Configure IP Group Set members according to the parameters described in the table below.

8. Click **Apply**, and then save your settings to flash memory.

IP Group Set Member Table Parameter Descriptions

Parameter	Description
Index <i>index</i> [IPGroupSetMember_IPGroupSetMemberIndex]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
IP Group [IPGroupSetMember_IPGroupName]	Assigns an IP Group to the IP Group Set. To configure IP Groups, see Configuring IP Groups. Note: The IP Group can only be a Server-type or Gateway-type.
Weight [IPGroupSetMember_Weight]	Defines the weight of the IP Group. The higher the weight, the more chance of the IP Group being selected as the destination of the call. The valid value is 1 to 9. The default is 1. Note: The parameter is applicable only if you configure the 'Policy' parameter to Random Weight .

27 SBC Manipulations

This section describes the configuration of the manipulation rules for the SBC application.

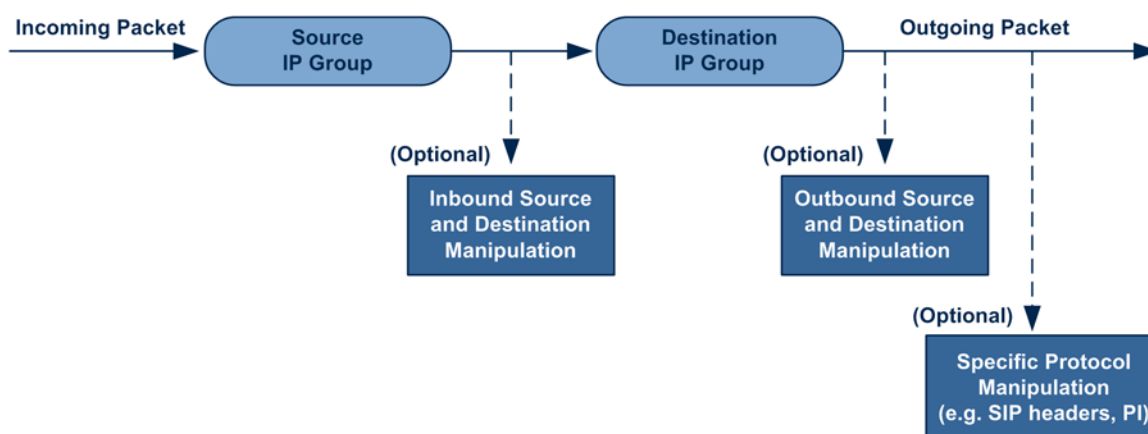


Note: For additional manipulation features, see the following:

- "Configuring SIP Message Policy Rules".
- "Configuring SIP Message Manipulation" on page 362.

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 27-1: 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 Groups 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;paramer1=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=OllAN;parameter1=abe
    
```

to

```

From:
<sip:97000@IP_PBX;user=phone;x=y;z=a>;tag=OWan;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=OllAN;parameter1=abe
    
```

to

```

From:
<sip:97000@IP_PBX;user=phone;x=y;z=a>;tag=OWan;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>
```

27.1 Configuring IP-to-IP Inbound Manipulations

The Inbound Manipulations table lets you configure up to 3,000 IP-to-IP Inbound Manipulation rules. An Inbound Manipulation rule defines a manipulation sequence for 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)

Configuration of Inbound Manipulation rules includes two areas:

- **Match:** Defines the matching characteristics of an incoming SIP dialog (e.g., source host name).
- **Action:** Defines the action that is done if the incoming call matches the characteristics of the rule. In other words, the device manipulates the source or destination SIP URI user part of the SIP dialog (e.g., removes a user-defined number of characters from the left of the SIP URI user part).



Note: Configure stricter classification rules higher up in the table than less strict rules to ensure the desired rule is used to manipulate the incoming dialog. *Strict* refers to the number of matching characteristics configured for the rule. For example, a rule configured with source host name and source IP Group as matching characteristics is stricter than a rule configured with only source host name. If the rule configured with only source host name appears higher up in the table, the device ("erroneously") uses the rule to manipulate incoming dialogs matching this source host name (even if they also match the rule appearing lower down in the table configured with the source IP Group as well).

To configure and apply an Inbound Manipulation rule, the rule must be associated with a Routing Policy. The Routing Policy associates the rule with an SRD(s). Therefore, the Routing Policy lets you configure manipulation rules for calls belonging to specific SRD(s). However, as multiple Routing Policies are relevant only for multi-tenant deployments (if needed), for most deployments, only a single Routing Policy is required. As the device provides a default Routing Policy ("Default_SBCRoutingPolicy"), when only one Routing Policy is required, the device automatically assigns the default Routing Policy to the routing rule. If you are implementing LDAP-based routing (with or without Call Setup Rules) and/or

Least Cost Routing (LCR), you need to configure these settings for the Routing Policy (regardless of the number of Routing Policies employed). For more information on Routing Policies, see "Configuring SBC Routing Policy Rules" on page 484.



Note: The IP Groups table can be used to configure a host name that overwrites the received host name. This manipulation can be done for source and destination IP Groups (see "Configuring IP Groups" on page 329).

The following procedure describes how to configure Inbound Manipulation rules through the Web interface. You can also configure it through ini file (IPInboundManipulation) or CLI (configure voip > sbc manipulation ip-inbound-manipulation).

➤ **To configure an Inbound Manipulation rule:**

1. Open the Inbound Manipulations table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Manipulation** > **Inbound Manipulations**).
2. Click **New**; the following dialog box appears:

Figure 27-2: Inbound Manipulations Table - Add Dialog Box

3. Configure the Inbound Manipulation rule according to the parameters described in the table below.
4. Click **Apply**.

Table 27-1: Inbound Manipulations Table Parameter Descriptions

Parameter	Description
Routing Policy routing-policy-name [IPInboundManipulation_RoutingPolicyName]	Assigns an Routing Policy to the rule. The Routing Policy associates the rule with an SRD(s). The Routing Policy also defines default LCR settings as well as the LDAP servers if the routing rule is based on LDAP routing (and Call Setup Rules).

Parameter	Description
	<p>If only one Routing Policy is configured in the Routing Policies table, the Routing Policy is automatically assigned. If multiple Routing Policies are configured, no value is assigned.</p> <p>To configure Routing Policies, see "Configuring SBC Routing Policy Rules" on page 484.</p> <p>Note: The parameter is mandatory.</p>
General	
Index [IPInboundManipulation_Index]	Defines an index number for the new table record. Note: Each table row must be configured with a unique index.
Name manipulation-name [IPInboundManipulation_ManipulationName]	Defines an arbitrary name to easily identify the manipulation rule. The valid value is a string of up to 20 characters. By default, no value is defined.
Additional Manipulation CLI: is-additional-manipulation [IPInboundManipulation_IsAdditionalManipulation]	Determines whether additional SIP URI user part manipulation is done for the table entry rule listed directly above it. <ul style="list-style-type: none"> ▪ [0] No = (Default) Regular manipulation rule (not done in addition to the rule above it). ▪ [1] Yes = If the above row entry rule matched the call, consider this row entry as a match as well and perform the manipulation specified by this rule. Note: Additional manipulation can only be done on a different SIP URI, source or destination, to the rule configured in the row above as configured by the 'Manipulated URI' parameter (see below).
Manipulation Purpose CLI: purpose [IPInboundManipulation_ManipulationPurpose]	Defines the purpose of the manipulation: <ul style="list-style-type: none"> ▪ [0] Normal = (Default) Inbound manipulations affect the routing input and source and/or destination number. ▪ [1] Routing input only = Inbound manipulations affect the routing input only, retaining the original source and destination number. ▪ [2] Shared Line = Used for 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 "Configuring BroadSoft's Shared Phone Line Call Appearance for Survivability" on page 533.
Match	
Request Type CLI: request-type [IPInboundManipulation_RequestType]	Defines the SIP request type to which the manipulation rule is applied. <ul style="list-style-type: none"> ▪ [0] All = (Default) All SIP messages. ▪ [1] INVITE = All SIP messages except REGISTER and SUBSCRIBE.

Parameter	Description
	<ul style="list-style-type: none"> ▪ [2] REGISTER = Only REGISTER messages. ▪ [3] SUBSCRIBE = Only SUBSCRIBE messages. ▪ [4] INVITE and REGISTER = All SIP messages except SUBSCRIBE. ▪ [5] INVITE and SUBSCRIBE = All SIP messages except REGISTER.
Source IP Group CLI: src-ip-group-name [IPInboundManipulation_SrcIpGroupName]	Defines the IP Group from where the incoming INVITE is received. The default is Any (i.e., any IP Group).
Source Username Prefix CLI: src-user-name-prefix [IPInboundManipulation_SrcUsernamePrefix]	Defines the prefix of the source SIP URI user name (usually in the From header). The default is the asterisk (*) symbol (i.e., any source username prefix). Note: 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 729.
Source Host CLI: src-host [IPInboundManipulation_SrcHost]	Defines the source SIP URI host name - full name (usually in the From header). The default is the asterisk (*) symbol (i.e., any host name).
Destination Username Prefix CLI: dst-user-name-prefix [IPInboundManipulation_DestUsernamePrefix]	Defines the prefix of the destination SIP URI user name, typically located in the Request-URI and To headers. The default is the asterisk (*) symbol (i.e., any destination username prefix). Note: 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 729.
Destination Host CLI: dst-host [IPInboundManipulation_DestHost]	Defines the destination SIP URI host name - full name, typically located in the Request URI and To headers. The default is the asterisk (*) symbol (i.e., any destination host name).
Operation Rule - Action	
Manipulated Item CLI: manipulated-uri [IPInboundManipulation_ManipulatedURI]	Determines whether the source or destination SIP URI user part is manipulated. <ul style="list-style-type: none"> ▪ [0] Source = (Default) Manipulation is done on the source SIP URI user part. ▪ [1] Destination = Manipulation is done on the destination SIP URI user part.
Remove From Left CLI: remove-from-left [IPInboundManipulation_RemoveFromLeft]	Defines the number of digits to remove from the left of the user name prefix. For example, if you enter 3 and the user name is "john", the new user name is "n".
Remove From Right CLI: remove-from-right [IPInboundManipulation_RemoveFromRight]	Defines the number of digits to remove from the right of the user name prefix. For example, if you enter 3 and the user name is "john", the new user name is "j". Note: If both 'Remove From Right' and 'Leave From Right' parameters are configured, the 'Remove From

Parameter	Description
	Right' setting is applied first.
Leave From Right CLI: leave-from-right [IPInboundManipulation_LeaveFromRight]	Defines the number of characters that you want retained from the right of the user name. Note: If both 'Remove From Right' and 'Leave From Right' parameters are configured, the 'Remove From Right' setting is applied first.
Prefix to Add CLI: prefix-to-add [IPInboundManipulation_Prefix2Add]	Defines the number or string that you want added to the front of the user name. For example, if you enter 'user' and the user name is "john", the new user name is "userjohn".
Suffix to Add CLI: suffix-to-add [IPInboundManipulation_Suffix2Add]	Defines the number or string that you want added to the end of the user name. For example, if you enter '01' and the user name is "john", the new user name is "john01".

27.2 Configuring IP-to-IP Outbound Manipulations

The Outbound Manipulations table lets you configure up to 3,000 IP-to-IP Outbound Manipulation rules. An Outbound Manipulation rule defines a manipulation action for the SIP Request-URI user part (source or destination) or calling name of outbound SIP dialog requests. Outbound Manipulation rules can be applied to any SIP request type (e.g., INVITE). 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 (if exists), P-Preferred (if exists), and Remote-Party-ID (if exists).

Configuration of Outbound Manipulation rules includes two areas:

- **Match:** Defines the matching characteristics of an incoming SIP dialog (e.g., source host name). As the device performs outbound manipulations only after the routing process, destination IP Groups can also be used as matching characteristics.
- **Action:** Defines the action that is done if the incoming call matches the characteristics of the rule. In other words, the device manipulates the source or destination SIP URI user part or calling name of the SIP dialog (e.g., removes a user-defined number of characters from the left of the SIP URI user part).



Note:

- Configure stricter classification rules higher up in the table than less strict rules to ensure the desired rule is used to manipulate the outbound dialog. *Strict* refers to the number of matching characteristics configured for the rule. For example, a rule configured with source host name and source IP Group as matching characteristics is stricter than a rule configured with only source host name. If the rule configured with only source host name appears higher up in the table, the device ("erroneously") uses the rule to manipulate outbound dialogs matching this source host name (even if they also match the rule appearing lower down in the table configured with the source IP Group as well).
- SIP URI host name (source and destination) manipulations can also be configured in the IP Groups table (see "Configuring IP Groups" on page 329). These manipulations are simply host name substitutions with the names configured for the source and destination IP Groups, respectively.

The following procedure describes how to configure Outbound Manipulations rules through the Web interface. You can also configure it through ini file (IPOutboundManipulation) or CLI (configure voip > sbc manipulation ip-outbound-manipulation).

➤ **To configure Outbound Manipulation rules:**

1. Open the Outbound Manipulations table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Manipulation** > **Outbound Manipulations**).
2. Click **New**; the following dialog box appears:

Figure 27-3: Outbound Manipulations Table- Add Dialog Box

3. Configure an Outbound Manipulation rule according to the parameters described in the table below.
4. Click **Apply**.

Table 27-2: Outbound Manipulations Table Parameter Description

Parameter	Description
Routing Policy routing-policy-name [IPOutboundManipulation_RoutingPolicyName]	Assigns a Routing Policy to the rule. The Routing Policy associates the rule with an SRD(s). The Routing Policy also defines default LCR settings as well as the LDAP servers if the routing rule is based on LDAP routing (and Call Setup Rules). If only one Routing Policy is configured in the Routing Policies table, the Routing Policy is automatically assigned. If multiple Routing Policies are configured, no value is assigned. To configure Routing Policies, see "Configuring SBC Routing Policy Rules" on page 484. Note: The parameter is mandatory.
General	
Index [IPOutboundManipulation_Index]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
Name manipulation-name [IPOutboundManipulation_ManipulationName]	Defines an arbitrary name to easily identify the row. The valid value is a string of up to 20 characters. By default, no value is defined.

Parameter	Description
onName]	
Additional Manipulation is-additional-manipulation [IPOutboundManipulation_IsAdditionalManipulation]	<p>Determines whether additional manipulation is done for the table entry rule listed directly above it.</p> <ul style="list-style-type: none"> ▪ [0] No = (Default) Regular manipulation rule - not done in addition to the rule above it. ▪ [1] 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. <p>Note: Additional manipulation can only be done on a different item (source URI, destination URI, or calling name) to the rule configured in the row above (configured by the 'Manipulated URI' parameter).</p>
Call Trigger trigger [IPOutboundManipulation_Trigger]	<p>Defines the reason (i.e., trigger) for the re-routing of the SIP request:</p> <ul style="list-style-type: none"> ▪ [0] Any = (Default) Re-routed for all scenarios (re-routes and non-re-routes). ▪ [1] 3xx = Re-routed if it triggered as a result of a SIP 3xx response. ▪ [2] REFER = Re-routed if it triggered as a result of a REFER request. ▪ [3] 3xx or REFER = Applies to options [1] and [2]. ▪ [4] 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.
Match	
Request Type request-type [IPOutboundManipulation_RequestType]	<p>Defines the SIP request type to which the manipulation rule is applied.</p> <ul style="list-style-type: none"> ▪ [0] All = (Default) all SIP messages. ▪ [1] INVITE = All SIP messages except REGISTER and SUBSCRIBE. ▪ [2] REGISTER = Only SIP REGISTER messages. ▪ [3] SUBSCRIBE = Only SIP SUBSCRIBE messages. ▪ [4] INVITE and REGISTER = All SIP messages except SUBSCRIBE. ▪ [5] INVITE and SUBSCRIBE = All SIP messages except REGISTER.
Source IP Group src-ip-group-name [IPOutboundManipulation_SrcIPGroupName]	<p>Defines the IP Group from where the INVITE is received. The default value is Any (i.e., any IP Group).</p>
Destination IP Group dst-ip-group-name [IPOutboundManipulation_DestIPGroupName]	<p>Defines the IP Group to where the INVITE is to be sent. The default value is Any (i.e., any IP Group).</p>
Source Username Prefix src-user-name-prefix [IPOutboundManipulation_SrcUsername]	<p>Defines the prefix of the source SIP URI user name, typically used in the SIP From header. The default value is the asterisk (*) symbol (i.e., any source</p>

Parameter	Description
amePrefix] [IPOutboundManipulation_SrcHost]	username prefix). 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 729. Note: If you need to manipulate calls of many different source URI user names, you can use tags (see 'Source Tags' parameter below) instead of this parameter.
Source Host src-host [IPOutboundManipulation_SrcHost]	Defines the source SIP URI host name - full name, typically in the From header. The default value is the asterisk (*) symbol (i.e., any source host name).
Source Tags src-tags [IPOutboundManipulation_SrcTags]	Assigns a prefix tag to denote source URI user names corresponding to the tag configured in the associated Dial Plan. The valid value is a string of up to 20 characters. The tag is case insensitive. To configure prefix tags, see "Configuring Dial Plans" on page 503. Note: <ul style="list-style-type: none"> ▪ Make sure that you assign the Dial Plan in which you have configured the prefix tag, to the related IP Group or SRD. ▪ Instead of using tags and configuring the parameter, you can use the 'Source Username Prefix' parameter to specify a specific URI source user or all source users.
Destination Username Prefix dst-user-name-prefix [IPOutboundManipulation_DestUser namePrefix]	Defines the prefix of the destination SIP URI user name, typically located in the Request-URI and To headers. The default value is the asterisk (*) symbol (i.e., any destination username prefix). 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 729. Note: If you need to manipulate calls of many different destination URI user names, you can use tags (see 'Destination Tags' parameter below) instead of this parameter.
Destination Host dst-host [IPOutboundManipulation_DestHost]	Defines the destination SIP URI host name - full name, typically located in the Request-URI and To headers. The default value is the asterisk (*) symbol (i.e., any destination host name).
Destination Tags dest-tags [IPOutboundManipulation_DestTags]	Assigns a prefix tag to denote destination URI user names corresponding to the tag configured in the associated Dial Plan. The valid value is a string of up to 20 characters. The tag is case insensitive. To configure prefix tags, see "Configuring Dial Plans" on page 503. Note: <ul style="list-style-type: none"> ▪ Make sure that you assign the Dial Plan in which you have configured the prefix tag, to the related IP Group or SRD. ▪ Instead of using tags and configuring the parameter, you can use the 'Destination Username Prefix' parameter to specify a specific URI destination user or all destinations users.

Parameter	Description
Calling Name Prefix calling-name-prefix [IPOutboundManipulation_CallingNamePrefix]	Defines the prefix of the calling name (caller ID). The calling name appears in the SIP From header. The valid value is a string of up to 37 characters. By default, no prefix is defined.
Message Condition message-condition-name [IPOutboundManipulation_MessageConditionName]	Assigns a Message Condition rule as a matching characteristic. Message Condition rules define required SIP message formats. To configure Message Condition rules, see "Configuring Message Condition Rules" on page 469.
ReRoute IP Group re-route-ip-group-name [IPOutboundManipulation_ReRouteIPGroupName]	Defines the IP Group that initiated (sent) the SIP redirect response (e.g., 3xx) or REFER message. The parameter is typically used for re-routing requests (e.g., INVITEs) when interworking is required for SIP 3xx redirect responses or REFER messages. The default is Any (i.e., any IP Group). Note: <ul style="list-style-type: none"> The parameter functions together with the 'Call Trigger' parameter (see below). For more information on interworking of SIP 3xx redirect responses or REFER messages, see "Interworking SIP 3xx Redirect Responses" on page 444 and "Interworking SIP REFER Messages" on page 446, respectively.
Action	
Manipulated Item manipulated-uri [IPOutboundManipulation_IsAdditionalManipulation]	Defines the element in the SIP message that you want manipulated. <ul style="list-style-type: none"> [0] Source URI = (Default) Manipulates the source SIP Request-URI user part. [1] Destination URI = Manipulates the destination SIP Request-URI user part. [2] Calling Name = Manipulates the calling name in the SIP message.
Remove From Left remove-from-left [IPOutboundManipulation_RemoveFromLeft]	Defines the number of digits to remove from the left of the manipulated item prefix. For example, if you enter 3 and the user name is "john", the new user name is "n".
Remove From Right remove-from-right [IPOutboundManipulation_RemoveFromRight]	Defines the number of digits to remove from the right of the manipulated item prefix. For example, if you enter 3 and the user name is "john", the new user name is "j".
Leave From Right leave-from-right [IPOutboundManipulation_LeaveFromRight]	Defines the number of digits to keep from the right of the manipulated item.
Prefix to Add prefix-to-add [IPOutboundManipulation_Prefix2Add]	Defines the number or string to add in the front of the manipulated item. For example, if you enter 'user' and the user name is "john", the new user name is "userjohn".

Parameter	Description
d]	If you set the 'Manipulated Item' parameter to Source URI or Destination URI , you can configure the parameter to a string of up to 49 characters. If you set the 'Manipulated Item' parameter to Calling Name , you can configure the parameter to a string of up to 36 characters.
Suffix to Add suffix-to-add [IPOutboundManipulation_Suffix2Add]	Defines the number or string to add at the end of the manipulated item. For example, if you enter '01' and the user name is "john", the new user name is "john01". If you set the 'Manipulated Item' parameter to Source URI or Destination URI , you can configure the parameter to a string of up to 49 characters. If you set the 'Manipulated Item' parameter to Calling Name , you can configure the parameter to a string of up to 36 characters.
Privacy Restriction Mode privacy-restriction-mode [IPOutboundManipulation_PrivacyRestrictionMode]	Defines user privacy handling (i.e., restricting source user identity in outgoing SIP dialogs). <ul style="list-style-type: none"> ▪ [0] Transparent = (Default) No intervention in SIP privacy. ▪ [1] Don't change privacy = The user identity in the outgoing SIP dialog 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"> ✓ From URL header: "anonymous@anonymous.invalid" ✓ 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". ▪ [2] Restrict = The user identity is restricted. The restriction presentation is as follows: <ul style="list-style-type: none"> ✓ From URL header: "anonymous@anonymous.invalid" ✓ 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". ▪ [3] 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. 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>Note:</p> <ul style="list-style-type: none"> ▪ Restriction is done only after user number manipulation (if any). ▪ The device identifies an incoming user as restricted if one of the following exists: <ul style="list-style-type: none"> ✓ From header user is "anonymous". ✓ P-Asserted-Identity and Privacy headers contain the value "id".

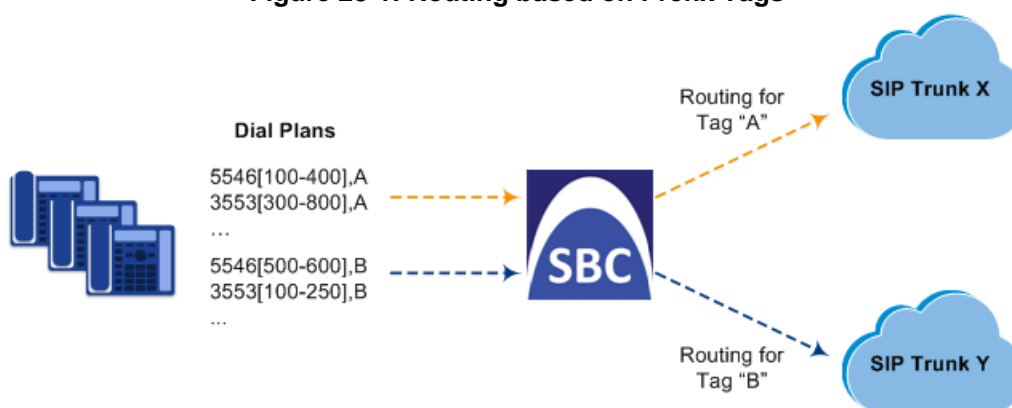
28 Configuring Dial Plans

Dial Plans let you categorize users (source and/or destination) according to source and/or destination numbers of the incoming SIP dialog-initiating requests. The device categorizes users by searching in the Dial Plan for rules that match these numbers according to prefix, suffix, and/or whole number. The categorization result in the Dial Plan is a *tag* corresponding to the matched rules. You can then use the tags to represent these users (source and/or destination users) as matching characteristics (source and/or destination tags) for the following:

- IP-to-IP Routing rules (see "Using Dial Plan Tags for IP-to-IP Routing" on page 511)
- Outbound Manipulations rules ("Using Dial Plan Tags for Outbound Manipulation" on page 514)

The figure below shows a conceptual example of routing based on tags, where users categorized as tag "A" are routed to SIP Trunk "X" and those categorized as tag "B" are routed to SIP Trunk "Y":

Figure 28-1: Routing based on Prefix Tags



Note:

- User categorization by Dial Plan is done only after the device's Classification and Inbound Manipulation processes, and before the routing process.
- Once the device successfully categorizes an incoming call by Dial Plan, it not only uses the resultant tag in the immediate routing or manipulation process, but also in subsequent routing and manipulation processes that may occur, for example, due to alternative routing or local handling of call transfer and call forwarding (SIP 3xx\REFER).
- For manipulation, tags are applicable only to outbound manipulation.



You can assign a Dial Plan to an IP Group or SRD. After Classification and Inbound Manipulation, the device checks if a Dial Plan is associated with the incoming call. It first checks the source IP Group and if no Dial Plan is assigned, it checks the SRD. If a Dial Plan is assigned to the IP Group or SRD, the device first searches the Dial Plan for a dial plan rule that matches the source number and then it searches the Dial Plan for a rule that matches the destination number. If matching dial plan rules are found, the tags configured for these rules are used in the routing and/or manipulation processes as source and/or destination tags.

The Dial Plan itself is a set of dial plan rules having the following attributes:

- **Prefix:** The prefix is matched against the source and/or destination number of the incoming SIP dialog-initiating request.

- **Tag:** The tag corresponds to the matched prefix of the source and/or destination number and is the categorization result.

You can use various syntax notations to configure the prefix numbers in dial plan rules. You can configure the prefix as a complete number (all digits) or as a partial number using some digits and various syntax notations (patterns) to allow the device to match a dial plan rule for similar source and/or destination numbers. For more information, see the description of the 'Prefix' parameter (DialPlanRule_Prefix) described later in this section.

The device employs a "best-match" method instead of a "first-match" method to match the source/destination numbers to prefixes configured in the dial plan. The matching order is done digit-by-digit and from left to right. The numbers are first matched to the rule configured with the most constrained (specific) character set. Most constrained implies that the dial plan pattern that has the fewest possible matches for a digit is matched first. For example, if one rule contains the "x" wildcard character, which has ten possible matches (i.e., 0-9) and another rule a specific digit (e.g., 4), the rule with the specific digit is selected as the matching rule. The best match priority is listed below in chronological order:

- Specific character (prefix)
- "x" wildcard, which denotes any digit (0-9)
- Number range
- Suffix, where the longest digits is first matched. For example, ([001-999]) takes precedence over ([01-99]) which takes precedence over ([1-9]).
- . (dot), which denotes any character

For example, the table below shows the best match priority of an incoming call with prefix number "5234":

Table 28-1: Dial Plan Best Match Priority

Dial Plan	Best Match Priority (Where 1 is Highest)
523x,A	2
523([4]),A or [(5234)]	4
523[2-6],A	3
523.,A	5
5234,B	1

The following examples show how the best-matching method is done. Each example has two dial plan rules which are shown listed in chronological order as they would be configured in the table.

- For incoming calls with prefix number "5234", the rule with tag B is chosen (more specific for digit "4"):

```
523x,A
5234,B
```

- For incoming calls with prefix number "5234", the rule with tag B is chosen (more specific for digit "4"):

```
523x,A
523[1-9],B
```

- For incoming calls with prefix number "53211111", the rule with tag B is chosen (more specific for fourth digit):

```
532[1-9]1111,A
5321,B
```

- For incoming calls with prefix number "53124", the rule with tag B is chosen (more specific for digit "1"):


```
53([2-4]),A
531(4),B
```

- For incoming calls with prefix number "321444", the rule with tag A is chosen and for incoming calls with prefix number "32144", the rule with tag B is chosen:

```
321xxx,A
321,B
```

- For incoming calls with prefix number "5324", the rule with tag B is chosen (prefix is more specific for digit "4"):

```
532[1-9],A
532[2-4],B
```

- For incoming calls with prefix number "53124", the rule with tag C is chosen (longest suffix - C has three digits, B two digits and A one digit):

```
53([2-4]),A
53([01-99]),B
53([001-999]),C
```

- For incoming calls with prefix number "53124", the rule with tag B is chosen (suffix is more specific for digit "4"):

```
53([2-4]),A
53(4),B
```

Dial Plans are configured using two tables with parent-child type relationship:

- **Parent table:** Dial Plan table, which defines the name of the Dial Plan. You can configure up to 50 Dial Plans.
- **Child table:** Dial Plan Rule table, which defines the actual dial plans (rules) per Dial Plan. You can configure up to 2,000 for Mediant VE of less than 16-GB RAM and 20,000 for greater than (inclusive) 16-GB RAM dial plan rules in total (where all can be configured for one Dial Plan or configured between different Dial Plans).

The following procedure describes how to configure Dial Plans through the Web interface. You can also configure it through other management platforms:

- **Dial Plan table:** *ini* file (DialPlans) or CLI (configure voip > sbc dial-plan)
- **Dial Plan Rule table:** *ini* file (DialPlanRule) or CLI (configure voip > sbc dial-plan-rule)

➤ To configure Dial Plans:

1. Open the Dial Plan table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Dial Plan**).
2. Click **New**; the following dialog box appears:

Figure 28-2: Dial Plan Table - Add Dialog Box

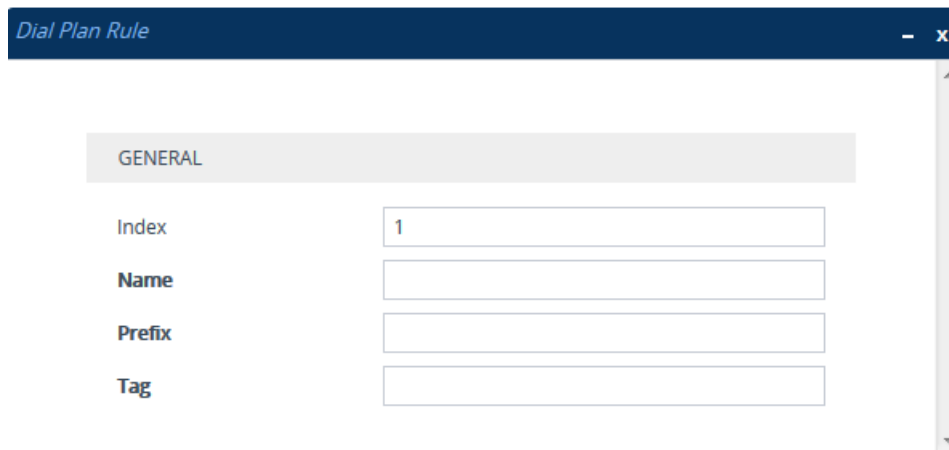
The screenshot shows a web-based dialog box titled "Dial Plan". It has a dark blue header with the title and window control icons. Below the header is a light gray tab labeled "GENERAL". Underneath the tab, there are two input fields. The first is labeled "Index" and contains the number "2". The second is labeled "Name" and is currently empty.

3. Configure a Dial Plan name according to the parameters described in the table below.
4. Click **Apply**.

Table 28-2: Dial Plan Table Parameter Descriptions

Parameter	Description
Index [DialPlans_Index]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
Name name [DialPlans_Name]	Defines an arbitrary name to easily identify the row. The valid value is a string of up to 15 characters.

- In the Dial Plan table, select the row for which you want to configure dial plan rules, and then click the **Dial Plan Rule** link located below the table; the Dial Plan Rule table appears.
- Click **New**; the following dialog box appears:

Figure 28-3: Dial Plan Rule Table - Add Dialog Box


The screenshot shows a dialog box titled "Dial Plan Rule". Inside the dialog, there is a "GENERAL" tab. Below the tab, there are four input fields:

- Index:** A text box containing the number "1".
- Name:** An empty text box.
- Prefix:** An empty text box.
- Tag:** An empty text box.

- Configure a dial plan rule according to the parameters described in the table below.
- Click **New**, and then save your settings to flash memory.

Table 28-3: Dial Plan Rule Table Parameter Descriptions

Parameter	Description
Index index [DialPlanRule_DialPlanIndex]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
Name name [DialPlanRule_Name]	Defines an arbitrary name to easily identify the row. The valid value is a string of up to 15 characters. Note: Each row must be configured with a unique name.
Prefix prefix [DialPlanRule_Prefix]	Defines the prefix number of the source or destination number. The valid value is up to 50 characters. The following syntax can be used: <ul style="list-style-type: none"> 0-9: Specific digit. x: Wildcard denoting any digit from 0 through 9. z: Denotes a number from 1 through 9. n: Denotes a number from 2 through 9. a-z: Lower-case letter. A-Z: Upper-case letter.

Parameter	Description
	<ul style="list-style-type: none"> ▪ *: (Asterisk symbol) If it is the only character in the rule, it denotes any number. To denote the asterisk "*" symbol itself, precede it with the escape "\\" character (see below). ▪ \: (Backslash escape character) When it prefixes a wildcard character (*, z, n, and x), the character itself is used and not the meta-meaning. For example, "\\x" denotes the character "x", while "x" is the wildcard denoting any digits from 0-9. ▪ #: (Pound or hash symbol) When used at the end of the prefix it denotes the end of the number. For example, "54324#" represents a 5-digit number that starts with the digits 54324. ▪ .: (Period) Denotes any letter or digit. ▪ [n-m], (n-m), or ([n1-m1,n2-m2,a,b,c,n3-m3]): Represents a mixed notation of single numbers and multiple ranges. To represent the prefix, the notation is enclosed by square brackets [...]; to represent the suffix, the notation is enclosed by square brackets which are enclosed by parenthesis ([...]). For example, to denote numbers 123 through 130, 455, 766, and 780 through 790: <ul style="list-style-type: none"> ✓ Prefix: [123-130,455,766,780-790] ✓ Suffix: ([123-130,455,766,780-790]) <p>Note: The ranges and the single numbers in the syntax must have the same amount of digits. For example, each number range and single number in the example above consists of three digits.</p>
Tag tag [DialPlanRule_Tag]	Defines a tag. The valid value is up to 16 characters (alphanumeric and special characters such as the dollar \$ sign). The tag is case insensitive.

28.1 Importing and Exporting Dial Plans

You can import and export Dial Plans in comma-separated value (CSV) file format. The Web interface lets you import and export Dial Plans from and to a local folder on the PC running the Web client. The CLI lets you import and export Dial Plans from and to a remote server.

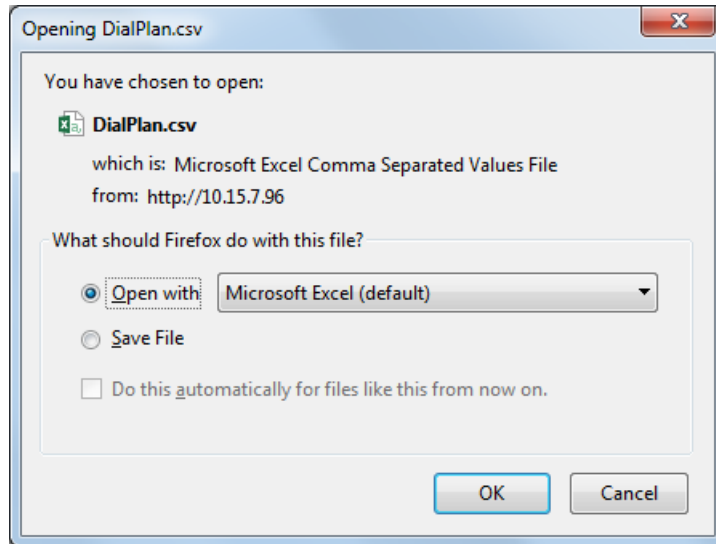
The following procedures describe how to export configured Dial Plans.

➤ To export all configured dial plan rules:

- Web interface (to a local folder):
 1. Open the Dial Plan table.

2. From the 'Action' drop-down menu, choose **Export**; the following dialog box appears:

Figure 28-4: Exporting Dial Plan



3. Select the **Save File** option, and then click **OK**; the file is saved to the default folder on your PC for downloading files.

- CLI (to a remote server):

```
(config-voip)# sbc dial-plan-rule export-csv-to all <URL to CSV file>
```

- **To export rules of a specific Dial Plan:**

- Web interface (to a local folder):

1. Open the Dial Plan table.
2. Select the required Dial Plan, and then click the **Dial Plan Rule** link; the Dial Plan Rule table opens, displaying the rules of the selected Dial Plan.
3. From the 'Action' drop-down menu, choose **Export**; a dialog box appears (as shown above).
4. Select the **Save File** option, and then click **OK**; the file is saved to the default folder on your PC for downloading files.

- CLI (to a remote server):

```
(config-voip)# sbc dial-plan-rule export-csv-to <Dial Plan name or index> <URL of server>
```

For example:

```
(config-voip)# sbc dial-plan-rule export-csv-to 0 http://10.8.8.20/upload/index_0_Dial_Plans.csv
```

The following procedures describe how to import a Dial Plan file.

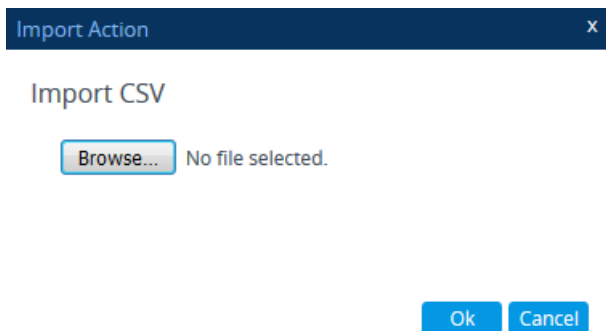
- **To overwrite all existing Dial Plans with imported Dial Plan file:**

- Web interface (from a local folder):

1. Open the Dial Plan table.

2. From the 'Action' drop-down menu, choose **Import**; the following dialog box appears:

Figure 28-5: Importing Dial Plan Rules for Specific Dial Plan



3. Use the **Browse** button to select the Dial Plan file on your PC, and then click **OK**.

- CLI (from a remote server):

```
(config-voip)# sbc dial-plan-rule import-csv-from all <URL of server>
```

Note:

- The file import feature only imports rules of Dial Plans that already exist in the Dial Plan table. If a Dial Plan in the file does not exist in the table, the specific Dial Plan is not imported.
- Make sure that the names of the Dial Plans in the imported file are **identical** to the existing Dial Plan names in the Dial Plan table; otherwise, Dial Plans in the file with different names are not imported.
- When importing a file, the rules in the imported file replace all existing rules of the corresponding Dial Plan. For existing Dial Plans in the Dial Plan table that are not listed in the imported file, the device deletes all their rules. For example, if the imported file contains only the Dial Plan "MyDialPlan1" and the device is currently configured with "MyDialPlan1" and "MyDialPlan2", the rules of "MyDialPlan1" in the imported file replace the rules of "MyDialPlan1" on the device, and the rules of "MyDialPlan2" on the device are deleted (the Dial Plan name itself remains).



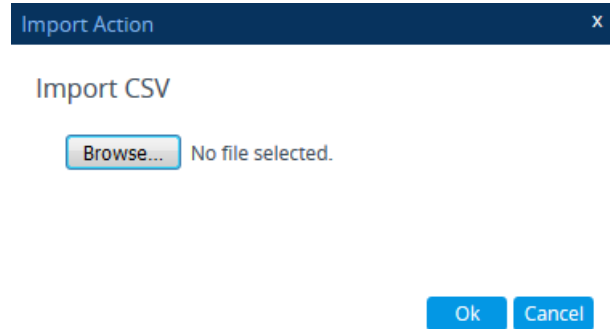
- **To import dial plan rules for a specific Dial Plan:**

- Web interface (from a local folder):

1. Open the Dial Plan table.
2. Select the required Dial Plan, and then click the **Dial Plan Rule** link; the Dial Plan Rule table opens, displaying all the rules of the selected Dial Plan.

- From the 'Action' drop-down menu, choose **Import**; the following dialog box appears:

Figure 28-6: Importing Dial Plan Rules for Specific Dial Plan



- Use the **Browse** button to select the Dial Plan file on your PC, and then click **OK**.



Note: The rules in the imported file replace **all** existing rules of the specific Dial Plan.

- CLI (from a remote server):

```
(config-voip)# sbc dial-plan-rule import-csv-from <Dial Plan name or index> <URL path to CSV file>
```

For example:

```
(config-voip)# sbc dial-plan-rule import-csv-from 0 http://10.8.8.20/upload/Dial_Plan_1_Rules.csv
```

For creating Dial Plans in a CSV file for import, see "Creating Dial Plan Files for Import" on page 510.

28.2 Creating Dial Plan Files

You can configure Dial Plans in an external file (*.csv) and then import them into the device, as described in "Importing and Exporting Dial Plans" on page 507. You can create the file using any text-based editor such as Notepad or Microsoft Excel. The file must be saved with the *.csv file name extension.

To configure Dial Plans in a file, use the following syntax:

```
DialPlanName,Name,Prefix,Tag
```

Where:

- DialPlanName:** Name of the Dial Plan.
- Name:** Name of the dial plan rule belonging to the Dial Plan.
- Prefix:** Source or destination number prefix.
- Tag:** Result of the user categorization and can be used as matching characteristics for routing and outbound manipulation

For example:

```
DialPlanName,Name,Prefix,Tag
PLAN1,rule_100,5511361xx,A
PLAN1,rule_101,551136184[4000-9999]#,B
MyDialPlan,My_rule_200,5511361840000#,itasp_1
MyDialPlan,My_rule_201,66666#,itasp_2
```

28.3 Using Dial Plan Tags for IP-to-IP Routing

For deployments requiring hundreds of routing rules (which may exceed the maximum number of rules that can be configured in the IP-to-IP Routing table), you can employ tags to represent the many different calling (source URI user name) and called (destination URI user name) prefix numbers in your routing rules. Tags are typically implemented when you have users of many different called and/or calling numbers that need to be routed to the same destination (e.g., IP Group or IP address). In such a scenario, instead of configuring many routing rules to match all the required prefix numbers, you need only to configure a single routing rule using the tag to represent all the possible prefix numbers.

An example scenario where employing tags could be useful is in deployments where the device needs to service calls in a geographical area that consists of hundreds of local area codes, where each area code is serviced by one of two SIP Trunks in the network. In such a deployment, instead of configuring hundreds of routing rules to represent each local area code, you can simply configure two routing rules where each is assigned a unique tag representing a group of local area codes and the destination IP Group associated with the SIP Trunk servicing them.



Note:

- Source and destination tags can be used in the same routing rule.
- The same tag can be used for source and destination tags in the same routing rule.

The following procedure describes how to configure IP-to-IP routing based on tags.

➤ **To configure IP-to-IP routing based on tags:**

1. In the Dial Plan table, configure a Dial Plan (see "Configuring Dial Plans" on page 503). For example, the Dial Plan file below defines two tags, "LOC" and "INTL" to represent different called number prefixes for local and long distance (International) calls:

INDEX ↕	NAME	PREFIX	TAG
0	Local	42520[3-5]	LOC
1	Local	425207	LOC
2	Local	42529	LOC
3	International	425200	INTL
4	International	425100	INTL

2. For the IP Group or SRD associated with the calls for which you want to use tag-based routing, assign the Dial Plan that you configured in Step 1.
 - IP Groups table: 'Dial Plan' parameter (IPGroup_SBCDialPlanName) - see "Configuring IP Groups" on page 329
 - SRDs table: 'Dial Plan' parameter (SRD_SBCDialPlanName) - see "Configuring SRDs" on page 311
3. In the IP-to-IP Routing table (see "Configuring SBC IP-to-IP Routing Rules" on page 470), configure a routing rule with the required destination and whose matching characteristics include the tag(s) that you configured in your Dial Plan in Step 1. The tags are assigned under the **Match** group, using the following parameters:
 - 'Source Tags' parameter (IP2IPRouting_SrcTags): tag denoting the calling user
 - 'Destination Tags' parameter (IP2IPRouting_DestTags): tag denoting the called user

28.3.1 Dial Plan Backward Compatibility



Note: This section is for backward compatibility **only**. It is recommended to migrate your Dial Plan configuration to the latest Dial Plan feature (see "Using Dial Plan Tags for IP-to-IP Routing" on page 511).

Configure prefix tags in the Dial Plan file using the following syntax:

```
[ PLAN<index> ]
<prefix number>,0,<prefix tag>
```

where:

- *Index* is the Dial Plan index
- *prefix number* is the called or calling number prefix (ranges can be defined in brackets)
- *prefix tag* is the user-defined prefix tag of up to nine characters, representing the prefix number

Each prefix tag type - called or calling - must be configured in a dedicated Dial Plan index number. For example, Dial Plan 1 can be for called prefix tags and Dial Plan 2 for calling prefix tags.

The example Dial Plan file below defines the prefix tags "LOCL" and "INTL" to represent different called number prefixes for local and long distance calls:

```
[ PLAN1 ]
42520[3-5],0,LOCL
425207,0,LOCL
42529,0,LOCL
425200,0,INTL
425100,0,INTL
....
```



Note:

- Called and calling prefix tags can be used in the same routing rule.
- When using prefix tags, you need to configure manipulation rules to remove the tags before the device sends the calls to their destinations.

The following procedure describes how to configure IP-to-IP routing using prefix tags.

➤ **To configure IP-to-IP routing using prefix tags:**

1. Configure a Dial Plan file with prefix tags, and then load the file to the device.
2. Add the prefix tags to the numbers of specific incoming calls using Inbound Manipulation rules:
 - a. Open the Inbound Manipulations table (see "Configuring IP-to-IP Inbound Manipulations" on page 493), and then click **New**.
 - b. Configure matching characteristics for the incoming call (e.g., set 'Source IP Group' to "1").
 - c. From the 'Manipulated Item' drop-down list, select **Source** to add the tag to the calling URI user part, or **Destination** to add the tag to the called URI user part.

28.4 Using Dial Plan Tags for Outbound Manipulation

You can use Dial Plan tags to denote source and/or destination URI user names in Outbound Manipulation rules in the Outbound Manipulations table.

The following procedure describes how to configure Outbound Manipulation based on tags.

➤ **To configure Outbound Manipulation based on tags:**

1. In the Dial Plan table, configure a Dial Plan (see "Configuring Dial Plans" on page 503).
2. In the IP Group or SRD associated with the calls for which you want to use tag-based routing, assign the Dial Plan that you configured in Step 1.
 - IP Groups table: 'Dial Plan' parameter (IPGroup_SBCDialPlanName) - see "Configuring IP Groups" on page 329
 - SRDs table: 'Dial Plan' parameter (SRD_SBCDialPlanName) - see "Configuring SRDs" on page 311
3. In the Outbound Manipulations table (see "Configuring IP-to-IP Outbound Manipulations" on page 497), configure a rule with the required manipulation and whose matching characteristics include the tag(s) that you configured in your Dial Plan in Step 1. The tags are assigned using the following parameters:
 - 'Source Tags' parameter (IPOutboundManipulation_SrcTags): tag denoting the calling users
 - 'Destination Tags' parameter (IPOutboundManipulation_DestTags): tag denoting the called users

28.5 Using Dial Plan Tags for Call Setup Rules

You can use Dial Plan tags in Call Setup rules, configured in the Call Setup Rules table (see [Configuring Call Setup Rules](#) on page 370). The Call Setup rule can be assigned to an IP Group and is processed by the device for the classified source IP Group immediately before the routing process (i.e., Classification > Manipulation > Dial Plan table > Call Setup rules > Routing). The result of the Call Setup rule (i.e., source and/or destination tag) can be used as the matching characteristics for locating a suitable IP-to-IP Routing rule in the IP-to-IP Routing table.

You can configure Call Setup rules to query the Dial Plan table for a specified search key (prefix) in a specified Dial Plan to obtain the corresponding tag. The Call Setup rule can then perform many different manipulations (based on Message Manipulation syntax), including modifying the name of the tag. The tags can be used only in the 'Condition', 'Action Subject' and 'Action Value' fields.

28.6 Using Dial Plan Tags for Message Manipulation

You can use Dial Plan tags (srctags and dsttags) in Message Manipulation rules, configured in the Message Manipulations table (see [Configuring SIP Message Manipulation](#) on page 362). The tags can be used only in the 'Condition' and 'Action Value' fields. For example, you can configure a rule that adds the SIP header "City" with the value "ny" (i.e., City: ny) to all outgoing SIP INVITE messages associated with the source tag "ny":

Message Manipulations

—
×

<div style="background-color: #f0f0f0; padding: 5px; margin-bottom: 5px; font-weight: bold;">GENERAL</div> <p>Index: <input type="text" value="0"/></p> <p>Name: <input type="text" value="New Header for Tag ny"/></p> <p>Manipulation Set ID: <input type="text" value="0"/></p> <p>Row Role: <input type="text" value="Use Current Condition"/></p>	<div style="background-color: #f0f0f0; padding: 5px; margin-bottom: 5px; font-weight: bold;">ACTION</div> <p>Action Subject: <input type="text" value="header.City"/></p> <p>Action Type: <input type="text" value="Add"/></p> <p>Action Value: <input type="text" value="srctags"/></p>
<div style="background-color: #f0f0f0; padding: 5px; margin-bottom: 5px; font-weight: bold;">MATCH</div> <p>Message Type: <input type="text" value="invite.request"/></p> <p>Condition: <input type="text" value="srctags=='ny'"/></p>	



Note: You cannot modify Dial Plan tags using Message Manipulation rules.

29 Configuring Malicious Signatures

The Malicious Signature table lets you configure up to 30 Malicious Signature patterns. Malicious Signatures are signature patterns that identify SIP user agents (UA) who perform malicious attacks on SIP servers by SIP scanning. Malicious Signatures allow you to protect SBC calls handled by the device from such malicious activities, thereby increasing your SIP security. The Malicious Signature patterns identify specific scanning tools used by attackers to search for SIP servers in the network. The feature identifies and protects against SIP (Layer 5) threats by examining new inbound SIP dialog messages. Once the device identifies an attack based on the configured malicious signature pattern, it marks the SIP message as invalid and discards it or alternatively, rejects it with a SIP response (by default, 400), configured in the Message Policies table. Protection applies only to new dialogs (e.g., INVITE and REGISTER messages) and unauthenticated dialogs.

Malicious signatures can also be used with the Intrusion Detection System (IDS) feature (see "Configuring IDS Policies" on page 164). You can configure an IDS Policy that is activated if the device detects a malicious signature (when the 'Reason' parameter is configured to **Dialog establishment failure**).

Malicious signature patterns are typically based on the value of SIP User-Agent headers, which attackers use as their identification string (e.g., "User-Agent: VaxSIPUserAgent"). However, you can configure signature patterns based on any SIP header. To configure signature patterns, use the same syntax as that used for configuring Conditions in the Message Manipulations table (see "Configuring SIP Message Manipulation" on page 362). Below are configured signature patterns based on the User-Agent header:

- Malicious signature for the VaxSIPUserAgent malicious UA:

```
header.user-agent.content prefix 'VaxSIPUserAgent'
```

- Malicious signature for the scanning tool "sip-scan":

```
Header.User-Agent.content prefix 'sip-scan'
```

By default, the table provides preconfigured malicious signatures of known, common attackers.



Note:

- Malicious Signatures do not apply to the following:
 - ✓ Calls from IP Groups where Classification is by Proxy Set.
 - ✓ In-dialog SIP sessions (e.g., refresh REGISTER requests and re-INVITEs).
 - ✓ Calls from users that are registered with the device.
- If you delete all the entries in the table, when you next reset the device, the table is populated again with all the default signatures.

You can export / import Malicious Signatures in CSV file format to / from a remote server through HTTP, HTTPS, or TFTP. To do this, use the following CLI commands:

```
(config-voip)# sbc malicious-signature-database <export-csv-to |
import-csv-from> <URL>
```

To apply malicious signatures to calls, you need to enable the use of malicious signatures for a Message Policy and then assign the Message Policy to the SIP Interface associated with the calls (i.e., IP Group). To configure Message Policies, see "Configuring SIP Message Policy Rules".

The following procedure describes how to configure Malicious Signatures through the Web interface. You can also configure it through ini file (MaliciousSignatureDB) or CLI (configure voip > sbc malicious-signature-database).

➤ **To configure a Malicious Signature:**

1. Open the Malicious Signature table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **Malicious Signature**).
2. Click **New**; the following dialog box appears:

Figure 29-1: Malicious Signature Table - Add Dialog Box



3. Configure a Malicious Signature according to the parameters described in the table below.
4. Click **Apply**.

Table 29-1: Malicious Signature Table Parameter Descriptions

Parameter	Description
Index [ConditionTable_Index]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
Name name [MaliciousSignatureDB_Name]	Defines an name to easily identify the row. The valid value is a string of up to 30 characters. Note: Each row must be configured with a unique name.
Pattern pattern [MaliciousSignatureDB_Pattern]	Defines the signature pattern. The valid value is a string of up to 60 characters. Note: The parameter is mandatory.

30 Advanced SBC Features

30.1 Configuring Call Preemption for SBC Emergency Calls

The device supports emergency call preemption for SBC calls by prioritizing emergency calls over regular calls. If the device receives an incoming emergency call when there are unavailable resources to process the call, the device preempts one of the regular calls to free up resources for sending the emergency call to its' destination (i.e., emergency service provider), instead of rejecting it. The device may preempt more than one active call in order to provide sufficient resources for processing the emergency call. Available resources depends on the number of INVITE messages currently processed by the device.

If the device preempts a call, it disconnects the call as follows:

- If the call is being setup (not yet established), it sends a SIP 488 response to the incoming leg and a SIP CANCEL message to the outgoing leg.
- If the call is already established, it sends a SIP BYE message to each leg. The device includes in the SIP BYE message, the Reason header describing the cause as "preemption".

Once the device terminates the regular call, it immediately sends the INVITE message of the emergency call to its' destination without waiting for any response from the remote sides (e.g., 200 OK after BYE). If the device is unable to preempt a call for the emergency call, it rejects the emergency call with a SIP 503 "Emergency Call Failed" (instead of "Service Unavailable") response.

For the device to identify incoming calls as emergency calls, you need to configure a Message Condition rule in the Message Conditions table. Below are examples of Message Condition rules for identifying emergency calls:

Figure 30-1: Examples of Message Conditions for Identifying Emergency Calls

INDEX ↕	NAME	CONDITION
0	Emergency1 - RP header	header.resource-priority contains 'emergency'
1	Emergency2 - RP header	header.resource-priority contains 'esnet'
2	Emergency1 - user with providers address	param.call.dst.user=='911'
3	Emergency2 - user with providers address	param.call.dst.user=='100' param.call.dst.user=='101' param.call.dst.user=='102'
4	Emergency3 - user with providers address	header.request.uri contains 'urn:service:sos'

- Indices 0 and 1: SIP Resource-Priority header contains a string indicating an emergency call.
- Indices 2 to 4: Destination user-part contains the emergency provider's address.

The device applies the Message Condition rule only after call classification (but, before inbound manipulation).



Note:

- The device does not preempt established emergency calls.
- The device does not monitor emergency calls with regards to Quality of Experience (QoE).

➤ **To configure SBC emergency call preemption:**

1. In the Message Conditions table (see "Configuring Message Condition Rules" on page 469), configure a Message Condition rule to identify incoming emergency calls. See

above for examples.

2. Open the SBC General Settings page (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **SBC General Settings**), and then scroll down to the Call Priority and Preemption group:

Figure 30-2: Configuring Emergency SBC Call Preemption

CALL PRIORITY AND PREEMPTION	
Preemption Mode	Enable
Emergency Message Condition	1
Emergency RTP DiffServ	46
Emergency Signaling DiffServ	40

3. From the 'Preemption Mode' drop-down list (SBCPreemptionMode), select **Enable** to enable call preemption.
4. In the 'Emergency Message Condition' field, enter the row index of the Message Condition rule that you configured in Step 1.
5. (Optional) Assign DiffServ levels (markings) to packets belonging to emergency calls:
 - a. In the 'Emergency RTP DiffServ' field (SBCEmergencyRTPDiffServ), enter the QoS level for RTP packets.
 - b. In the 'Emergency Signaling DiffServ' field (SBCEmergencySignalingDiffServ), enter the QoS level for SIP signaling packets.
6. Click **Apply**.

30.2 Emergency Call Routing using LDAP to Obtain ELIN

The device can route emergency calls (e.g., 911) for INVITE messages that are received without an ELIN number. This is in contrast to when the device is deployed in a Microsoft Skype for Business environment, whereby INVITE messages received from Skype for Business contain ELIN numbers. For a detailed explanation on ELIN numbers and handling of emergency calls by emergency server providers, see "E9-1-1 Support for Microsoft Skype for Business" on page 277.

To obtain an ELIN number for emergency calls received without ELINs, you can configure the device to query an LDAP server for the 911 caller's ELIN number. The device adds the resultant ELIN number and a Content-Type header for the PIDF XML message body to the outgoing INVITE message, for example:

```
Content-Type: application/pidf+xml
<NAM>1234567890</NAM>
```


➤ **To enable emergency call routing using LDAP to obtain ELIN:**

1. Configure a Call Setup rule in the Call Setup Rules table (see "Configuring Call Setup Rules" on page 370). The following example shows a Call Setup rule that queries an Active Directory (AD) server for the attribute "telephoneNumber" whose value is the E9-1-1 caller's number (source), and then retrieves the user's ELIN number from the attribute "numberELIN":

Figure 30-3: Example of Call Setup Rule for LDAP Query for ELIN

The screenshot shows the 'Call Setup Rules' configuration window with two tabs: 'GENERAL' and 'ACTION'.

GENERAL	ACTION
Index: 0	Action Subject: body.application/pdf+xml
Rules Set ID: 1	Action Type: Add
Attributes To Query: 'telephoneNumber='+param.call.src.user	Action Value: '<NAM>+ldap.attr.numberELIN+</NAM>'
Attributes To Get: numberELIN	
Row Role: Use Current Condition	
Condition: ldap.attr.numberELIN exists	

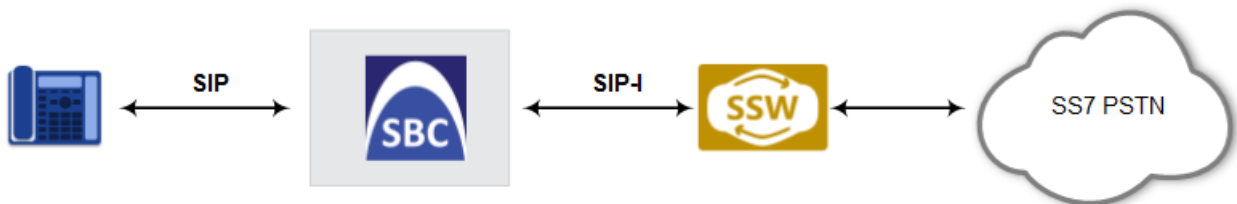
2. Enable the E9-1-1 feature, by configuring the 'PSAP Mode' parameter to **PSAP Server** in the IP Groups table for the IP Group of the PSAP server (see "Enabling the E9-1-1 Feature" on page 287).
3. Configure routing rules in the IP-to-IP Routing table for routing between the emergency callers' IP Group and the PSAP server's IP Group. The only special configuration required for the routing rule from emergency callers to the PSAP server:
 - Configure the emergency number (e.g., 911) in the 'Destination Username Prefix' field.
 - Assign the Call Setup rule that you configured for obtaining the ELIN number from the AD (see Step 1) in the 'Call Setup Rules Set ID' field (see "Configuring SBC IP-to-IP Routing Rule for E9-1-1" on page 287).

30.3 Enabling Interworking of SIP and SIP-I Endpoints

The device can interwork between SIP and SIP-I endpoints for SBC calls. SIP-I endpoints are entities that are connected to the SS7 PSTN network, referred to as the ISDN User Part (ISUP) domain. The device supports the SIP-I Application-layer signaling protocol, which is the standard for encapsulating a complete copy of the SS7 ISUP message in SIP messages, according to ITU-T Q.1912.5, Interworking between Session Initiation Protocol (SIP) and Bearer Independent Call Control protocol or ISDN User Part. In other words, SIP-I is SIP encapsulated with ISUP and the interworking is between SIP signaling and ISUP signaling. This allows you to deploy the device in a SIP environment where part of the call path involves the PSTN.

The SIP-I sends calls, originating from the SS7 network, to the SIP network by adding ISUP messaging in the SIP INVITE message body. The device can receive such a message from the SIP-I and remove the ISUP information before forwarding the call to the SIP endpoint. In the other direction, the device can receive a SIP INVITE message that has no ISUP information and before forwarding it to the SIP-I endpoint, create a SIP-I message by adding ISUP information in the SIP body. For SIP-I to SIP-I calls, the device can pass ISUP data transparently between the endpoints.

Figure 30-4: Example of Interworking SIP and SIP-I



For the interworking process, the device maps between ISUP data (including cause codes) and SIP headers. For example, the E.164 number in the Request-URI of the outgoing SIP INVITE is mapped to the Called Party Number parameter of the IAM message, and the From header of the outgoing INVITE is mapped to the Calling Party Number parameter of the IAM message.

The ISUP data is included in SIP messages using the Multipurpose Internet Mail Extensions (MIME) body part, for example (some headers have been removed for simplicity):

```
INVITE sip:1774567@172.20.1.177;user=phone SIP/2.0
Via: SIP/2.0/UDP 172.20.73.230:5060;branch=z9hG4bK.iI
...
Accept: application/sdp, application/isup, applicatio
Content-Type: multipart/mixed; boundary=unique-bounda
MIME-Version: 1.0
Content-Length: 350
...
Content-Type: application/isup; version=FTSSURI; base
Content-Disposition: signal; handling=required
01 00 40 01 0a 02 02 08 06 83 10 71 47 65 07 08
01 00 00
--unique-boundary-1-
D6 SIP-T ISUP/IAM (Initial address message)
(--) len:-- >> Nature of connection indicators
Oct 1 : ---0---- Echo ctrl = Half echo not included
----00-- Cont. check = Not required
-----00 Satellite = No circuit
(--) len:-- >> Forward call indicators
Oct 1 : 01----- ISUP pref. = Not req. all the way
```

```
--0----- ISUP indic. = Not used all the way
---0----- End-end inf = Not available
----0--- Interwork. = Not encountered
-----00- Method. ind = No method available
-----0 Call indic. = as National call
Oct 2 : -----00- SCCP method = No indication
```

ISUP data, received in the MIME body of the incoming SIP message is parsed according to the ISUP variant (SPIROU itu or ansi), indicated in the SIP Content-Type header. The device supports the following ISUP variants (configured by the 'ISUP Variant' parameter in the IP Profile table):

- French (France) specification, SPIROU (Système Pour l'Interconnexion des Réseaux OUverts), which regulates Telecommunication equipment that interconnect with networks in France. For SPIROU, the device sets the value of the SIP Content-Type header to "version=spirou; base=itu-t92+".
- ITU-92, where the device sets the value of the SIP Content-Type header to "version=itu-t92+; base=itu-t92+".

To configure interworking of SIP and SIP-I endpoints, using the 'ISUP Body Handling' parameter (IpProfile_SBCISUPBodyHandling) in the IP Profile table (see "Configuring IP Profiles" on page 388).

You can manipulate ISUP data, by configuring manipulation rules for the SIP Content-Type and Content-Disposition header values in the Message Manipulations table (see "Configuring SIP Message Manipulation" on page 362). For a complete description of the ISUP manipulation syntax, refer to the *SIP Message Manipulation Reference Guide*. In addition, you can use AudioCodes proprietary SIP header X-AC-Action in Message Manipulation rules to support the following call actions (e.g., SIP-I SUS and RES messages) for the ISUP SPIROU variant:

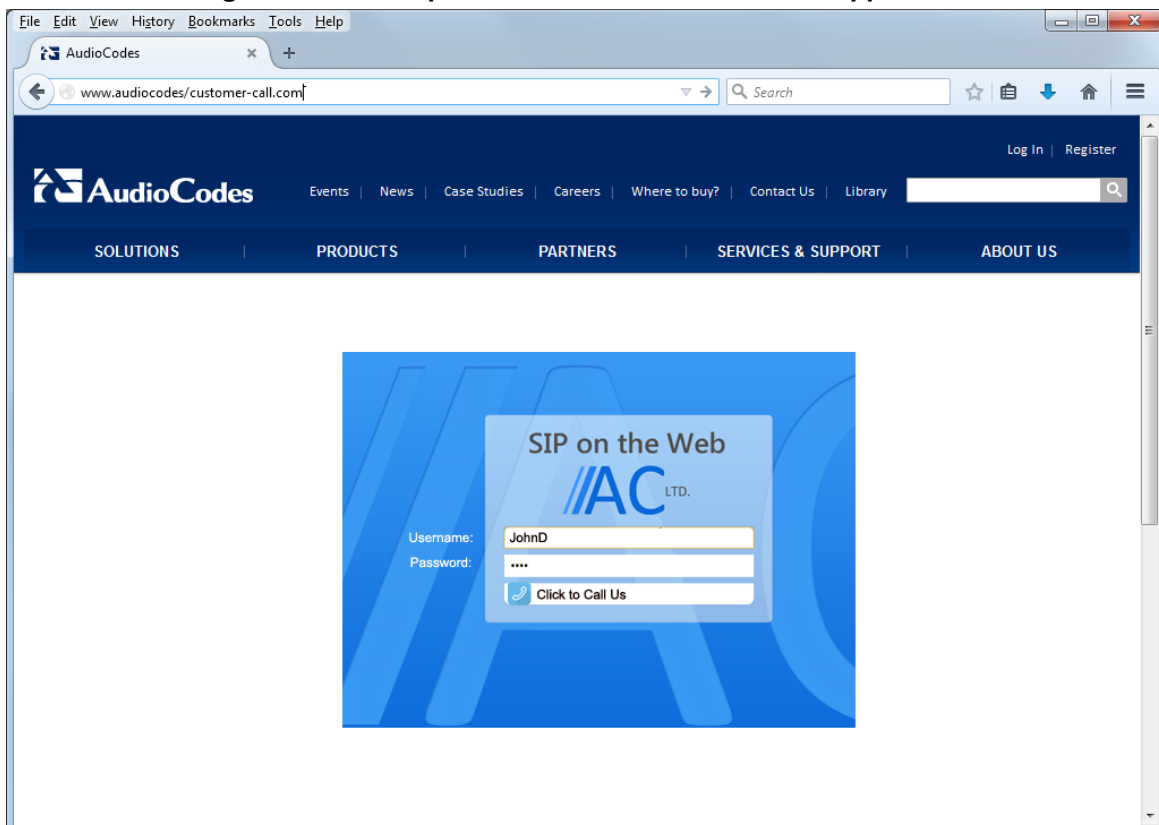
- Disconnect call (optionally, after a user-defined time): disconnect[;delay=<time in ms>]
- Resume previously suspended call: abort-disconnect
- Reply to the message with a SIP response without forwarding the response to the other side: reply[;response=<response code, e.g., 200>]
- Switch IP Profile for the call (re-INVITE only), as defined in the IP Group: switch-profile [;reason=<reason - PoorInVoiceQuality or PoorInVoiceQualityFailure >]

30.4 WebRTC

The device supports interworking of Web Real-Time Communication (WebRTC) and SIP-based VoIP communication. The device interworks WebRTC calls made from a Web browser (WebRTC client) and the SIP destination. The device provides the media interface to WebRTC.

WebRTC is a browser-based real-time communication protocol. WebRTC is an open source, client-side API definition (based on JavaScript) drafted by the World Wide Web Consortium (W3C) that supports browser-to-browser applications for voice calling (video chat, and P2P file sharing) without plugins. Currently, WebRTC is supported only by Mozilla Firefox and Google Chrome Web browsers. Though the WebRTC standard has obvious implications for changing the nature of peer-to-peer communication, it is also an ideal solution for customer-care solutions to allow direct access to the contact center. An example of a WebRTC application is a click-to-call button on a consumer Web site (see following figure). After clicking the button, the customer can start a voice and/or video call with a customer service personnel directly from the browser without having to download any additional software plugins. The figure below displays an example of a click-to-call application from a customer Web page, where the client needs to enter credentials (username and password) before placing the call.

Figure 30-5: Example of WebRTC for Click-to-Call Application



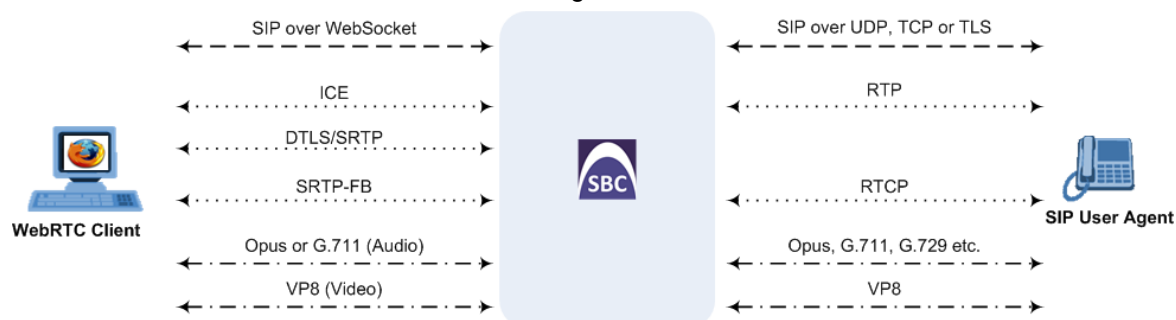
**Note:**

- The WebRTC feature is a license-dependent feature and is available only if it is included in the License Key that is installed on the device. For ordering the feature, please contact your AudioCodes sales representative.
- The maximum concurrent WebRTC sessions (signaling-over-secure WebSocket and media-over-DTLS) supported by the device is 5,000 for Mediant SE and 3,500 for Mediant VE.

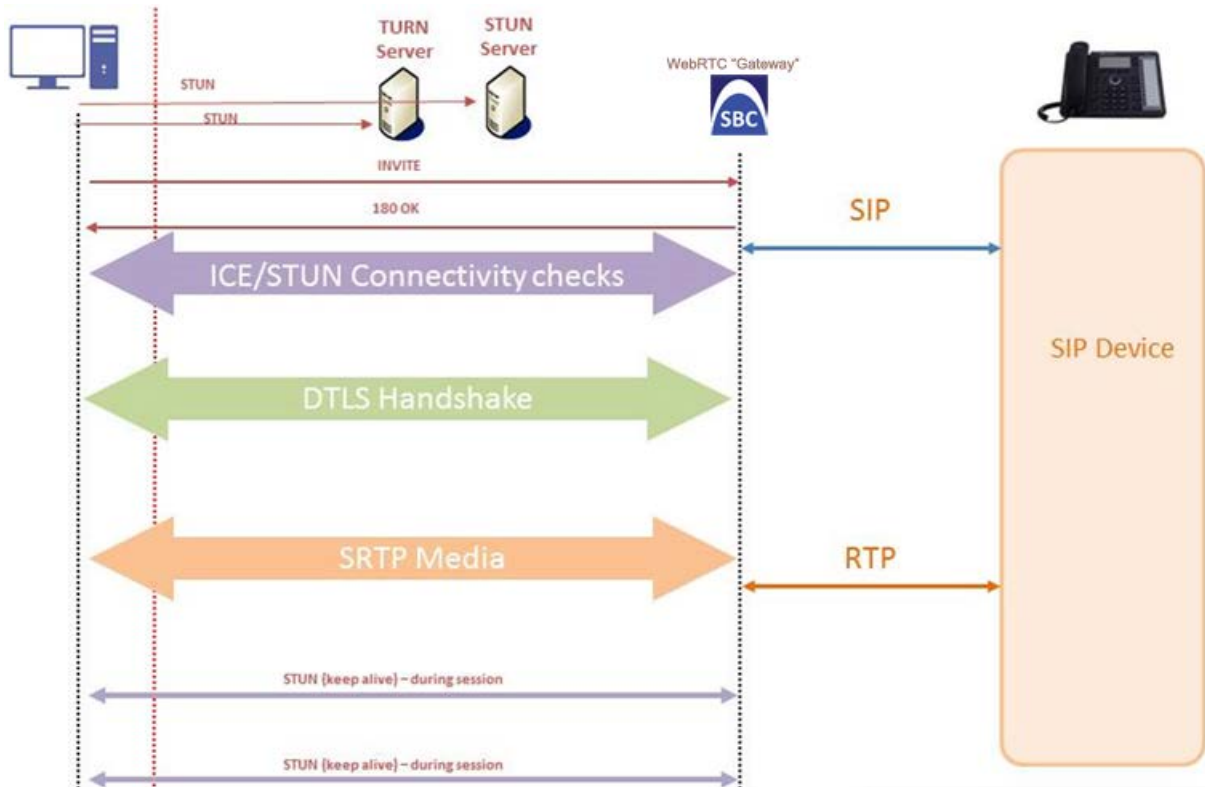
The WebRTC standard requires the following mandatory components, which are supported by the device:

- **Voice coders:** Narrowband G.711 and wideband Opus (Version 1.0.3, per RFC 6176).
- **Video coders:** VP8 video coder. The device transparently forwards the video stream, encoded with the VP8 coder, between the endpoints.
- **ICE (per RFCs 5389/5766/5245):** Resolves NAT traversal problems, using STUN and TURN protocols to connect peers. For more information, see "ICE Lite".
- **DTLS-SRTP (RFCs 5763/5764):** Media channels must be encrypted (secured) through Datagram Transport Layer Security (DTLS) for SRTP key exchange. For more information, see "SRTP using DTLS Protocol" on page 199.
- **SRTP (RFC 3711):** Secures media channels by SRTP.
- **RTP Multiplexing (RFC 5761):** Multiplexing RTP data packets and RTCP control packets onto a single port for each RTP session. For more information, see "Interworking RTP-RTCP Multiplexing".
- **Secure RTCP with Feedback (i.e., RTP/SAVPF format in the SDP - RFC 5124):** Combines secured voice (SRTP) with immediate feedback (RTCP) to improve session quality. The SRTP profile is called SAVPF and must be in the SDP offer/answer (e.g., "m=audio 11050 RTP/SAVPF 103"). For more information, see the IP Profile parameter, IPProfile_SBCRTCPFeedback (see "Configuring IP Profiles" on page 388).
- **WebSocket:** WebSocket is a signaling (SIP messaging) transport protocol, providing full-duplex communication channels over a single TCP connection for Web browsers and clients. SIP messages are sent to the device over the WebSocket session. For more information, see "SIP over WebSocket" on page 526.

For more information on WebRTC, go to <http://www.webrtc.org/>. Below shows a summary of the WebRTC components and the device's interworking of these components between the WebRTC client and the SIP user agent:



The call flow process for interworking WebRTC with SIP endpoints by the device is illustrated below and subsequently described:



1. The WebRTC client uses a Web browser to visit the Web site page.
2. The Web page receives Web page elements and JavaScript code for WebRTC from the Web hosting server. The JavaScript code runs locally on the Web browser.
3. When the client clicks the Call button or call link, the browser runs the JavaScript code which sends the HTTP upgrade request for WebSocket in order to establish a WebSocket session with the device. The address of the device is typically included in the JavaScript code.
4. A WebSocket session is established between the WebRTC client and the device in order for the WebRTC client to register with the device. This is done using a SIP REGISTER message sent over the WebSocket session (SIP over WebSocket). Registration can be initiated when the client enters credentials (username and password) on the Web page or it can be done automatically when the client initially browses to the page. This depends on the design of the Web application (JavaScript).
5. Once registered with the device, the client can receive or make calls, depending on the Web application.
6. To make a call, the client clicks the call button or link on the Web page.
7. Negotiation of a workable IP address between the WebRTC client and the device is done through ICE.
8. Negotiation of SRTP keys using DTLS is done between WebRTC and the client on the media.
9. Media flows between the WebRTC client and the SIP client located behind the device.

30.4.1 SIP over WebSocket

The device supports the transmission of SIP signaling over WebSocket. WebSocket is a protocol providing real-time, full-duplex (two-way) communication over a single TCP connection (socket) between a Web browser or page (client) and a remote host (server). This is used for browser-based applications such as click-to-call from a Web page. As

WebSocket has been defined by the WebRTC standard as mandatory, its support by the device is important for deployments implementing WebRTC.

A WebSocket connection starts as an HTTP connection between the Web client and the server, guaranteeing full backward compatibility with the pre-WebSocket world. The protocol switch from HTTP to WebSocket is referred to as the WebSocket handshake, which is done over the same underlying TCP/IP connection. A WebSocket connection is established using a handshake between the Web browser (WebSocket client) and the server (i.e., the device). The browser sends a request to the server, indicating that it wants to switch protocols from HTTP to WebSocket. The client expresses its' desire through the Upgrade header (i.e., upgrade from HTTP to WebSocket protocol) in an HTTP GET request, for example:

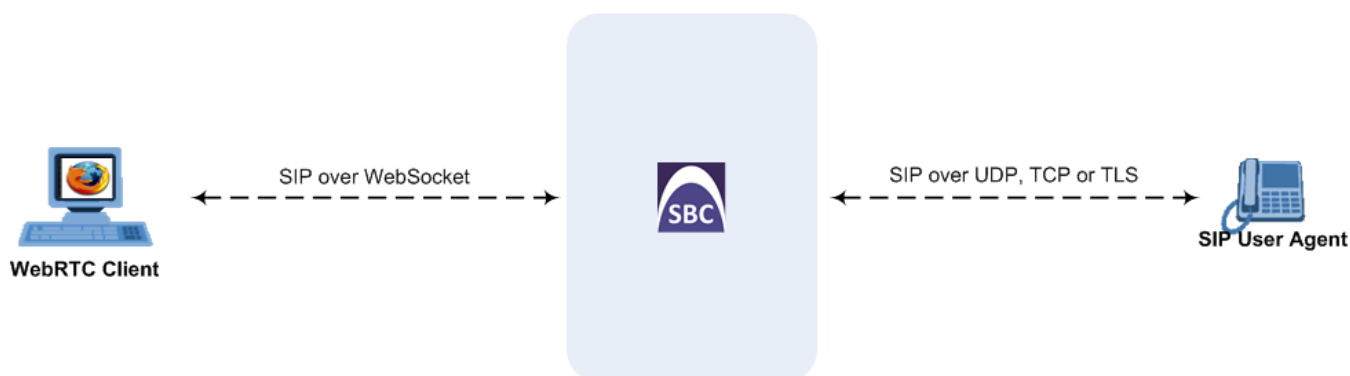
```
GET /chat HTTP/1.1
Upgrade: websocket
Connection: Upgrade
Host: <IP address:port of SBC device>
Sec-WebSocket-Protocol: SIP
Sec-WebSocket-Key: dGhlIHhnbXBsZSBub25jZQ==
Origin: <server that provided JavaScript code to browser, e.g.,
http://domain.com>
Sec-WebSocket-Version: 13
```

If the server understands the WebSocket protocol, it agrees to the protocol switch through the Upgrade header in an HTTP 101 response, for example:

```
HTTP/1.1 101 Switching Protocols
Upgrade: WebSocket
Connection: Upgrade
Sec-WebSocket-Accept: rLHCkw/SKsO9GAH/ZSFhBATDKrU=
Sec-WebSocket-Protocol: SIP
Server: SBC
```

At this stage, the HTTP connection breaks down and is replaced by a WebSocket connection over the same underlying TCP/IP connection. By default, the WebSocket connection uses the same ports as HTTP (80) and HTTPS (443).

Once a WebSocket connection is established, the SIP messages are sent over the WebSocket session. The device, as a "WebSocket gateway" or server can interwork WebSocket browser originated traffic to SIP over UDP, TCP or TLS, as illustrated below:



The SIP messages over WebSocket are indicated by the "ws" value, as shown in the example below of a SIP REGISTER request received from a client:

```
REGISTER sip:10.132.10.144 SIP/2.0
Via: SIP/2.0/ws v6iq1t8lne5c.invalid;branch=z9hG4bK7785666
Max-Forwards: 69
To: <sip:101@10.132.10.144>
From: "joe" <sip:101@10.132.10.144>;tag=ub50pqjgpr
Call-ID: fhddgc3kc3hhu32h01fghl
```

```

CSeq: 81 REGISTER
Contact: <sip:0bfr9fd5@v6iq1t8lne5c.invalid;transport=ws>;reg-id=1;+sip.instance="<urn:uuid:4405bbe2-cf06-4c27-9c59-6caf83af9b00>";expires=600
Allow: ACK,CANCEL,BYE,OPTIONS,INVITE,MESSAGE
Supported: path, outbound, gruu
User-Agent: JsSIP 0.3.7
Content-Length: 0
  
```

To keep a WebSocket session alive, it is sometimes necessary to send regular messages to indicate that the channel is still being used. Some servers, browsers or proxies may close an idle connection. The Ping-Pong WebSocket messages are designed to send non-application level traffic that prevents the channel from being prematurely closed. You can configure how often the device pings the WebSocket client, using the `WebSocketProtocolKeepAlivePeriod` parameter (see "Configuring WebRTC" on page 528). The device always replies to ping control messages with a pong message.



Note: When the device operates in High-Availability (HA) mode, if a WebSocket connection has been established and a switchover subsequently occurs, the WebSocket session is not copied to the redundant device. As Chrome does not renew the WebSocket connection with the device, WebRTC calls remain open indefinitely; the Chrome side will stop the call, but the device will keep all of the call's resources open and the other side will have an active call with no voice. To prevent this, for the IP Profile associated with the WebRTC clients, configure the ' Broken Connection Mode' parameter to Disconnect.

30.4.2 Configuring WebRTC

To support WebRTC, you need to perform special configuration settings for the device's SBC leg interfacing with the WebRTC client (i.e., Web browser), as described in the following procedure.

For the WebRTC deployment environment, you need to install a signed certificate by a Certificate Authority (CA) on you Web server machine (hosting the WebRTC JavaScript) and on your AudioCodes SBC device (i.e., WebSocket server).



Note:

- Google announced a security policy change that impacts new versions of the Chrome Web browser. Any Web site that has integrated WebRTC, geolocation technology, screen-sharing and more, now requires to be served from a secure (HTTPS) site, including WebRTC-based WebSocket servers (WSS instead of WS). The configuration described below accommodates for this basic requirement.
- WebRTC JavaScript configuration is beyond the scope of this document.

➤ To configure WebRTC:

1. Configure a TLS Context (certification):
 - a. Open the TLS Contexts table (see "Configuring TLS Certificate Contexts" on page 99).
 - b. Add a new TLS Context (e.g., "WebRTC") or edit an existing one.
 - c. Create a certificate signing request (CSR) to request a digitally signed certificate from a Certification Authority (CA).
 - d. Send the CSR to the CA for signing.

- e. When you have received the signed certificate, install it on the device as the "Device Certificate" and install the CA's root certificate into the device's trusted root store ("Trusted Certificates").

For more information on CSR, see "Assigning CSR-based Certificates to TLS Contexts" on page 103.

2. Configure the keep-alive interval with the WebSocket client:
 - a. On the Transport Settings page (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Transport Settings**), and then in the 'WebSocket Keep-Alive Period' field (WebSocketProtocolKeepAlivePeriod), enter the keep-alive interval:

Figure 30-6: Configuring Keep-alive with WebSocket Client

WebSocket Keep-Alive Period [sec]

- b. Click **Apply**.
3. Configure a SIP Interface for the WebRTC clients that identifies WebSocket traffic:
 - a. Open the SIP Interfaces table (see "Configuring SIP Interfaces" on page 321).
 - b. Do the following:
 - ◆ From the 'Encapsulating Protocol' drop-down list (SIPInterface_EncapsulatingProtocol), select **WebSocket**.
 - ◆ In the 'TLS Port' field, configure the TLS port.
 - ◆ From the 'TLS Context Name' drop-down list, assign the TLS Context that you configured in Step 1 (e.g., "WebRTC").

Figure 30-7: Configuring SIP Interface for WebRTC Clients

SIP Interfaces

SRD #0 [DefaultSRD]

GENERAL	MEDIA
Index <input type="text" value="1"/>	Media Realm -- View
Name <input type="text" value="WebRTC clients"/>	Direct Media Disable
Topology Location <input type="text" value="Down"/>	
Network Interface #0 [O+M+C] View	
Application Type <input type="text" value="SBC"/>	SECURITY
UDP Port <input type="text" value="0"/>	TLS Context Name #1 [WebRTC] View
TCP Port <input type="text" value="0"/>	TLS Mutual Authentication <input type="text" value=""/>
TLS Port <input type="text" value="10081"/>	Message Policy -- View
Encapsulating Protocol <input type="text" value="WebSocket"/>	User Security Mode Not Configured
Enable TCP Keepalive <input type="text" value="Disable"/>	Enable Un-Authenticated Registrations Not configured
	Max. Number of Registered Users -1

- c. Click **Apply**.
4. Configure an IP Profile for the WebRTC clients:

- a. Open the IP Profiles table (see "Configuring IP Profiles" on page 388).
- b. Do the following:
 - ◆ From the 'ICE Mode' drop-down list (IPProfile_SBCIceMode), select **Lite** to enable ICE.
 - ◆ From the 'RTCP Mux' drop-down list (IPProfile_SBCRTCPMux), select **Supported** to enable RTCP multiplexing.
 - ◆ From the 'RTCP Feedback' drop-down list (IPProfile_SBCRTCPFeedback), select **Feedback On** to enable RTCP feedback.

Figure 30-8: Configuring WebRTC-related Parameters for IP Profile

ICE Mode	Lite
SDP Handle RTCP	Don't Care
RTCP Mux	Supported
RTCP Feedback	Feedback On

- c. Click **Apply**.
5. Configure an IP Group for the WebRTC clients:
- a. Open the IP Groups table (see "Configuring IP Groups" on page 329).
 - b. Do the following:
 - ◆ From the 'Type' drop-down list, select **User**.
 - ◆ From the 'IP Profile' drop-down list, select the IP Profile that you configured for the WebRTC clients in Step 3 (e.g., "WebRTC").
 - ◆ From the 'DTLS Context' drop-down list, select the TLS Context that you configured in Step 1. For more information on DTLS, see "SRTP using DTLS Protocol" on page 199.

Figure 30-9: Configuring IP Group for WebRTC Clients

The screenshot shows the 'IP Groups' configuration window. At the top, there is a dropdown for 'SRD' set to '#0 [DefaultSRD]'. Below this are two main sections: 'GENERAL' and 'QUALITY OF EXPERIENCE'. The 'GENERAL' section includes fields for 'Index' (1), 'Name' (WebRTC clients), 'Topology Location' (Down), 'Type' (User), 'Proxy Set' (--), and 'IP Profile' (#2 [WebRTC]). The 'QUALITY OF EXPERIENCE' section includes 'QoE Profile' (--), 'Bandwidth Profile' (--), and a 'MESSAGE MANIPULATION' section with 'Inbound Message Manipulation Set' (-1) and 'Outbound Message Manipulation Set' (-1). At the bottom, there is a 'DTLS Context' dropdown set to '#1 [WebRTC]'. 'View' links are present next to several dropdowns.

- 6. Configure IP-to-IP routing rules to route calls between the WebRTC clients and the enterprise:

- a. Open the IP-to-IP Routing table (see "Configuring SBC IP-to-IP Routing Rules" on page 470).
- b. Configure routing rules for the following call scenarios:
 - ◆ Call routing from WebRTC clients (IP Group configured in Step 4) to the enterprise.
 - ◆ Call routing from the enterprise to the WebRTC clients (IP Group configured in Step 4).

30.5 Call Forking

This section describes various Call Forking features supported by the device.

30.5.1 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 Groups table's parameter, 'SBC Client Forking Mode' (see "Configuring IP Groups" on page 329).

The device can also fork INVITE messages received for a Request-URI of a specific contact (user), belonging to the destination IP Group User-type, registered in the database to all other users located under the same AOR as the specific contact. This is configured using the SBCSendInviteToAllContacts parameter.

30.5.2 Configuring SIP Forking Initiated by SIP Proxy

The device can handle the receipt of multiple SIP 18x responses as a result of SIP forking initiated by a proxy server. This occurs when the device forwards an INVITE, received from a user agent (UA), to a proxy server and the proxy server then forks the INVITE request to multiple UAs. Several UAs may answer and the device may therefore, receive several replies (responses) for the single INVITE request. Each response has a different 'tag' value in the SIP To header.

During call setup, forked SIP responses may result in a single SDP offer with two or more SDP answers. The device "hides" all the forked responses from the INVITE-initiating UA, except the first received response ("active" UA) and it forwards only subsequent requests and responses from this active UA to the INVITE-initiating UA. All requests/responses from the other UAs are handled by the device; SDP offers from these UAs are answered with an "inactive" media.

The device supports two forking modes:

- **Latch On First:** The device forwards only the first received 18x response to the

INVITE-initiating UA and disregards subsequently received 18x forking responses (with or without SDP).

- **Sequential:** The device forwards all 18x responses to the INVITE-initiating UA, sequentially (one after another). If 18x arrives with an offer only, only the first offer is forwarded to the INVITE-initiating UA.

➤ **To configure the call forking mode:**

1. Open the SBC General Settings page (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **SBC General Settings**).
2. From the 'Forking Handling Mode' drop-down list (SBCForkingHandlingMode), select the required mode:

Forking Handling Mode Latch On First ▼

3. Click **Apply**.

The device 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, it is possible that the SDP answer that was forwarded to the INVITE-initiating UA is irrelevant and thus, 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 SDP offer to the INVITE-initiating UA. This causes the INVITE-initiating UA to send an offer which the device forwards to the UA that confirmed the call. Media synchronization is enabled by the EnableSBCMediaSync parameter.

30.5.3 Configuring Call Forking-based IP-to-IP Routing Rules

You can configure call forking routing rules in the IP-to-IP Routing table. This is done by configuring multiple routing rules under a forking group. These rules send an incoming IP call to multiple destinations of any type (e.g., IP Group or IP address). The device forks the call by sending simultaneous INVITE messages to all the specified destinations. It handles the multiple SIP dialogs until one of the calls is answered and then terminates the other SIP dialogs. For more information, see "Configuring SBC IP-to-IP Routing Rules" on page 470.

30.6 Call Survivability

This section describes various call survivability features supported by the SBC device.

30.6.1 Enabling Auto-Provisioning of Subscriber-Specific Information of 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. The feature enables local users to dial a local extension (or any other configured alias) that identifies another local user, in survivability mode.

In normal operation, when subscribers (such as IP phones) register with 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), as shown in the example below:

```
<?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>
```

The device forwards the 200 OK to the subscriber (without the XML body). The call flow is shown below:

Figure 30-10: 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 communication with the BroadWorks server is lost. 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.

➤ **To enable the BroadWorks survivability feature:**

1. Open the SBC General Settings page (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **SBC General Settings**).
2. From the 'BroadWorks Survivability Feature' drop-down list (SBCForkingHandlingMode), select **Enable**:

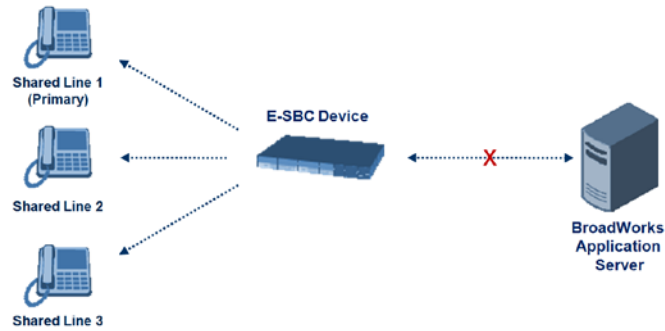
BroadWorks Survivability Feature •

3. Click **Apply**.

30.6.2 Configuring BroadSoft's Shared Phone Line Call Appearance for 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.

The 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 "Configuring SIP Forking Initiated by SIP Proxy" on page 531. Note that incoming calls specific to extensions 601 or 602 ring only at these specific extensions.

Figure 30-11: 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 following procedure describes the main configuration required.


Note:

- 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).
- You can configure whether REGISTER messages from secondary lines are terminated on the device or forwarded transparently (as is), using the `SBCSharedLineRegMode` parameter.
- The LED indicator of a shared line may display the wrong current state.

➤ To configure BroadSoft's Shared Line feature:

1. In the IP Groups table (see "Configuring IP Groups" on page 329), add a Server-type IP Group for the BroadWorks server.
2. In the IP Groups table, add a User-type IP Group for the IP phone users and set the 'SBC Client Forking Mode' parameter to **Parallel** so that the device forks incoming calls to all contacts under the same AOR registered in the device's registration database.
3. In the IP-to-IP Routing table (see "Configuring SBC IP-to-IP Routing Rules" on page 470), add a rule for routing calls between the above configured IP Groups.
4. In the Inbound Manipulations table (see "Configuring IP-to-IP Inbound Manipulations" on page 493), add a manipulation rule for the secondary extensions (e.g., 601 and 602) so that they also register to the device's database under the primary extension contact (e.g., 600):
 - 'Manipulation Purpose': **Shared Line**
 - Match:
 - ◆ 'Request Type': **REGISTER**
 - ◆ 'Source IP Group': IP Group created for the users (e.g., 2)
 - ◆ 'Source Username Prefix': Represents the secondary extensions, e.g., 601 and 602
 - Action:
 - ◆ 'Manipulated URI': **Source** (manipulates the source URI)
 - ◆ 'Remove From Right': "1" (removes the last digit of the extensions, e.g., 601 is changed to 60)
 - ◆ 'Suffix to Add': "0" (adds 0 to the end of the manipulated number, e.g., 60 is changed to 600).

30.6.3 Configuring 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 30-12: Normal Operation in Call Center Application

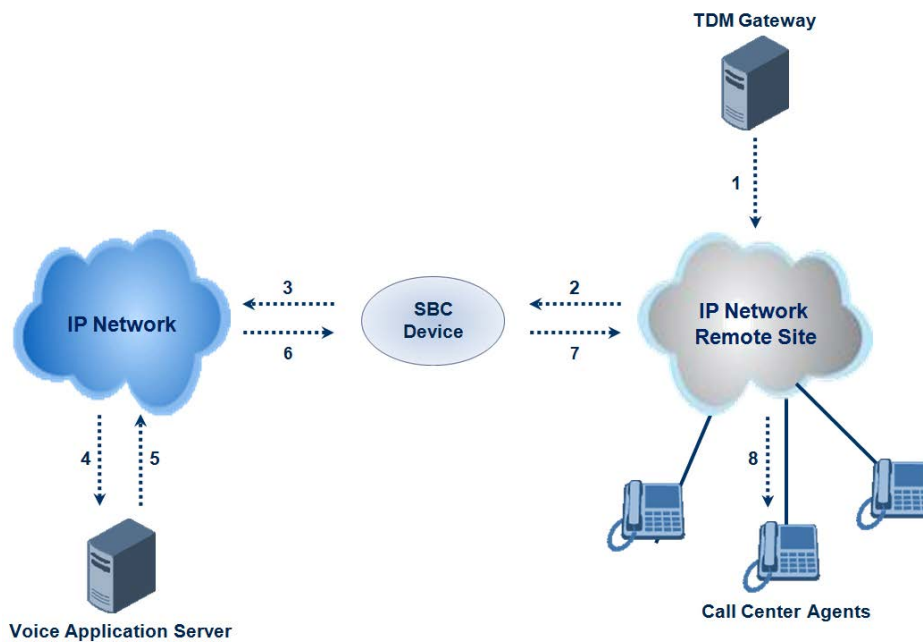
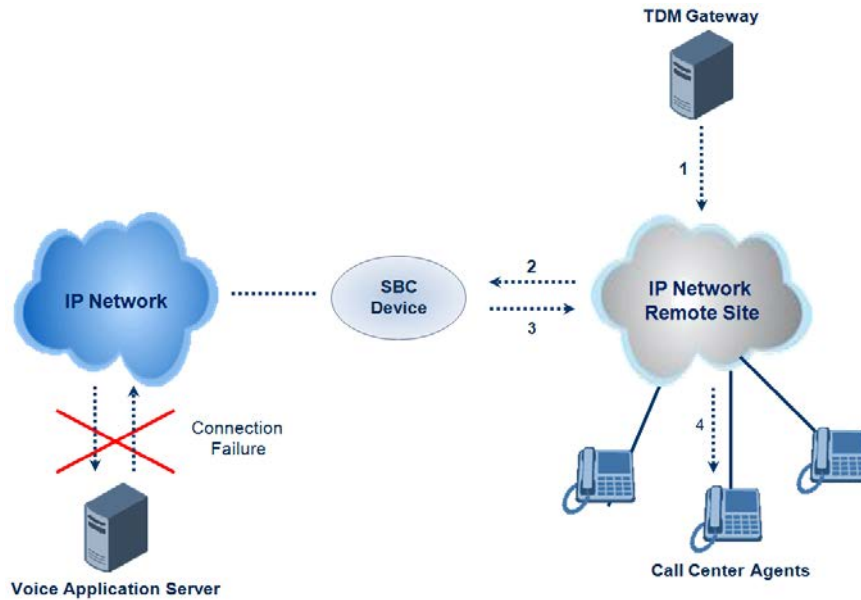


Figure 30-13: Call Survivability for Call Center



➤ **To configure call survivability for a call center application:**

1. In the IP Groups table (see "Configuring IP Groups" on page 329), 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 461), 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 Rules" on page 470), 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' 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' 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 30-14: Routing Rule Example for Call Center Survivability

The screenshot shows the configuration interface for a routing rule. It is divided into two main sections: GENERAL and ACTION. The GENERAL section is further divided into MATCH and ACTION sub-sections.

GENERAL - MATCH:

- Source IP Group: #1 [TDM Gateway] (View)
- Request Type: All
- Source Username Prefix: *
- Source Host: *
- Source Tags: (empty)
- Destination Username Prefix: *
- Destination Host: *

GENERAL - ACTION:

- Index: 3
- Name: TDM GW > Call Center
- Alternative Route Options: Route Row

ACTION:

- Destination Type: Hunt Group
- Destination IP Group: #3 [Call Center] (View)
- Destination SIP Interface: -- (View)
- Destination Address: (empty)
- Destination Port: 0
- Destination Transport Type: (empty)
- Call Setup Rules Set ID: -1
- Group Policy: None
- Cost Group: -- (View)

30.6.4 Enabling Survivability 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, "Stand Alone Mode" on their LCD screens.

If you enable the feature and the 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>
```

➤ **To enable survivability display on Aastra phones:**

1. Load an ini file to the device that includes the following parameter setting:

```
SBCEnableSurvivabilityNotice = 1
```

30.7 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.

30.8 VoIPerfect

AudioCodes VoIPerfect™ feature combines the device's Access and Enterprise SBC technology to ensure high speech (call) quality (MOS) between the Enterprise SBC and the Access SBC (located at the Internet service provider / ISP) during periods of adverse WAN network conditions (such as packet loss and bandwidth reduction). VoIPerfect adapts itself to current network conditions. Before adverse WAN network conditions can affect the quality of the call, VoIPerfect employs sophisticated technology using the Opus coder (as later explained in this section) to ensure that high call quality is maintained.

VoIPerfect guarantees that 95% of your calls will achieve a Perceptual Evaluation of Speech Quality (PESQ) score greater than or equal to 3.6 if the summation of bandwidth overuse and packet loss is less than or equal to 25%. ISPs can therefore offer service level agreements (SLAs) to their customers based on the VoIPerfect feature. For more information, contact your AudioCodes sales representative. In addition, by ensuring high call quality even in adverse network conditions, VoIPerfect may reduce costs for ISPs such as SIP trunk providers and Unified Communications as a Service (UCaaS) by eliminating the need for dedicated WAN links (such as MPLS and leased links) and instead, allow the use of standard broadband Internet connections. However, it can also be used in tandem with existing infrastructure.

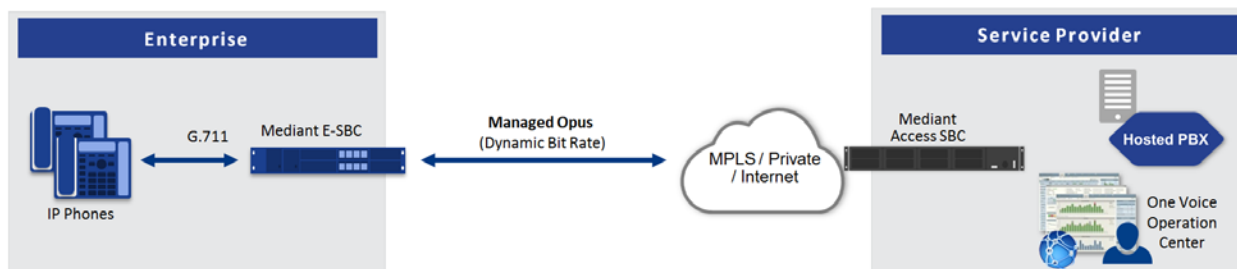
VoIPerfect uses Temporary Maximal Media Stream Bit Rate (TMMBR) negotiation capabilities for Opus coders. Through TMMBR, VoIPerfect can receive indications of network quality and dynamically change the coder's payload bit rate accordingly during the call to improve voice quality. TMMBR is an RTCP feedback message (per RFC 4585) which enables SIP users to exchange information regarding the current bit rate of the media stream. The information can be used by the receiving side to change the media stream parameters (e.g., coder rate or coder) to enhance voice quality. TMMBR is negotiated in the SDP Offer/Answer model using the 'tmbbr' attribute and following syntax:

```
a=rtcp-fb:<payload type> ccm tmmbr smaxpr=<sent TMMBR packets>
```

VoIPerfect also supports the SDP attribute 'a=rtcp-rsize', which reduces the RTCP message size (RFC 5506). As feedback messages are frequent and take a lot of bandwidth, the attribute attempts to reduce the RTCP size. The attribute can only be used in media sessions defined with the AVPF profile and must also be included in sessions supporting TMMBR; otherwise, the call is rejected.

VoIPerfect supports two modes of operation, where the Access SBC can be configured to support both modes and each Enterprise SBC serviced by the Access SBC can be configured to support one of the modes:

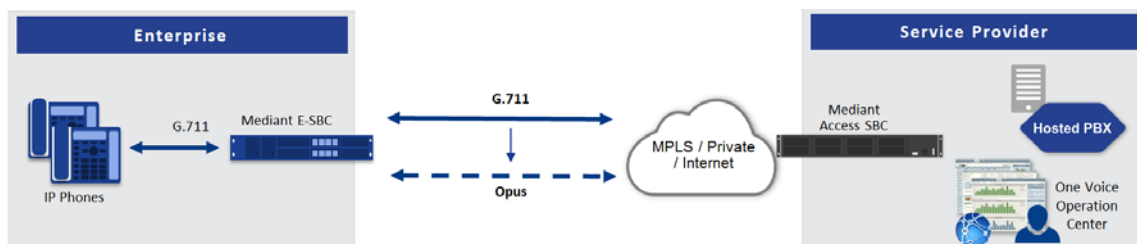
- **Managed Opus:** If the SBC detects WAN network impairments during a call using the Opus coder between the Enterprise SBC and Access SBC, it can adjust the Opus coder's attributes (e.g., bit rate) for that specific call to ensure high voice quality is maintained. The advantage of the Opus coder is that its' bit rate can change dynamically according to bandwidth availability. This mode is useful for unstable networks, allowing Opus to dynamically adapt to adverse network conditions.



Configuration of the Enterprise SBC:

- Coders Group with Opus
- Allowed Audio Coders Group with Opus
- IP Profile:
 - ◆ Extension Coders Group: Coders Group with Opus
 - ◆ Allowed Audio Coders: Allowed Audio Coders Group with Opus
 - ◆ Allowed Coders Mode: Restriction
 - ◆ Voice Quality Enhancement: Enable
 - ◆ RTCP Feedback: Feedback On
 - ◆ Max Opus Bandwidth: 0

- **Smart Transcoding:** If the SBC (Enterprise or Access) detects WAN network impairments during a call between the Enterprise SBC and Access SBC, the SBC employs voice transcoding by switching the coder from G.711 to Opus for that specific call only. Transcoding is done only on the path between the Enterprise SBC and Access SBC. As Smart Transcoding is applied only on a per call basis, it preserves valuable DSP resources that may be required for other functionalities. An advantage of using the Opus coder is that it consumes less bandwidth than G.711 and overcomes packet loss (by dynamic packet redundancy), allowing the SBC to support more concurrent calls than with G.711 for the same bandwidth. This mode is useful for WAN networks that are relatively stable, allowing the use of G.711 whenever possible and switching to Opus only during adverse network conditions.



Configuration of the Enterprise SBC:

- Device's License Key includes the SBC transcoding feature
- Coder Groups (see Configuring Coder Groups on page 379):
 - ◆ Coders Group with G.711
 - ◆ Coders Group with Opus
- Allowed Audio Coders Groups (see Configuring Allowed Audio Coder Groups on page 384):
 - ◆ Allowed Audio Coders Group with G.711
 - ◆ Allowed Audio Coders Group with Opus
- Main IP Profile (see Configuring IP Profiles on page 388):
 - ◆ Extension Coders Group: Coders Group with G.711
 - ◆ Allowed Audio Coders: Allowed Audio Coders Group with G.711

- ◆ Allowed Coders Mode: Restriction
- ◆ RTCP Feedback: Feedback On
- ◆ Voice Quality Enhancement: Enable
- Alternative IP Profile:
 - ◆ Extension Coders Group: Coders Group with Opus
 - ◆ Allowed Audio Coders: Allowed Audio Coders Group with Opus
 - ◆ Allowed Coders Mode: Restriction
 - ◆ RTP Redundancy Mode: Enable
 - ◆ RTCP Feedback: Feedback On
 - ◆ Voice Quality Enhancement: Enable
 - ◆ Max Opus Bandwidth: 80000
- Quality of Service Rules (see Configuring Quality of Service Rules on page 300):
 - ◆ Rule Metric: Poor InVoice Quality
 - ◆ Alternative IP Profile Name: name of Alternative IP Profile (above)

Configuration of the Access SBC for both methods:

- Coder Groups:
 - Coders Group with G.711 and Opus
 - Coders Group with Opus
- Allowed Audio Coders Group with Opus
- IP Profile:
 - Extension Coders Group: Coders Group with G.711 and Opus
 - Voice Quality Enhancement: Enable
 - RTP Redundancy Mode: Enable
 - RTCP Feedback: Feedback On
 - Max Opus Bandwidth: 0
- Alternative IP Profile:
 - Extension Coders Group: Coders Group with Opus
 - Allowed Audio Coders: Allowed Audio Coders Group with Opus
 - Allowed Coders Mode: Restriction
 - Voice Quality Enhancement: Enable
 - RTP Redundancy Mode: Enable
 - RTCP Feedback: Feedback On
 - Max Opus Bandwidth: 0
- Quality of Service Rules (see Configuring Quality of Service Rules on page 300):
 - Rule Metric: Poor InVoice Quality
 - Alternative IP Profile Name: name of Alternative IP Profile (above)

**Note:**

- VoIPerfect is applicable only to G.711 calls.
- If you are deploying a third-party device between the Enterprise SBC and Access SBC, make sure that the third-party device adheres to the following:
 - ✓ Enable RFC 2198 in SDP negotiation
 - ✓ Enable TMMBR in SDP negotiation
 - ✓ Forward the SDP with feedback (SAVPF) as is
 - ✓ Forward TMMBR messages as is
 - ✓ Forward RTCP messages as is (not terminate them)
 - ✓ (Smart Transcoding only) Forward re-INVITE messages for using Opus as is
 - ✓ (Smart Transcoding only) Forward the SIP header, X-Ac-Action as is

This page is intentionally left blank.

Part VI

Cloud Resilience Package

31 CRP Overview

The device's Cloud Resilience Package (CRP) application enhances cloud-based or hosted communications environments by ensuring survivability, high voice quality and security at enterprise branch offices and cloud service customer premises. CRP is designed to be deployed at customer sites and branches of:

- Cloud-based and hosted communications
- Cloud-based or hosted contact-center services
- Distributed PBX or unified communications deployments

The CRP application is based on the functionality of the SBC application, providing branch offices with call routing and survivability support. CRP is implemented in a network topology where the device is located at the branch office, routing calls between the branch users, and/or between the branch users and other users located elsewhere (at headquarters or other branch offices), through a hosted server (IP PBX) located at the Enterprise's headquarters. The device maintains call continuity even if a failure occurs in communication with the hosted IP PBX.



Note:

- The CRP application is applicable only to Mediant VE SBC.
- The CRP application is available only if the device is installed with a License Key that includes this feature. For installing a License Key, see "License Key" on page 597.
- For the maximum number of supported CRP sessions and CRP users than can be registered in the device's registration database, see "Technical Specifications" on page 857.

For cloud providers, CRP ensures uninterrupted communications in the event of lost connection with the cloud providers' control systems. For distributed enterprises and contact centers, CRP is an essential solution for enterprises deploying geographically distributed communications solutions or distributed call centers with many branch offices. CRP ensures the delivery of internal and external calls even when the connection with the centralized control servers is lost.

Table 31-1: Key Features

Survivability	Quality of Experience/Service	Security
<ul style="list-style-type: none"> ■ PSTN fallback ■ WAN redundancy ■ Local mode ■ High availability ■ Emergency calling (E911) ■ Basic call routing between registering users and device, or any other route to responding server ■ Short number dialog (short numbers are learned dynamically in the registration process) ■ Survivability indication to IP phone 	<ul style="list-style-type: none"> ■ QoE monitoring ■ Call Admission Control ■ SLA fulfillment ■ SIP mediation ■ Media transcoding ■ Test call agent 	<ul style="list-style-type: none"> ■ Layer 3 to 7 protection ■ Media encryption ■ Call control encryption ■ NAT traversal ■ Topology hiding

Survivability	Quality of Experience/Service	Security
<ul style="list-style-type: none"> ▪ Call hold and retrieve ▪ Call transfer (if IP phone initiates REFER) ▪ Basic Shared Line Appearance (excluding correct busy line indications) ▪ Call waiting (if supported by IP phone) 		

One of the main advantages of CRP is that it enables quick-and-easy configuration. This is accomplished by its pre-configured routing entities, whereby only minimal configuration is required. For example, defining IP addresses to get the device up and running and deployed in the network.

32 CRP Configuration

This section describes configuration specific to the CRP application. As CRP has similar functionality to the SBC application, for configuration that is common to the SBC, which is not covered in this section, see the following SBC sections:

- "Configuring Admission Control" on page 457
- "Configuring Allowed Audio Coder Groups" on page 384
- "Configuring Classification Rules" on page 461
- "Configuring Message Condition Rules" on page 469
- "Configuring SBC IP-to-IP Routing Rules" on page 470
- "Configuring SIP Response Codes for Alternative Routing Reasons" on page 482
- "Configuring IP-to-IP Inbound Manipulations" on page 493
- "Configuring IP-to-IP Outbound Manipulations" on page 497



Note: The main difference in the common configuration between the CRP and SBC applications is the navigation menu paths to opening these Web configuration pages. Wherever "SBC" appears in the menu path, for the CRP application it appears as "CRP".

32.1 Enabling the CRP Application

Before you can start configuring the CRP, you must first enable the CRP application. Once enabled, the Web interface displays the menus and parameter fields relevant to the CRP application.



Note: The CRP feature is available only if the device is installed with a License Key that includes this feature. For installing a License Key, see "License Key" on page 597.

➤ **To enable the CRP application:**

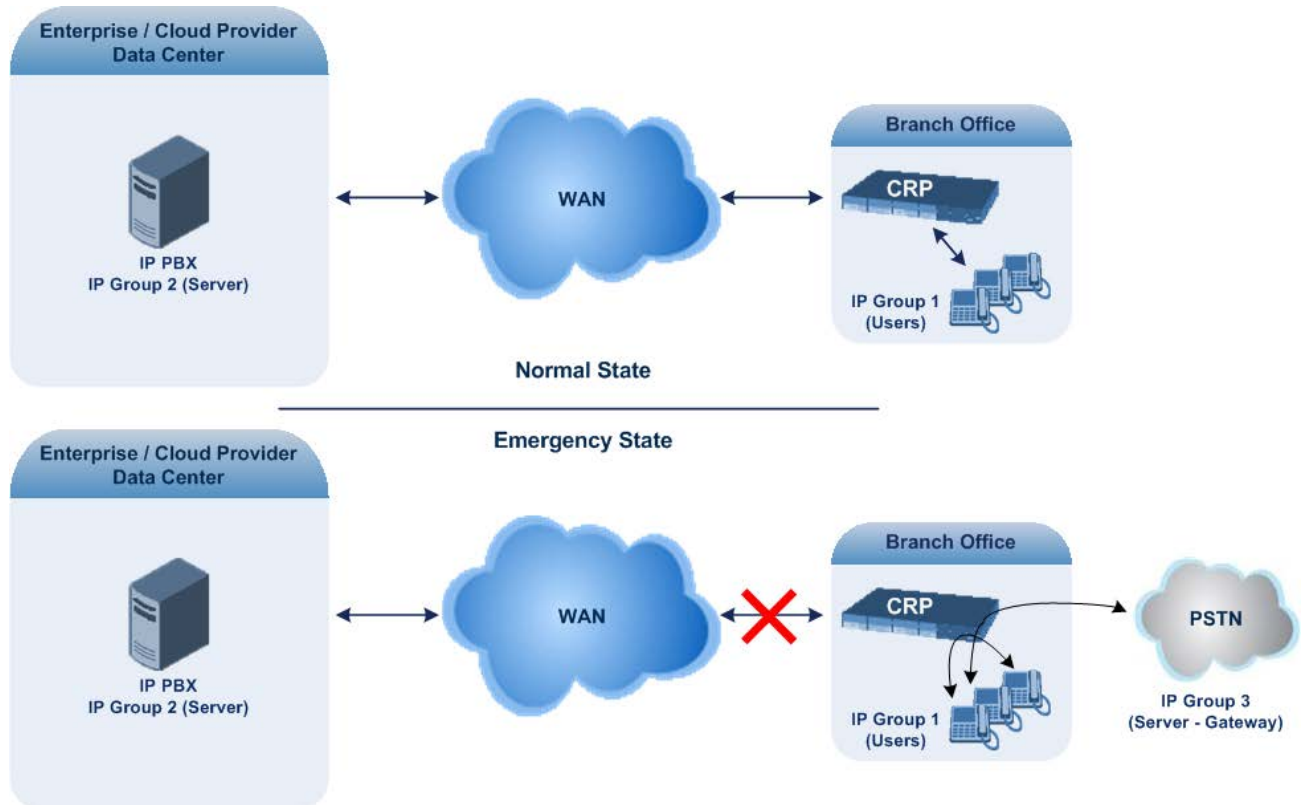
1. Open the Applications Enabling page (**Setup** menu > **Signaling & Media** tab > **Core Entities** folder > **Applications Enabling**).
2. From the 'CRP Application' drop-down list, select **Enable**.
3. Click **Apply**, and then reset the device with a save-to-flash for your settings to take effect.

32.2 Configuring Call Survivability Mode

The CRP can be configured to operate in one of the following call survivability modes:

- Normal (Default):** The CRP interworks between the branch users and the IP PBX located at headquarters. The CRP forwards all requests (such as for registration) from the branch users to the IP PBX, and routes the calls based on the IP-to-IP routing rules. If communication with the IP PBX fails (i.e., Emergency mode), it still allows calls between the branch users themselves. If this fails, it routes the calls to the PSTN (if employed).

Figure 32-1: CRP in Normal & Auto Answer to Registrations Modes



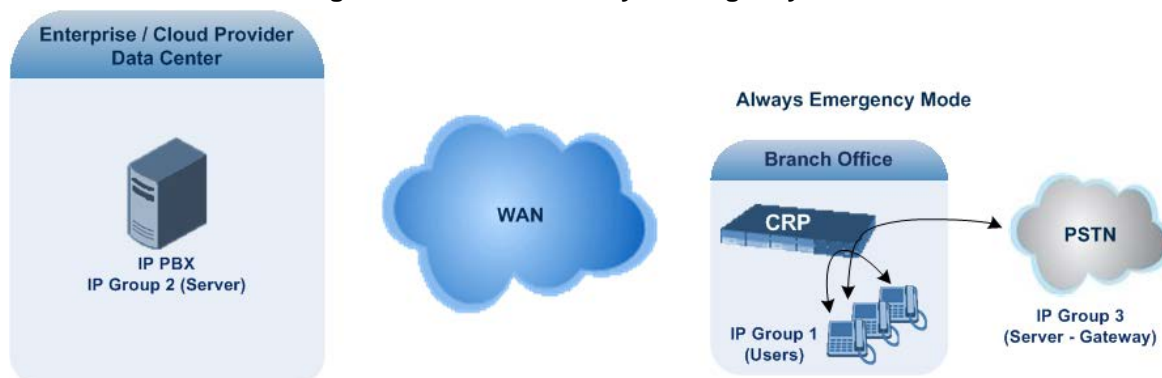
- Auto Answer to Registrations:** This mode is the same as the Normal mode, except that the CRP registers the branch users in its registration database instead of forwarding them to the IP PBX.



Note: SIP REGISTER and OPTIONS requests are terminated at the CRP.

- **Always Emergency:** The CRP routes the calls between the branch users themselves as if connectivity failure has occurred with the IP PBX. The CRP also registers the branch users in its registration database.

Figure 32-2: CRP in Always Emergency Mode



➤ **To configure the Call Survivability mode:**

1. Open the General Settings page (**Setup** menu > **Signaling & Media** tab > **CRP** folder > **CRP General Settings**).
2. From the 'CRP Survivability Mode' drop-down list, select the required mode.
3. Click **Apply**.

32.3 Pre-Configured IP Groups

For CRP, the device is pre-configured with the following IP Groups in the IP Groups table:

Table 32-1: Pre-configured IP Groups in the IP Groups Table

Index	Type	Description
1	User	Users
2	Server	Proxy
3	Server	Gateway

These IP Groups represent the following IP entities:

- **"Users" IP Group:** LAN users (e.g., IP phones) at the branch office
- **"Server" IP Group:** Server (e.g., hosted IP PBX at the Enterprise's headquarters)
- **"Gateway" IP Group:** Device's interface with the PSTN

These IP Groups are used in the IP-to-IP routing rules to indicate the source and destination of the call (see "Pre-Configured IP-to-IP Routing Rules" on page 550).



Note:

- These IP Groups cannot be deleted and additional IP Groups cannot be configured. The IP Groups can be edited, except for the fields listed above, which are read-only.
- For accessing the IP Groups table and for a description of its parameters, see "Configuring IP Groups" on page 329.

32.4 Pre-Configured IP-to-IP Routing Rules

For the CRP application, the IP-to-IP Routing table is pre-configured with IP-to-IP routing rules. These rules depend on the configured Call Survivability mode, as described in "Configuring Call Survivability Mode" on page 547.



Note:

- The IP-to-IP Routing table is read-only.
- For accessing the IP-to-IP Routing table and for a description of its parameters, see "Configuring SBC IP-to-IP Routing Rules" on page 470.

32.4.1 Normal Mode

The pre-configured IP-to-IP routing rules for the Normal CRP call survivability mode are shown in the table below:

Table 32-2: Pre-Configured IP-to-IP Routing Rules for CRP Normal Mode

Index	Source IP Group / Emergency	Request Type	Destination Type	Destination IP Group	Destination Address	Alternative Route Options
1	*	OPTIONS	Dest Address	-	Internal	Route Row
3	1	All	IP Group	2	-	Route Row
4	1	All	IP Group	1	-	Alternative
5	1	All	IP Group	3	-	Alternative
6	2	All	IP Group	1	-	Route Row
7 ¹	2	All	IP Group	3	-	Route Row
8	3	All	IP Group	2	-	Route Row
9	3	All	IP Group	1	-	Alternative

Note:

1. Index 7 appears only if the CRPGatewayFallback parameter is enabled (see "Configuring PSTN Fallback" on page 552). This routing rule is used if the device can't find a matching destination user for IP Group 1 (User-type IP Group) in its registration database. If the CRPGatewayFallback parameter is disabled and no matching user is found, the device rejects the call.

32.4.2 Emergency Mode

The pre-configured IP-to-IP routing rules for the Emergency CRP call survivability mode are shown in the table below:

Table 32-3: Pre-Configured IP-to-IP Routing Rules for Emergency Mode

Mode	Index	Source IP Group ID / Emergency	Request Type	Destination Type	Destination IP Group ID	Destination Address	Alternative Route Options
Always Emergency	1	*	OPTIONS	Dest Address	-	Internal	Route Row
	4	1	All	IP Group	1	-	Route Row
	5	1	All	IP Group	3	-	Alternative
	9	3	All	IP Group	1	-	Route Row

32.4.3 Auto Answer to Registrations

The pre-configured IP-to-IP routing rules for the Auto Answer to Registrations CRP call survivability mode are shown in the table below:

Table 32-4: Pre-Configured IP-to-IP Routing Rule for Auto Answer to Registrations Mode

Mode	Index	Source IP Group	Request Type	Destination Type	Destination IP Group	Destination Address	Alternative Route Options
Auto Answer to Registrations	1	*	OPTIONS	Dest Address	-	Internal	Route Row
	2 ¹	*	REGISTER	IP Group	-2	-	Route Row
	3	1	All	IP Group	2	-	Route Row
	4	1	All	IP Group	1	-	Alternative
	5	1	All	IP Group	3	-	Alternative
	6	2	All	IP Group	1	-	Route Row
	7 ²	2	All	IP Group	3	-	Route Row
	8	3	All	IP Group	2	-	Route Row
	9	3	All	IP Group	1	-	Alternative

Note:

1. For the routing rule of Index 2, the destination is the source IP Group (i.e., from where the REGISTER message was received).
2. Index 7 appears only if the CRPGatewayFallback parameter is enabled (see "Configuring PSTN Fallback" on page 552).

32.5 Configuring PSTN Fallback

You can enable the CRP to route emergency calls (or PSTN-intended calls) such as "911" from the Proxy server (IP Group 2) to the PSTN (IP Group 3). In addition, for calls from the Proxy server to Users (IP Group 1), the device searches for a matching user in its Users Registration database and if not located, it sends the call to the PSTN (IP Group 3), as an alternative route.

To enable this feature, set the ini file parameter CRPGatewayFallback to 1. When enabled, the alternative routing rule appears immediately below the IP Group 2 to IP Group 1 rule in the IP-to-IP Routing table.

**Note:**

- Enabling this feature (this routing rule) may expose the device to a security "hole", allowing calls from the WAN to be routed to the Gateway. Thus, configure this feature with caution and only if necessary.
- This PSTN routing rule is not an alternative routing rule. In other words, if a match for a user is located in the database, this PSTN rule will never be used regardless of the state of the user endpoint (e.g., busy).

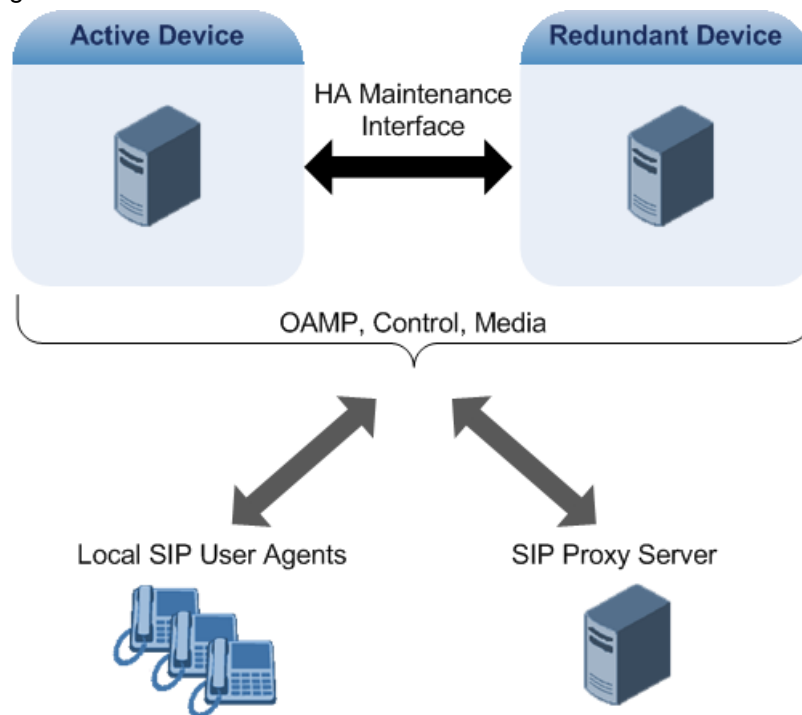
Part VII

High Availability System

33 HA Overview

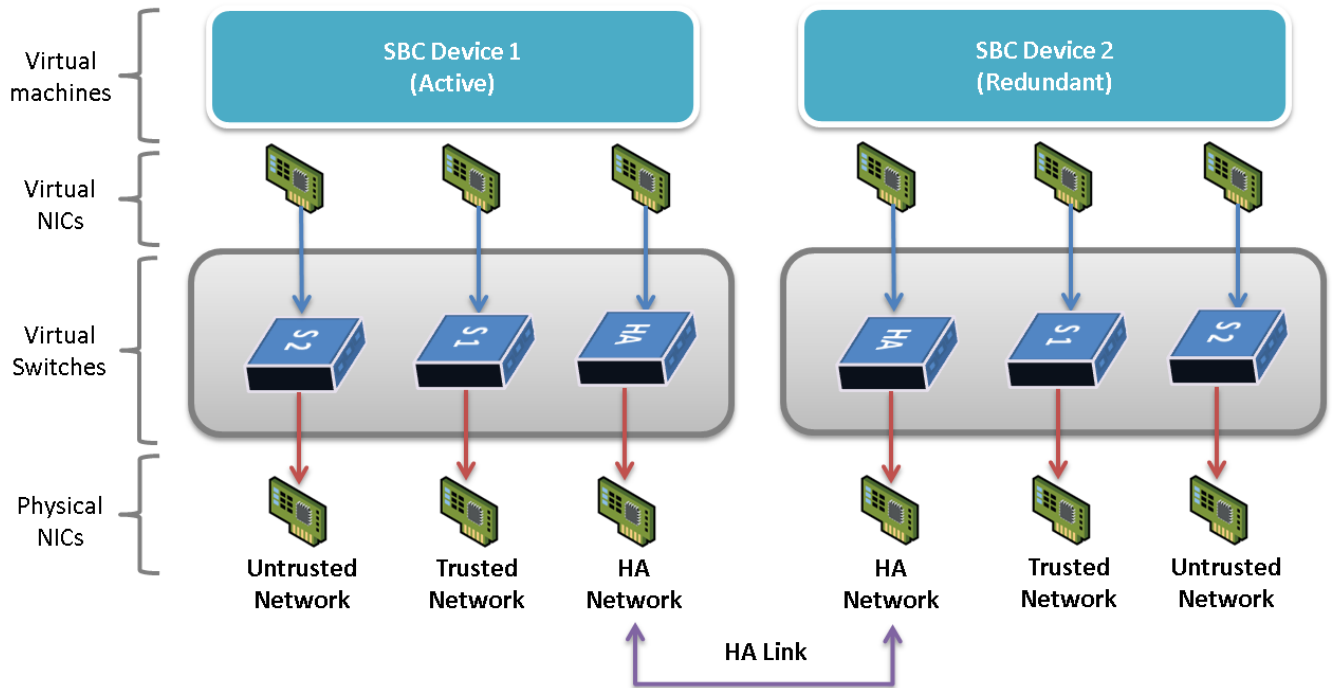
The device's High Availability (HA) feature provides 1+1 system redundancy using two Mediant Software E-SBC devices. If failure occurs in the active device, a switchover occurs to the redundant device which takes over the call handling process. Thus the continuity of call services is ensured. All active 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.



The figure below shows two Virtual Machines -- Mediant VE SBCs -- running on different servers to work in an HA configuration:

Figure 33-1: Mediant VE SBC HA - Virtual Network Setup



Note: The physical NICs used by the Mediant SBC VE virtual machine must not share traffic with other applications such as other virtual machines or the hypervisor itself. This also applies to the physical NICs used for the HA link because overloading these NICs may cause false switchovers

33.1 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. This ensures that the two units are synchronized regarding configuration and software.



Note: If the active unit runs an earlier version (e.g., 7.0) than the redundant unit (e.g., 7.2), the redundant unit is downgraded to the same version as the active unit (e.g., 7.0).

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.

33.2 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 Preempt mode:

- **Enabled:** The Preempt mode specifies one of the device's as the "preferred" device. This is done by assigning different priority levels (1 to 10, where 1 is the lowest) to the two devices. Typically, you would configure the active device with a higher priority level (number) than the redundant device. The only factor that influences the configuration is which device has the greater number; the actual number is not important. For example, configuring the active with 5 and redundant with 4, or active with 9 and redundant with 2 both assign highest priority to the active device. 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, Preempt mode is disabled. Please see note below when using priority level 10.
- **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 Preempt 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 Preempt 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, 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.

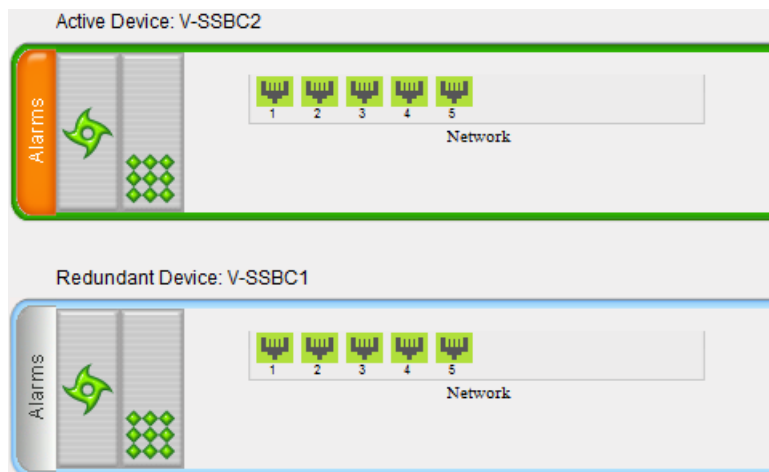


Note:

- Switchover triggered by loss of physical connectivity in one or more Ethernet Group is not done if the active device has been configured to a Preempt mode level of 10. In such a scenario, the device remains active.
- After HA switchover, the active device updates other hosts in the network about the new mapping of its Layer-2 hardware address to the global IP address, by sending a broadcast gratuitous Address Resolution Protocol (ARP) message.

33.3 Viewing HA Status on Monitor Web Page

You can view the status of the HA system on the Monitor page of the device's Web interface. The page provides a graphical display of both active and redundant devices, as shown below:



You can distinguish between active and redundant devices as follows:

- **Active device:**
 - Color of border surrounding device is green.
 - Title above device is "Active Device". The default name is "Device 1".
- **Redundant device:**
 - Color of border surrounding device is blue.
 - Title above device is "Redundant Device". The default name is "Device 2".

The Monitor page also displays the HA operational status of the device to which you are currently logged in. This is displayed in the 'HA Status' field under the Device Information:

- "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

You can change the name of each device, as described in the following procedure:

➤ **To define a name for the device:**

1. Open the HA Settings page (**Setup** menu > **IP Network** tab > **Core Entities** folder > **HA Settings**).
2. In the 'HA Device Name' field, enter a name for the active device.
3. In the 'Redundant HA Device Name' field, enter a name for the redundant device.

Figure 33-2: Configuring Device Names for HA

HA Device Name	• 84
Redundant HA Device Name	86

4. Click **Apply**.



Note: Once the devices are running in HA mode, you can change the name of the redundant device, through the active device only, in the 'Redundant HA Device Name' field.

This page is intentionally left blank.

34 HA Configuration

This section describes HA configuration.

34.1 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.

34.1.1 Network Topology Types and Rx/Tx Ethernet Port Group Settings

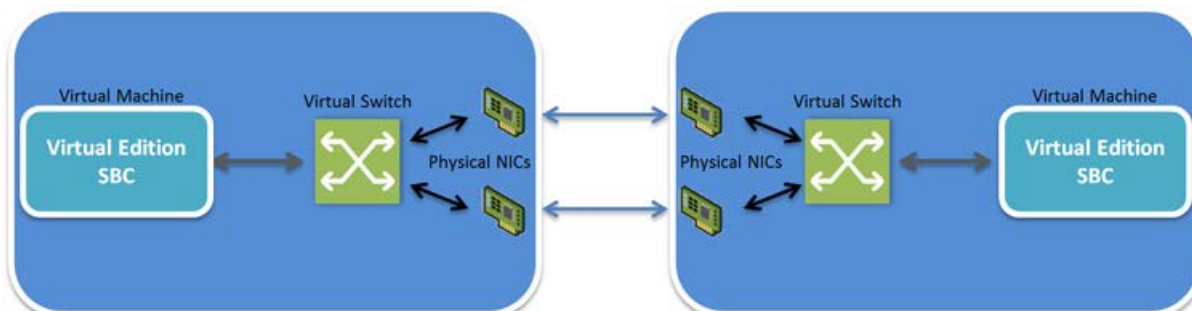
The initial configuration of HA depends on how you want to deploy your HA system in the network. The Maintenance interface, used for the HA link between Active and Redundant units, should be configured on a dedicated Ethernet Device and Ethernet Group (port), separate from the other IP network interfaces. The separation of the Maintenance interface from other interfaces must also be done externally to the units, either by physical separation (i.e., different physical networks) or by logical separation (using VLANs). When using VLANs, make sure that you use a different Ethernet Device for each IP network interface (see "Configuring Underlying Ethernet Devices" on page 128 and "Configuring IP Network Interfaces" on page 130).



Note: If you assign the same Underlying Ethernet Device to all the IP network interfaces, logical separation of traffic may not occur.

The Maintenance interface can employ Ethernet port redundancy (recommended), by using two ports. This is enabled by configuring the Ethernet Group associated with the Maintenance interface with two ports. However, for Mediant Virtual Edition (VE), Ethernet port redundancy is not relevant as the virtual NIC ("port") is logical and always available. Therefore, it is sufficient to configure the Ethernet Group with only one port member. To employ Ethernet port redundancy, you need to configure the virtual switch of the hypervisor for Ethernet port redundancy (or bonding) with the physical NICs. Refer to your hypervisor's support material on how to do this.

Figure 34-1: Connectivity of Maintenance Interfaces for Mediant VE HA

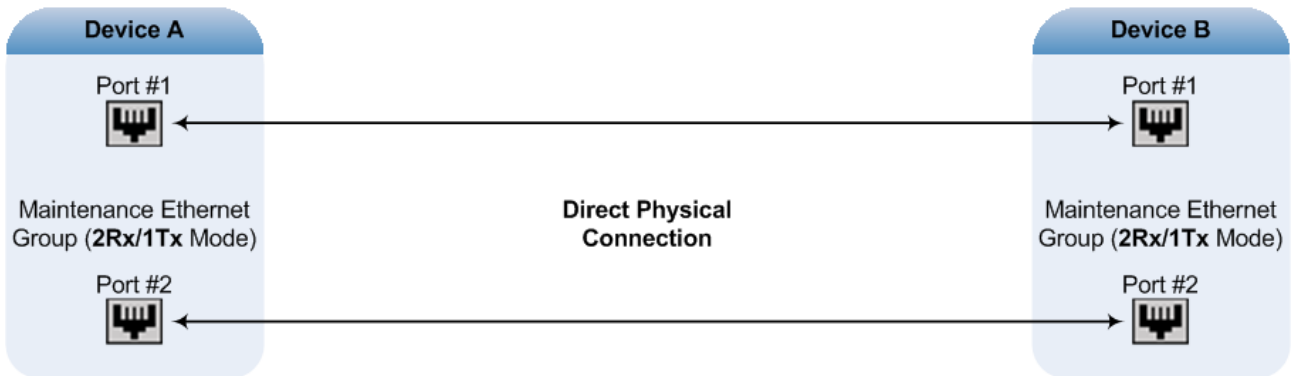


The required receive (Rx) and transmit (TX) mode for the port pair in the Ethernet Group used by the Maintenance interface is as follows (not applicable to Mediant VE):

- (Recommended Physical Connectivity) If the Maintenance ports of both devices are connected directly to each other without intermediation of switches, configure the

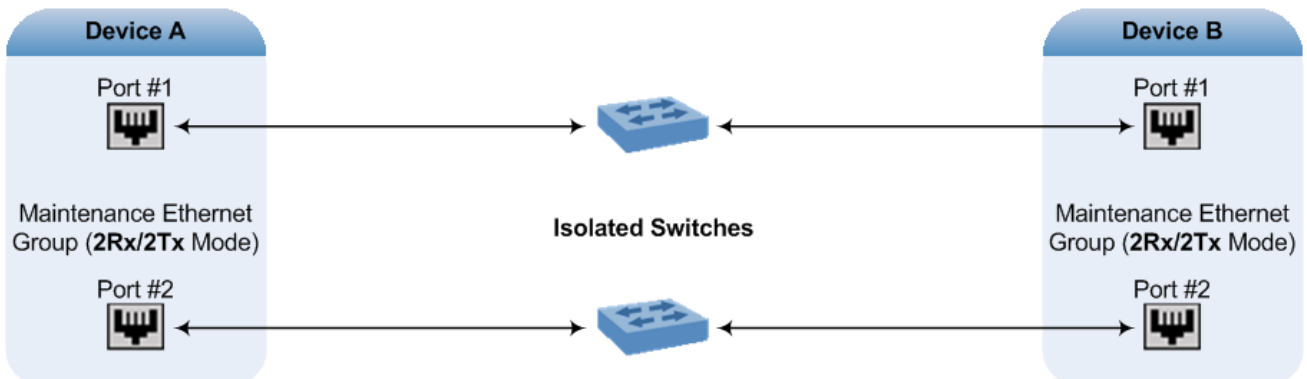
mode to **2RX/1TX**:

Figure 34-2: Rx/Tx Mode for Direct Connection



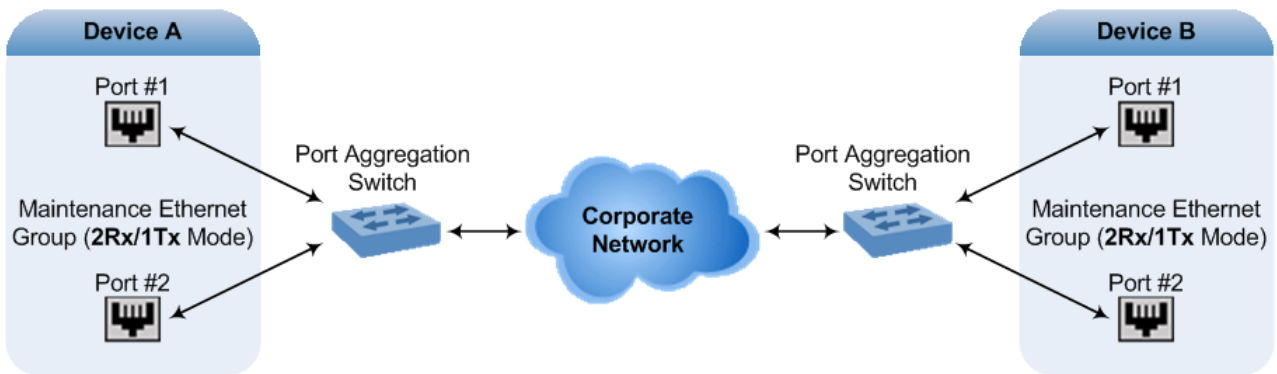
- If the two devices are connected through two (or more) isolated LAN switches (i.e., packets from one switch cannot traverse the second switch), configure the mode to **2RX/2TX**:

Figure 34-3: Redundancy Mode for Two Isolated Switches



- 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 34-4: Rx/Tx Mode for Geographical HA



Note:



- When two LAN switches are used, the LAN switches must be in the same subnet (i.e., broadcast domain).
- To configure Rx/Tx modes of the Ethernet ports, see "Configuring Ethernet Port Groups" on page 126

34.1.2 Configuring the HA Devices

To initially configure the two devices comprising the HA system, do the following procedures listed in chronological order:

1. Configuring the first device for HA (see "Step 1: Configure the First Device" on page 563)
2. Configuring the second device for HA (see "Step 2: Configure the Second Device" on page 565)
3. Activating HA on the devices (see "Step 3: Initialize HA on the Devices" on page 566)



Note:

- The HA feature is available only if both devices are installed with a License Key that includes this feature. For installing a License Key, see "License Key" on page 597.
- 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 Groups and the port numbers belonging to these Ethernet Groups. For example, if the first device uses Ethernet Group 1 (with ports 1 and 2), the second device must also use Ethernet Group 1 (with ports 1 and 2).
- Before configuring HA, determine the required network topology, as described in "Network Topology Types and Rx/Tx Ethernet Port Group Settings" on page 561.
- The Maintenance network should be able to perform a fast switchover in case of link failure and thus, Spanning Tree Protocol (STP) should not be used in this network; the Ethernet connectivity of the Maintenance interface between the two devices should be constantly reliable without any disturbances.

34.1.2.1 Step 1: Configure the First Device

The first stage is to configure the first device for HA, as described in the following procedure:



Note: During this stage, make sure 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:
 - a. If you are already connected to the SBC via keyboard and monitor, change the OAMP parameters to suit your networking scheme through CLI (refer to the Installation Manual).
 - b. Connect to the SBC's Web interface with the newly assigned OAMP IP address.
 - c. Open the IP Interfaces table (see "Configuring IP Network Interfaces" on page 130).
 - d. Configure the Control and Media network interfaces, as required.
 - e. Add the HA Maintenance interface (i.e., the **MAINTENANCE** Application Type).



Note: Make sure that the Maintenance interface uses an Ethernet Device and Ethernet Group that is **not** used by any other IP network interface. The Ethernet Group is associated with the Ethernet Device, which is assigned to the interface.

The IP Interfaces table below shows an example where the Maintenance interface is configured with Ethernet Device "vlan 2" (which is associated with Ethernet Group "GROUP_2"), while the other interface is assigned "vlan 1" (associated with Ethernet Group "GROUP_1"):

Figure 34-5: Configuring MAINTENANCE Interface

INDEX	NAME	APPLICATION TYPE	INTERFACE MODE	IP ADDRESS	PREFIX LENGTH	DEFAULT GATEWAY	PRIMARY DNS	SECONDARY DNS	ETHERNET DEVICE
0	Voice	OAMP + Media	IPv4 Manual	10.8.40.47	16	10.8.0.1	0.0.0.0	0.0.0.0	vlan 1
1	maint	MAINTENANCE	IPv4 Manual	10.3.0.11	16	10.3.0.1	0.0.0.0	0.0.0.0	vlan 2

- If the connection is through a switch, the packets of both interfaces should generally be untagged. To do this, open the Ethernet Devices table (see "Configuring Underlying Ethernet Devices" on page 128), and then configure the 'Tagging' parameter to **Untagged** for the Ethernet Device assigned to the Maintenance interface. The figure below shows an example (highlighted) where VLAN 2 is configured as the Native (untagged) VLAN ID of the Ethernet Group "GROUP_2":

Figure 34-6: Configuring Untagged VLAN for Maintenance and Other Interfaces

INDEX	VLAN ID	UNDERLYING INTERFACE	NAME	TAGGING
0	1	GROUP_1	vlan 1	Untagged
1	2	GROUP_2	vlan 2	Untagged

- Set the Ethernet port Tx / Rx mode of the Ethernet Group used by the Maintenance interface (see "Configuring Ethernet Port Groups" on page 126). The port mode depends on the type of Maintenance connection between the devices, as described in "Network Topology Types and Rx/Tx Ethernet Port Group Settings" on page 561. For Mediant VE, the Tx / Rx mode is 1 RX / 1 TX as the Ethernet Group is configured with only a single port (for more information, see Network Topology Types and Rx/Tx Ethernet Port Group Settings on page 561).
- Configure HA parameters:
 - Open the HA Settings page (**Setup** menu > **IP Network** tab > **Core Entities** folder > **HA Settings**):

Figure 34-7: HA Settings Page

HA Settings

HIGH AVAILABILITY

HA Remote Address ⚡

Preempt Mode ⚡

Preempt Priority ⚡

Redundant HA Priority

Redundant HA Device Name

- In the 'HA Remote Address' field, enter the Maintenance IP address of the **second** device.

- c. (Optional) Enable the HA Preempt feature by configuring the 'Preempt Mode' parameter to **Enable**, and then setting the priority level of the device in the 'Preempt Priority' field. Make sure that you configure different priority levels for the two devices. Typically, you would configure the active device with a higher priority level (number) than the redundant device. The only factor that influences the configuration is which device has the greater number; the actual number is not important. For example, configuring the active with 5 and redundant with 4, or active with 9 and redundant with 2 both assign highest priority to the active device. Configuring the level to 10 does not cause a switchover upon Ethernet connectivity loss. For more information on the feature, see "Device Switchover upon Failure" on page 557.
5. Burn the configuration to flash **without** a reset.
6. Power down the device.
7. Configure the second device (see "Step 2: Configure the Second Device" on page 565).

34.1.2.2 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 following procedure briefly describes each 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 563).



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 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. The Maintenance interfaces of the devices must be in the same subnet.
 4. Configure the **same** Ethernet Groups and VLAN IDs of the network interfaces as configured for the first device.
 5. Configure the **same** Ethernet port Tx / Rx mode of the Ethernet Group used by the Maintenance interface as configured for the first device.
 6. Configure HA parameters in the HA Settings page:
 - a. In the 'HA Remote Address' field, enter the Maintenance IP address of the **first** device.

- b. (Optional) Enable the HA Preempt feature by configuring the 'Preempt Mode' parameter to **Enable**, and then setting the priority level of the device in the 'Preempt Priority' field. Make sure that you configure different priority levels for the two devices. Typically, you would configure the active device with a higher priority level (number) than the redundant device. The only factor that influences the configuration is which device has the greater number; the actual number is not important. For example, configuring the active with 5 and redundant with 4, or active with 9 and redundant with 2 both assign highest priority to the active device. Configuring the level to 10 does not cause a switchover upon Ethernet connectivity loss. For more information on the HA Preempt feature, see "Device Switchover upon Failure" on page 557.
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 566.

34.1.2.3 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 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 Monitor page displays "Synchronizing" in the 'HA Status' field.

When synchronization completes, 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 Monitor page displays "Operational" in the 'HA Status' field.
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 is Operational" on page 566.

34.2 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: The address is set as the new 'HA Remote Address' value on the redundant device.
 - ◆ Modified 'HA Remote Address' value on the active device: The address is set as the new Maintenance interface address on the redundant device (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.
- 'Preempt Mode' parameter (requires a device reset).
- 'Preempt Priority' parameter is set for the active device.
- Modified 'Redundant Preempt Priority' value is set for the redundant device (requires a device reset).



Note: If the HA system is already in HA Preempt 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).

34.3 Configuring Firewall Allowed Rules

If you have configured firewall rules in the Firewall table (see "Configuring Firewall Rules" on page 157) that block specific traffic, you also need to configure rules that ensure traffic related to HA is allowed:

- 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 transfer (e.g., Rule #7 in the figure below).
- HTTP protocol for file transfer 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, where 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 34-8: 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	Active	0.0.0.0	0	0	80-80	tcp	Enable	O+M+C	0	0	0	ALLOW	248
1	Active	10.31.4.61	669	32	669-669	udp	Enable	HA_IF	0	0	0	ALLOW	921
2	Active	10.31.4.62	669	32	669-669	udp	Enable	HA_IF	0	0	0	ALLOW	0
3	Active	10.31.4.61	0	32	2442-2442	TCP	Enable	HA_IF	0	0	0	ALLOW	57
4	Active	10.31.4.62	2442	32	0-65535	TCP	Enable	HA_IF	0	0	0	ALLOW	0
5	Active	10.31.4.61	2442	32	0-65535	TCP	Enable	HA_IF	0	0	0	ALLOW	0
6	Active	10.31.4.62	0	32	2442-2442	TCP	Enable	HA_IF	0	0	0	ALLOW	0
7	Active	10.31.4.61	80	32	0-65535	TCP	Enable	HA_IF	0	0	0	ALLOW	0
8	Active	10.31.4.62	80	32	0-65535	TCP	Enable	HA_IF	0	0	0	ALLOW	0
9	Not Active	0.0.0.0	0	0	65535	Any	Disable	None	0	0	0	Block	0

34.4 Monitoring IP Entity and HA Switchover upon Ping Failure

The device can monitor a specified network entity, using pings. If the device does not receive a ping response from the entity, a switchover to the redundant device occurs. The switchover happens only if a ping was initially successful and then a subsequent ping failed. The feature is referred to as *HA Network Reachability*. The feature can be used, for example, to check connectivity with a nearby router (first hop) that the device uses to reach other destinations.

The network entity is defined by IP address. The IP interface from where the ping is sent can be selected from one of the device's configured network interfaces in the IP Interfaces table.



Note:

- The HA Network Reachability feature is not functional under the following conditions:
 - ✓ HA is disabled (i.e., active device is in standalone mode).
 - ✓ HA Preempt Priority is used (to prevent endless loops of switchovers).
 - ✓ Number of Ethernet Groups in the redundant device that are in "up" state are less than on the active device (to prevent endless loops of switchovers).
- If you have configured the HA Network Reachability feature, but the feature is not operational (see note above), the device sends the SNMP trap event, acHANetworkWatchdogStatusAlarm to notify of the situation.
- If a switchover occurs due to no ping reply, the device sends the SNMP trap alarm, acHASystemFaultAlarm to notify of the switchover due to the HA Network Reachability feature.
- For a detailed description of the HA ping parameters, see "HA Parameters" on page 764.

➤ **To configure monitoring of IP entity using pings:**

1. Open the HA Settings page (**Setup** menu > **IP Network** tab > **Core Entities** folder > **HA Settings**).
2. Configure the following:
 - From the 'HA Network Reachability' (HAPingEnabled) drop-down list, select **Enable**.
 - In the 'Destination Address' field, enter the address of the IP entity that you want to monitor.
 - In the 'Source Interface Name' field, enter the device's IP network interface from where you want to ping the destination entity.
 - In the 'Ping Timeout' field, enter the timeout for which the ping request waits for a response.

- In the 'Ping Retries' field, enter the number of ping requests that the device sends after no ping response is received from the destination, before it considers the destination as unavailable.

Figure 34-9: Configuring HA Network Reachability

NETWORK REACHABILITY	
HA Network Reachability	Disable
Destination Address	::
Source Interface Name	
Ping Timeout [sec]	1
Ping Retries	2

3. Click Apply.

If the feature is operational, the status of the connectivity to the pinged destination is displayed in the 'Monitor Destination Status' read-only field:

- "Enabled": Ping is sent as configured.
- "Disabled by configuration and HA state": HA and ping are not configured.
- "Disabled by HA state": same as above.
- "Disabled by configuration": same as above.
- "Disabled by invalid configuration": invalid configuration, for example, invalid interface name or destination address (destination address must be different than a local address and from the redundant device's Maintenance address).
- "Disabled by HA priority in use": when HA priority is used, ping mechanism is disabled.
- "Disabled by Eth groups error": when the number of Ethernet Groups in the redundant device becomes less than in the active device, the ping mechanism is disabled.
- "Failed to be activated": Internal error (failed activating the ping mechanism).

This page is intentionally left blank.

35 HA Maintenance

This section describes HA maintenance procedures.

35.1 Maintenance of Redundant Device

The only interface that is operational on the redundant device is the Maintenance interface. The following protocols can be used for maintenance purposes for this interface:

- **Syslog:** To receive Syslog messages from the redundant device, make sure that you have configured a valid VLAN and routing rule from the Maintenance network to the Syslog server.
- **Telnet:** A Telnet server is always available on the redundant device (even if disabled by configuration).

The active device runs the above maintenance protocols on its' OAMP interface.

35.2 Replacing a Failed Device

If you need to replace a faulty device, the new device must be configured exactly as the second device, as described in "Configuring the HA Devices" on page 563.

35.3 Initiating an HA Switchover

You can initiate a switchover from the Active to Redundant device.

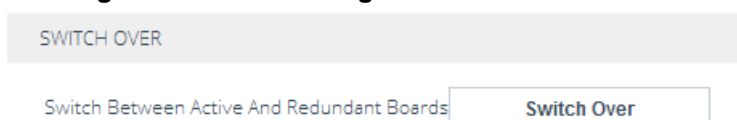


Note: When performing an HA switchover, the HA mode becomes temporarily unavailable.

➤ To perform a switch-over:

1. Open the High Availability Maintenance page:
 - Toolbar: Click the **Actions** button, and then from the drop-down menu, choose **Switchover**.
 - Navigation tree: **Setup** menu > **Administration** tab > **Maintenance** folder > **High Availability Maintenance**.

Figure 35-1: Performing a Device HA Switchover



2. Click **Switch Over**; a confirmation box appears requesting you to confirm.
3. Click **OK**.

35.4 Resetting the Redundant Unit

You can reset the Redundant device, if necessary.

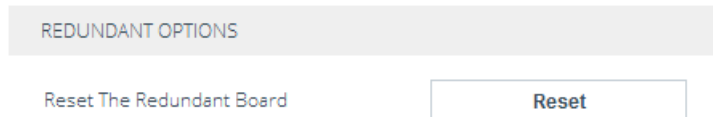


Note: When resetting the Redundant device, the HA mode becomes temporarily unavailable.

➤ **To reset the Redundant device:**

1. Open the High Availability Maintenance page:
 - Toolbar: Click the **Actions** button, and then from the drop-down menu, choose **Switchover**.
 - Navigation tree: **Setup** menu > **Administration** tab > **Maintenance** folder > **High Availability Maintenance**.

Figure 35-2: Resetting Redundant Device



2. click **Reset**; a confirmation box appears requesting you to confirm.
3. Click **OK**.

35.5 Software Upgrade

You can perform the following types of software upgrades 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).

For more information, see "Software Upgrade Wizard" on page 604.

35.6 Rescue Options

The device features a System Snapshots mechanism that provides the capability of returning the system to a previous state. The mechanism may be used as a rescue option if a system malfunction occurs.



Note: For Mediant VE SBC, in addition to the functionality described in this chapter, you can use the snapshots functionality provided by the virtual machine hypervisor.

35.6.1 Taking a Snapshot

Taking a System Snapshot captures a complete state of the device, including:

- Installed software
- Current configuration
- Auxiliary files
- License Key

The first 'factory' snapshot is automatically taken when initial installation is performed. Additional snapshots (up to 10) may be taken. The device can be returned to a snapshot, as described below.

➤ **To take a snapshot in the CLI:**

1. Connect to the CLI interface.
2. At the prompt, type the following and then press Enter:

```
> enable
```
3. At the prompt, type the password and then press Enter:

```
Password: Admin
```
4. At the prompt, type the following to save the current configuration (burn) before creating a snapshot:

```
# write
```
5. Type the following commands to take a snapshot:

```
# configure troubleshoot
# startup-n-recovery
(startup-n-recovery)# create-system-snapshot <name>
```

35.6.2 Viewing Available Snapshots

Currently available system snapshots can be viewed by using the **show-system-snapshots** command. The 'default' snapshot is indicated by an asterisk.

```
(startup-n-recovery)# show-system-snapshots
first-install-2010-01-01_03-18-29
pre-production-6.70.037.010-2010-01-08_00-39-58
*production-6.70.037.010-2010-01-08_00-41-30
```

35.6.3 Changing the Default Snapshot

The 'default' snapshot indicates a restore point that is used by Automatic Recovery in the case of software malfunction (see "Automatic Recovery" on page 576) and/or Manual Recovery (see "Manual Recovery" on page 574). The last user-created snapshot is automatically set as 'default' though it can be changed using the following command:

```
(startup-n-recovery)# set-default-snapshot pre-production-6.70.037.010-2010-01-08_00-40-27
```

35.6.4 Deleting a Snapshot

To delete a snapshot, use the following command:

```
(startup-n-recovery)# delete-system-snapshot pre-production-6.70.037.010-2010-01-08_00-39-58
```

35.6.5 Manual Recovery

You can perform a Manual recovery. When the device reboots, a GRUB menu is displayed that lets you select one of the following rescue options:

- Return to default snapshot
- Fix current installation
- Browse available system snapshots
- Return to factory snapshot (after install from CD)

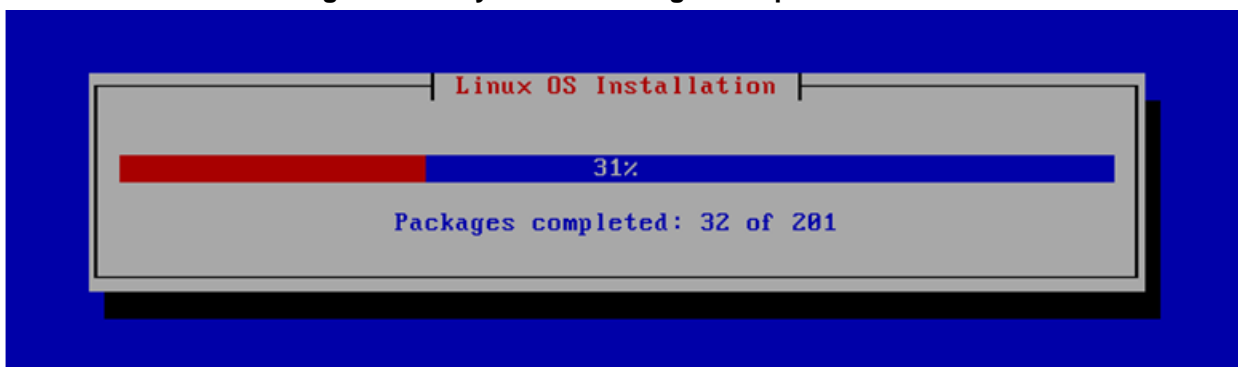
35.6.5.1 Returning to the Default Snapshot

➤ **To return to the default snapshot:**

1. Reboot the server.
2. In the GRUB menu that's displayed for 5 seconds during the server start-up, press the Down ↓ key, select **Rescue option**, and then press Enter.
3. In the Rescue Options menu, select **Return to default snapshot**, and then press Enter.

The system returns to the default snapshot, restoring the software version and the full configuration. The process can take up to 10 minutes to complete.

Figure 35-3: System Returning to Snapshot State



35.6.5.2 Fixing the Current Installation

- **To fix the current installation:**
 - In the GRUB menu, select **Fix current installation**, and then press Enter; the system is repaired while the currently installed software version and its configuration are preserved. The process can take up to 10 minutes to complete.

35.6.5.3 Returning to an Arbitrary Snapshot

- **To return to an arbitrary (non-default) system snapshot:**
 1. In the GRUB menu, select **Browse available system snapshots**, and then press Enter; you're prompted to select a snapshot.
 2. Select a snapshot, and then press Enter; the system returns to the selected snapshot, restores the software version and the full configuration. The process may take up to 10 minutes to complete.

35.6.5.4 Returning to a Factory Snapshot

- **To return to a factory snapshot (after install from CD):**
 - In the GRUB menu, select **Return to factory snapshot (after install from CD)**, and then press Enter; the system returns to the first snapshot automatically taken when initial installation from CD was performed. The process can take up to 10 minutes to complete.

35.6.6 Automatic Recovery

The device activates Automatic Recovery when it encounters a severe software malfunction that prevents it from successfully booting for three subsequent attempts. Automatic Recovery returns the system to the 'default' snapshot and may take up to 10 minutes to complete.

Part VIII

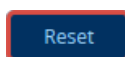
Maintenance

36 Basic Maintenance

This section describes basic maintenance procedures.

36.1 Resetting the Device

You can reset the device through the device's management tools. Device reset may be required for maintenance purposes. Certain parameters require a device reset for their settings to take effect. These parameters are displayed in the Web interface with the lightning ⚡ symbol. In addition, whenever you do any configuration change that requires a reset, the **Reset** button on the Web interface's toolbar is displayed with a red border, as shown below:



The Web interface also provides you with the following options when resetting the device:

- Save current configuration to the device's flash memory (non-volatile) prior to reset
- Reset the device only after a user-defined time (*Graceful Shutdown*) to allow current calls to end (calls are terminated after this interval)

To reset the device (and save configuration to flash) through CLI, use the following command:

```
# reset now
```

➤ To reset the device through Web interface:

1. Open the Maintenance Actions page:
 - Toolbar: Click the **Reset** button.
 - Navigation tree: **Setup** menu > **Administration** tab > **Maintenance** folder > **Maintenance Actions**.

Figure 36-1: Resetting the Device

2. From the 'Save To Flash' drop-down list, select one of the following:
 - **Yes:** Current configuration is saved (*burned*) to flash memory prior to reset (default).
 - **No:** The device resets without saving the current configuration to flash. All configuration done after the last configuration save will be discarded (lost) after reset.
3. From the 'Graceful Option' drop-down list, select one of the following:
 - **Yes:** Reset starts only after a user-defined time, configured in the 'Shutdown Timeout' field (see next step). During this interval, no new traffic is accepted. If no traffic exists and the time has not yet expired, the device resets immediately.
 - **No:** Reset begins immediately, regardless of traffic. Any existing traffic is immediately terminated.

4. In the 'Shutdown Timeout' field (available only if the 'Graceful Option' field is configured 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.
6. Click **OK** to confirm device reset; if the 'Graceful Option' field is configured 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 to notify you.

36.2 Remotely Resetting Device using SIP NOTIFY

The device can be remotely reset upon the receipt of a SIP NOTIFY that contains an Event header that is set to 'check-sync;reboot=true' (proprietary to AudioCodes), 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 Gateway Advanced Settings page (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Gateway Advanced Settings**).
2. From the 'Remote Management by Notify' (EnableSIPRemoteReset) drop-down list, select **Enable**:

Figure 36-2: Resetting Device by SIP NOTIFY

Remote Management by SIP Notify • ▼

3. Click **Apply**.

36.3 Locking and Unlocking the Device

You can lock the device so that it doesn't accept any new calls, maintaining only current calls. This may be useful, for example, when 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:
 - Toolbar: Click the **Reset** button.
 - Navigation tree: **Setup** menu > **Administration** tab > **Maintenance** folder > **Maintenance Actions**.

Figure 36-3: Locking and Unlocking the Device

The screenshot shows a configuration interface for locking and unlocking the device. At the top, there is a header 'LOCK / UNLOCK'. Below this, there are several fields and buttons:

- A 'Lock' button.
- A 'Graceful Option' dropdown menu currently set to 'Yes'.
- A 'Lock Timeout [sec]' text input field containing the value '0'.
- A 'Gateway Operational State' read-only field displaying 'UNLOCKED'.

2. From the 'Graceful Option' drop-down list, select one of the following options:
 - **Yes:** The device is locked only after a user-defined time, configured in the 'Lock Timeout' field (see next step). During this interval, no new traffic is accepted. If no traffic exists and the time has not yet expired, the device locks immediately.
 - **No:** The device is locked regardless of traffic. Any existing traffic is terminated immediately.

Note: These options are available only if the current status of the device is in "UNLOCKED" state.

3. If you configured 'Graceful Option' to **Yes** (see previous step), then in the 'Lock Timeout' field, enter the time (in seconds) after which the device locks.
4. Click the **LOCK** button; a confirmation message box appears requesting you to confirm device lock.
5. Click **OK** to confirm; if you configured 'Graceful Option' to **Yes**, a lock icon is displayed and a window appears displaying the number of remaining calls and time. If you configured 'Graceful Option' to **No**, the lock process begins immediately. The 'Gateway Operational State' read-only field displays "LOCKED" and the device does not process any calls.

➤ To unlock the device:

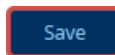
- Click the **UNLOCK** button; the device unlocks immediately and accepts new incoming calls. The 'Gateway Operational State' read-only field displays "UNLOCKED".

36.4 Saving Configuration

When you configure parameters and tables in the Web interface and then click the **Apply** button on the pages in which the configurations are done, changes are saved to the device's *volatile* memory (RAM). These changes revert to their previous settings if the device subsequently resets (hardware or software) or powers down. Therefore, to ensure that your configuration changes are retained, you must save them to the device's non-volatile memory (i.e., flash memory).

To save your settings to flash, click the **Save** button located on the toolbar. To remind you to save your settings to flash, the **Save** button is displayed with a red border, as shown below:

Figure 36-4: Saving Configuration to Flash



To save configuration to flash through CLI, use the following command:

```
# write
```



Note: Saving configuration to flash 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 581).

37 Channel Maintenance

This chapter describes various channel-related maintenance procedures.

37.1 Disconnecting Active Calls

You can forcibly disconnect all active calls, or disconnect specific calls based on Session ID.

➤ **To disconnect calls through CLI:**

- Disconnect all active calls:

```
# clear voip calls
```

- Disconnect active calls belonging to a specified Session ID:

```
# clear voip calls <Session ID>
```

This page is intentionally left blank.

38 Software Upgrade

This chapter describes various software update procedures.

38.1 Auxiliary Files

You can load various Auxiliary files to the device. Auxiliary files provide the device with additional configuration. The table below lists the different types of Auxiliary files.

Table 38-1: 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 through ini file. For more information, see "INI File-Based Management" on page 91.
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 587.
Prerecorded Tones	The Prerecorded Tones (PRT) file enhances the device's capabilities of playing a wide range of telephone exchange tones that cannot be defined in the CPT file. For more information, see "Prerecorded Tones File" on page 590.
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 591.
User Info	The User Information file maps PBX extensions to IP numbers. The 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 593.
AMD Sensitivity	Answer Machine Detector (AMD) Sensitivity file containing the AMD Sensitivity suites. For more information, see AMD Sensitivity File on page 597.

38.1.1 Loading Auxiliary Files

You can load Auxiliary files to the device using one of the following methods:

- Web interface - see "Loading Auxiliary Files through Web Interface" on page 586
- CLI - see Loading Auxiliary Files through CLI on page 587
- TFTP - see Loading Auxiliary Files through ini File using TFTP
- EMS (Software Manager) – refer to the *EMS User's Manual*



Note:

- You can automatically load Auxiliary files from a remote server using the device's Automatic Update mechanism (see Automatic Update Mechanism).
- Saving Auxiliary files 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 581.

38.1.1.1 Loading Auxiliary Files through Web Interface

The following procedure describes how to load Auxiliary files through the Web interface.



Note:

- When loading an ini file through the Auxiliary Files page (as described in this section), only parameter settings specified in the ini file are applied to the device; all other parameters remain at their current settings.
- If you load an ini file containing Auxiliary file(s), the Auxiliary files specified in the file overwrite the Auxiliary files currently installed on the device.

➤ **To load Auxiliary files through Web interface:**

1. Open the Auxiliary Files page:

- Toolbar: From the **Actions** drop-down menu, choose **Auxiliary Files**.
- Navigation tree: **Setup** menu > **Administration** tab > **Maintenance** folder > **Auxiliary Files**.

INI file (incremental)

Browse...

No file selected.


Load File

Voice Prompts file

Browse...

No file selected.

Load File

 **Call Progress Tones file**

Browse...

No file selected.

Load File

Prerecorded Tones file

Browse...

No file selected.

Load File

Dial Plan file

Browse...

No file selected.

Load File

2. Click the **Browse** button corresponding to the Auxiliary file type that you want to load, navigate to the folder in which the file is located, and then click **Open**; the name of the file appears next to the **Browse** button.
3. Click the corresponding **Load File** button.
4. Repeat steps 2 through 3 for each file you want to load.
5. Reset the device with a save-to-flash for your settings to take effect (if you have loaded a Call Progress Tones file).

38.1.1.2 Loading Auxiliary Files through CLI

You can load Auxiliary files from remote servers through CLI:

- **Single Auxiliary file:**

```
# copy <file> from <URL of remote server>
```

For example:

```
# copy call_progress_tones from
http://192.169.11.11:80/cpt_us.dat
```

- **Multiple (batch) Auxiliary files:** The Auxiliary files must be contained in a TAR (Tape ARchive) file (.tar). The TAR file can contain any number and type of Auxiliary files (e.g., Dial Plan file and CPT file).

```
# copy aux-package from | to <URL of remote server with TAR
file name>
```

For example:

```
# copy aux-package from http://192.169.11.11:80/aux_files.tar
```

For more information on CLI, refer to the *CLI Reference Guide*.

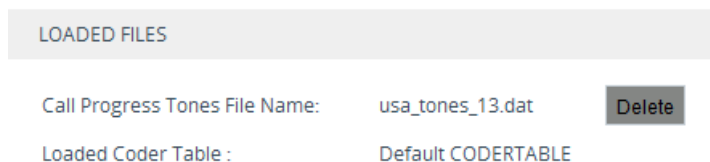
38.1.2 Deleting Auxiliary Files

You can delete loaded Auxiliary files through the Web interface, as described below.

- **To delete a loaded Auxiliary file:**

1. Open the Device Information page (see "Viewing Device Information" on page 637); the loaded files are listed under the Loaded Files group:

Figure 38-1: List of Loaded Auxiliary Files



2. Click the **Delete** button corresponding to the file that you want deleted; a confirmation message box appears.
3. Click **OK** to confirm.
4. Reset the device with a save-to-flash for your settings to take effect.

38.1.3 Call Progress Tones File

The Call Progress Tones (CPT) Auxiliary file contains definitions of the CPT (levels and frequencies) that are detected and 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 *dat* file format, using AudioCodes DConvert utility. For more information, refer to the *DConvert Utility User's Guide*.



Note: The CPT file can only be loaded in .dat file format.

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, the 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, the parameter defines the off time required after the burst tone ends and the tone detection is reported. For continuous tones, the 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.



Note:

- 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.

Below shows an example of a configured dial tone to 440 Hz only:

```
[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
    
```

38.1.4 Prerecorded Tones File

The Prerecorded Tone (PRT) is a .dat file containing a set of prerecorded tones that can be played by the device. For example, it can be used to play music on hold (MoH) to a call party that has been put on hold. Up to 40 tones (totaling approximately 10 minutes) can be stored in a single PRT file on the device's flash memory.

The PRT file overcomes the limitations of the CPT file such as limited number of predefined tones and limited number of frequency integrations in one tone. If a specific prerecorded tone exists in the PRT file, it overrides the same tone that exists in the CPT file, and is played instead.

You can define a PRT file with multiple tones of the same tone type but with different coders. If one of the tones is defined with the same coder as used in the current call, the device always selects it in order to eliminate the need for using DSP resources. If the coder of the tone is the same as that of the call, DSPs are not required. If they are different, DSPs are required.



Note:

- The PRT file only generates (plays) tones; detection of tones is according to the CPT file.
- The device does not require DSPs for playing tones from a PRT file if the coder defined for the tone is the same as that used by the current call. If the coders are different, the device uses DSPs.
- Local generation of tones is not supported.
- For SBC calls, the PRT file supports only the ringback tone and hold tone.

The prerecorded tones can be created using standard third-party, recording utilities such as Adobe Audition, and then combined into a single file (PRT file) using AudioCodes DConvert utility. For more information, refer to *DConvert Utility User's Guide*.

The raw data files must be recorded with the following characteristics:

- Coders: G.711 A-law or G.711 μ -law (and other coders)
- Rate: 8 kHz
- Resolution: 8-bit
- Channels: mono

The prerecorded tones are played repeatedly. This allows you to record only part of the tone and then play the tone for the full duration. For example, if a tone has a cadence of 2 seconds on and 4 seconds off, the recorded file should contain only these 6 seconds. The device repeatedly plays this cadence for the configured duration. Similarly, a continuous tone can be played by repeating only part of it.

Once created, you need to install the PRT file on the device. This can be done using the Web interface (see "Loading Auxiliary Files" on page 585).

38.1.5 Dial Plan File

The Dial Plan file can be used for various digit mapping features, as described in this section.



Note: The Dial Plan described in this section is for backward compatibility purposes only. For the new Dial Plan method, see Configuring Dial Plans on page 503.

38.1.5.1 Creating a Dial Plan File



Note: The Dial Plan described in this section is for backward compatibility purposes only. For the new method, see Configuring Dial Plans on page 503.

The Dial Plan file is a text-based file that can contain up to 8 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.

Creating a Dial Plan file is similar for 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 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. Load the converted file to the device, as described in "Loading Auxiliary Files" on page 585.
5. Select the Dial Plan index that you want to use. This depends on the feature and is described in the respective section.



Note:

- Only one Dial Plan file can be loaded to the device.
- The Dial Plan file can only be loaded in .dat file format.

38.1.5.2 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 (see note below) calls. This enables the mapping of called numbers to IP addresses (in dotted-decimal notation) or FQDNs (up to 15 characters).



Note: For the SBC application, the method described in this section for obtaining an IP address using the Dial Plan file is for backward compatibility purposes only. For the new method, see Configuring Dial Plans on page 503.

➤ **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: 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 (see "Creating a Dial Plan File" on page 591).
3. Assign the Dial Plan index to the required routing rule:
 - SBC Calls: In the SBC IP-to-IP Routing table, do the following:
 - a. Set the 'Destination Type' field to Dial Plan.
 - b. 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.

38.1.5.3 Viewing Information of Installed Dial Plan File

You can view information about the Dial Plan file currently installed on the device, through the device's CLI:

- **Viewing Dial Plan file information:** You can view the file name of the installed Dial Plan file and the names of the Dial Plans defined in the Dial Plan file, by entering the following CLI command (in Enable mode):

```
# debug auxiliary-files dial-plan info
```

For example, the following shows the file name of the installed Dial Plan file and lists its Dial Plans:

```
# debug auxiliary-files dial-plan info
File Name: MyDialPlan.txt
Plans:
Plan #0 = PLAN1
Plan #1 = PLAN2
```

Note that the index number of the first Dial Plan is 0.

- **Searching a prefix number:** You can check whether a specific prefix number is defined in a specific Dial Plan (and view the corresponding tag if the Dial Plan implements tags), by entering the following CLI command (in Enable mode):


```
# debug auxiliary-files dial-plan match-number <Dial Plan
number> <prefix number>
```

For example, the following checks whether the called prefix number 2000 is defined in Dial Plan 1, which is used for obtaining the destination IP address (tag):

```
# debug auxiliary-files dial-plan match-number PLAN1 2000
Match found for 4 digits
Matched prefix: 2000
Tag: 10.33.45.92
```

38.1.6 User Information File

This section describes the User Info table.

38.1.6.1 Enabling the User Info Table

Before you can use the User Info table, you need to enable the User Info functionality, as described in the following procedure.

➤ **To enable the User Info table:**

1. Make sure that your device's License Key provides far-end users support ("FEU"). To view the License Key, see "Viewing the License Key" on page 598.
2. Open the Proxy & Registration page (**Setup** menu > **Signaling & Media** tab > **SIP Definitions** folder > **Proxy & Registration**).
3. From the 'Enable User-Information Usage' drop-down list (EnableUserInfoUsage), select **Enable**:

Figure 38-2: Enabling User Info Table

Enable User-Information Usage • Enable ⚡



Note: The 'Enable User-Information Usage' parameter appears in the Web interface only if the device's License Key is defined with far-end users.

4. Reset the device with a save-to-flash for your settings to take effect; the User Info table now appears in the Web interface.

38.1.6.2 User Information File for SBC User Database

You can use the SBC User Info table 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. You can configure up to 3,000 users (table rows) in the SBC User Info table. The SBC User Info table can be configured using any of the following methods:

- Web interface - see "Configuring SBC User Info Table through Web Interface" on page 594

- CLI - see Configuring SBC User Info Table through CLI on page 595
- Loadable User Info file - see "Configuring SBC User Info Table in Loadable Text File" on page 596

38.1.6.2.1 Configuring SBC User Info Table through Web Interface

The following procedure describes how to configure the SBC User Info table through the Web interface.



Note:

- To configure the User Info table, make sure that you have enabled the feature, as described in "Enabling the User Info Table" on page 593.
- If you load any User Info file to the device, all previously configured entries are removed from the table in the Web interface and replaced with the entries from the loaded User Info file.

➤ **To configure the SBC User Info table through the Web interface:**

1. Open the SBC User Info table (**Setup** menu > **Signaling & Media** tab > **SBC** folder > **User Information**).
2. Click **New**; the following dialog box appears:

Figure 38-3: SBC User Info Table - Add Dialog Box

3. Configure a user according to the table below.
4. Click **Apply**.

To register a user, select the user's table entry, and then from the **Action** drop-down list, choose **Register**. To un-register a user, select the user, and then from the **Action** drop-down list, choose **Un-Register**.

Table 38-2: SBC User Info Table Parameter Descriptions

Parameter	Description
Index [SBCUserInfoTable_Index]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.

Parameter	Description
Local User [SBCUserInfoTable_LocalUser]	Defines the user and is used as the Request-URI user part for the AOR in the database. The valid value is a string of up to 10 characters.
Username [SBCUserInfoTable_Username]	Defines the username for registering the user when authentication is necessary. The valid value is a string of up to 40 characters.
Password [SBCUserInfoTable_Password]	Defines the password for registering the user when authentication is necessary. The valid value is a string of up to 20 characters.
IP Group [SBCUserInfoTable_IPGroupName]	Assigns an IP Group to the user and is used as the Request-URI source host part for the AOR in the database. To configure IP Groups, see "Configuring IP Groups" on page 329.
Status [SBCUserInfoTable_Status]	(Read-only field) Displays the status of the user - "Registered" or "Not Registered".

38.1.6.2.2 Configuring SBC User Info Table through CLI

The SBC User Info table can be configured in the CLI using the following commands:

- To add and/or modify a user (example):

```
# configure voip
(config-voip)# sip-definition proxy-and-registration
(sip-def-proxy-and-reg)# user-info sbc-user-info <index, e.g., 1>
(sbc-user-info-1)# username JohnDee
(sbc-user-info-1)# <activate | exit>
```

- To delete a specific user, use the `no` command:

```
(sip-def-proxy-and-reg)# no user-info sbc-user-info <index, e.g., 1>
```

- To view all table entries:

```
(sip-def-proxy-and-reg)# user-info sbc-user-info display
---- sbc-user-info-0 ----
  local-user (JohnDee)
  username (userJohn)
  password (s3fn+fn=)
  ip-group-id (1)
  status (not-resgistered)
---- sbc-user-info-1 ----
  local-user (SuePark)
  username (userSue)
  password (t6sn+un=)
  ip-group-id (1)
  status (not-resgistered)
```

- To view a specific entry (example):

```
(sip-def-proxy-and-reg)# user-info sbc-user-info <index, e.g., 0>
(sbc-user-info-0)# display
```

```

local-user (JohnDee)
username (userJohn)
password (s3fn+fn=)
ip-group-id (1)
status (not-resgistered)
    
```

- To search a user by local-user:

```

(sip-def-proxy-and-reg)# user-info find <local-user, e.g.,
JohnDoe>
JohnDee: Found at index 0 in SBC user info table, not
registered
    
```



Note: To configure the User Info table, make sure that you have enabled the feature as described in "Enabling the User Info Table" on page 593.

38.1.6.2.3 Configuring SBC User Info Table in Loadable Text File

The SBC User Info table can be configured as a User Info file using a text-based file (*.txt). This file can be created using any text-based program such as Notepad.

You can load the User Info file using any of the following methods:

- Web interface - see "Loading Auxiliary Files" on page 585
- *ini* file, using the `UserInfoFileName` parameter - see "Auxiliary and Configuration File Name Parameters" on page 742
- Automatic Update mechanism, using the `UserInfoFileURL` parameter - see Automatic Update Mechanism

To add SBC users to the SBC User Info file, use the following syntax:

```

[ SBC ]
FORMAT LocalUser ,UserName ,Password ,IPGroupID
    
```

where:

- `[SBC]` indicates that this part of the file is the SBC User Info table
- `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



Note:

- Make sure that there are **no** spaces between the values.
- To modify the SBC User Info table using a User Info file, you need to load to the device a new User Info file containing your modifications.

Below is an example of a configured User Info file:

```

[ SBC ]
FORMAT LocalUser ,UserName ,Password ,IPGroupID
john ,john_user ,john_pass ,2
sue ,sue_user ,sue_pass ,1
    
```

38.1.6.3 Viewing the Installed User Info File Name

You can view the name of the User Info file currently installed on the device, through the device's CLI (in Enable mode):

```
# debug auxiliary-files user-info info
```

For example:

```
# debug auxiliary-files user-info info
User Info File Name MyUsers.txt
```

38.1.7 AMD Sensitivity File

The device is shipped with a default, pre-installed *AMD Sensitivity* file for its Answering Machine Detection (AMD) feature. This file includes the detection algorithms for detecting whether a human or answering machine has answered the call, and is based on North American English. In most cases, the detection algorithms in this file suffice even when your deployment is in a region where a language other than English is spoken. However, if you wish to replace the default file with a different AMD Sensitivity file containing customized detection algorithms, please contact your AudioCodes sales representative for more information.

The AMD Sensitivity file is created in .xml format and then converted to a binary .dat file that can be installed on the device. The XML-to-binary format conversion can be done using AudioCodes DConvert utility. For more information on using this utility, refer to *DConvert Utility User's Guide*. Only one AMD Sensitivity file can be installed on the device. To install a new AMD Sensitivity file, use any of the following methods:

- Web interface: Auxiliary Files page - see "Loading Auxiliary Files" on page 585.
- TFTP during initialization: You need to configure the *ini* file parameter, *AMDSensitivityFileName*, and then copy the AMD Sensitivity file to the TFTP directory.
- Automatic Update feature: For more information, see Automatic Update Mechanism. For this method, the *AMDSensitivityFileUrl* parameter must be set through SNMP or *ini* file.

For more information on the AMD feature, see "Answering Machine Detection (AMD)" on page 192.

38.2 License Key

The device is shipped with a pre-installed 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 License Key to match your requirements.



Note:

- The device is shipped by default with a pre-installed License Key that enables up to three call sessions only. Once you have installed the Mediant Software E-SBC, you need to activate your license by loading a License Key file enabling the ordered call capacity and features. For more information, see Entering the Product Key on page 598 and Obtaining License Key for Initial Activation on page 599.
- For the High Availability (HA) system, the License Key includes the HA feature and is installed on both units - active and redundant. If the redundant unit's License Key is missing or invalid, the system is moved to mismatch configuration mode (alerted by SNMP).
- The availability of certain Web pages depends on the installed License Key.

38.2.1 Viewing the License Key

To view the device's License Key and its features, follow the procedure below:

➤ **To view the License Key:**

- Open the License Key page:
 - **Toolbar:** From the **Actions** drop-down menu, choose **License Key**.
 - **Navigation tree:** **Setup** menu > **Administration** tab > **Maintenance** folder > **License Key**.

The encrypted License Key is displayed in the 'Current License Key' field and the main features provided by the License Key are displayed in the pane below the field.

38.2.2 Entering the Product Key

The Product Key identifies a specific purchase of your device installation for the purpose of subsequent communication with AudioCodes, for example, for support and software upgrades. The Product Key is provided in an e-mail confirmation at the time the product is purchased and must be entered on the product through the Web interface in order to activate your product. Therefore, you only need to perform this procedure once.

➤ **To enter the Product Key:**

1. Open the License Key page (**Setup** menu > **Administration** tab > **Maintenance** folder > **License Key**).
2. In the 'Product Key' field, enter the Product Key.

Figure 38-4: Product Key on Software Upgrade Key Status Page

Product Key

3. Click the **Change Product Key** button.

You can view the Product Key on the Device Information page (see "Viewing Device Information" on page 637).

38.2.3 Obtaining License Key for Initial Activation

The procedure below describes how to obtain the License Key for initial activation of your device.

➤ **To obtain the License Key for initial activation:**

1. Make a note of the device's Serial Number (fingerprint). The Serial Number uniquely identifies the software installation. The Serial Number is displayed in the 'Serial Number' field on the Device Information page (see "Viewing Device Information" on page 637).
2. Activate your product through AudioCodes License Activation tool at <http://www.audiocodes.com/swactivation>. You will need your Product Key and Fingerprint (Serial Number) for this activation process. The Product Key is provided to you in the e-mail that was sent to confirm your purchase order from AudioCodes. Upon activation, an e-mail will be sent to you with a License Key file.
3. When you receive the new License Key file, open the file with any text-based program (e.g., Notepad), and then verify that the "S/N" value reflects the Serial Number of your product.



Warning: Do not modify the contents of the License Key file.



Note: For 1+1 High-Availability orders, you are provided with two Product Keys, one for each unit. In such cases, you need to perform the license activation process twice in order to obtain license keys for both units.

38.2.4 Obtaining License Key for Feature Upgrade

Before you can install a new License Key, you need to obtain a License Key file for your device with the required features from your AudioCodes representative. The 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 License Key for more than one device, the License Key file can include multiple License Keys (see figure below). In such cases, each License Key in the file is associated with a unique serial number identifying the specific device. When loading such a License Key file, the device installs only the License Key that is associated with its serial number.

Figure 38-5: License Key File with Multiple S/N Lines

```

sample.ini - Notepad
File Edit Format Help
[LicenseKeys]
:Board Type 29
S/N241182 =
okRTr5topwYMbIZd4NN2a3Qhm4Njfi daagUyehso94APbBF85hF4by0cmQZf2B8bMcze7JQ9kMSa5h641R1aOkeEb9AddF894Zx
S/N242519 = tmxTr5to0mlMblZdoPd2a3Qh9zJfidafiyehsogOQPbBF8pj4by0c9jdf2B8eOoze7JQgywSa5h6o391aOkeTlIAAddF8c6Fx
S/N226403 = tmxTr5to0lsmblZdoOB2a3Qh9yJfidafiyehsogN4PbBF8piZ4by0c9jdf2B8eOoze7JQgywSa5h6o2x1aOkeTlIAAddF8c6Fx
S/N226417 = r6xTr5to25sMblZdfB2a3Qh5OJfida92yehsoix4PbBF8eOZ4by0c52xf2B88yoze7JQINgSa5h6fyx1aOkeXZlIAAddF8amF8x
:Board Type 24
S/N241182 =
okRTr5topwYMbIZd4NN2a3wkm4Njfi daagUyehso94APbBF85hF4by0cmQZf2B8bMcze7JQ9kMSa5h641R1aOkeEb9AddF8938s
S/N242519 = tmxTr5to0mlMblZdoPd2a3wk9zJfidafiyehsogOQPbBF8pj4by0c9jdf2B8eOoze7JQgywSa5h6o391aOkeTlIAAddF8c1ss
S/N226403 = tmxTr5to0lsmblZdoOB2a3wk9yJfidafiyehsogN4PbBF8piZ4by0c9jdf2B8eOoze7JQgywSa5h6o2x1aOkeTlIAAddF8c1ss
S/N226417 = r6xTr5to25sMblZdfB2a3wk5OJfida92yehsoix4PbBF8eOZ4by0c52xf2B88yoze7JQINgSa5h6fyx1aOkeXZlIAAddF8ahss
  
```

➤ **To obtain a License Key:**

1. Open the Device Information page (see "Viewing Device Information" on page 637) and make a note of the device's serial number and product key:
 - 'Serial Number' field displays the serial number.
 - 'Product Key' field displays the product key.
2. If you need a License Key for more than one device, repeat Step 1 for each device.
3. Send the serial number and product key to your AudioCodes representative when requesting the required License Key.
4. When you receive the new License Key file, check the file as follows:
 - a. Open the file with any text-based program such as Notepad.
 - b. Verify that the first line displays "[LicenseKeys]".
 - c. Verify that the file contains one or more lines in the following format:
 "S/N<serial number> = <License Key string>"
 For example: "S/N370604 = jCx6r5tovCIKaBBbhPtT53Yj..."
 - d. Verify that the "S/N" value reflects the serial number of your device. If you have multiple License Keys, ensure that each "S/N" value corresponds to a device.



Warning: Do not modify the contents of the License Key file.

5. Install the License Key on the device, as described in "Installing the License Key" on page 600.

38.2.5 Installing the License Key

After you have received your License Key file from your AudioCodes representative, you can install it on the device as described in this section.



Note: When you install a new License Key, it is loaded to the device's non-volatile flash memory and overwrites the previously installed License Key.

38.2.5.1 Installing License Key through Web Interface

The following procedure describes how to install the License Key through the Web interface.

➤ **To install the License Key through the Web interface:**

1. Open the License Key page (**Setup** menu > **Administration** tab > **Maintenance** folder > **License Key**).
2. Back up the License Key currently installed on the device, as a precaution. If the new License Key does not comply with your requirements, you can re-load the backup to restore the device's original capabilities.

- a. In the 'Current License Key' field, select the entire text string and copy it to any standard text file (e.g., Notepad):

Figure 38-6: Copying License Key

Current License Key:

iSNTt05ji24S3xYVj1cioBRW3jitzfglk3yRqmkgEflgX3g0CihcrqTJsfM5zfglk3yOy8kgE2S8N2ffleCm?PwAK63hDeglk3yOy8kkF06sQ33cl

- 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 License Key file with a single License Key (i.e., one "S/N") or with multiple License Keys (i.e., more than one "S/N"), do one of the following:
 - **Loading a File with Multiple License Keys:**
 - a. Under the "Load License Key file ..." text, click the **Browse** button, and then navigate to and select the License Key file on your computer.
 - b. Click **Load File**; the new License Key is installed on the device and saved to flash memory. The License Key is displayed in the 'Current License Key' field.

Figure 38-7: Loading License Key File

Load "License Key" file from your computer to the device

No file selected.



Note: If the device is operating in High-Availability mode, you can only install the License Key by loading a License Key file, as the file includes two License Keys (for active and redundant devices).

- **Loading a File with a Single License Key:**
 - a. Open the License Key file using a text-based program such as Notepad.
 - b. Copy-and-paste the string from the file into the 'New License Key' field, and then click **Change Key**:

Figure 38-8: Installing Single License Key

New License Key

4. Verify that the License Key was successfully installed:
 - On the License Key page, check that the listed features and capabilities activated by the installed 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 License Key are activated.



Note: If the Syslog server indicates that the License Key was unsuccessfully loaded (i.e., the "SN_" line is blank), do the following preliminary troubleshooting procedures:

1. Open the 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.

38.2.5.2 Installing License Key through CLI

To install the License Key through CLI, use the following commands:

- To install the License Key:

```
(config-system)# feature-key <"string enclosed in double quotation marks">
```

- To view the License Key:

```
show system feature-key
```

38.3 Upgrading SBC Capacity Licenses by License Pool Manager Server

The device can receive SBC capacity licenses from a centralized pool of SBC resources managed by the License Pool Manager Server running on AudioCodes EMS. The License Pool Manager Server can dynamically allocate and de-allocate SBC capacity licenses from the pool to devices in the network to meet capacity demands of each device whenever required. The License Pool Manager Server holds a pool of customer-ordered SBC capacity (resource) licenses, which can include any of the following license types:

- SBC sessions (media and signaling)
- SBC signaling sessions
- SBC transcoding sessions
- SBC registrations (number of SIP endpoints that can register with the SBC)

Therefore, the device can be upgraded by the License Pool Manager Server with any of the above SBC license types.

Communication between the device and License Pool Manager Server is through HTTPS (port 443) and SNMP. If a firewall exists in the network, ensure that ports for these applications are opened. The device periodically checks with the License Pool Manager Server for SBC capacity licenses. The License Pool Manager Server identifies the device by serial number. If it has an SBC license for the device, it sends it to the device. If the device's installed License Key already includes SBC capacity figures, the SBC license allocated from the pool is simply added to it (but up to the device's maximum supported capacity capabilities). A device reset is required for the allocated SBC license to take effect.

You can view the SBC license allocated by the License Pool Manager Server in the License Key page (see "Installing License Key through Web Interface" on page 600):

- "SBC Sessions Capability":
 - "Local License": Number of SBC sessions according to the installed License Key. The actual license is indicated on the page in the "SBC=" field (e.g., SBC=5, as shown in the example figure below).
 - "Pool License": Number of SBC sessions allocated by the License Pool Manager Server.

- "Total (Actual)": Total number of SBC sessions permitted on the device based on the installed License Key and the SBC sessions allocated by the License Pool Manager Server.
- "LicensePool features":
 - "SBC": Number of SBC sessions (media and signaling) allocated by the License Pool Manager Server.
 - "CODER-TRANSCODING": Number of SBC transcoding sessions allocated by the License Pool Manager Server.
 - "FEU": Number of SBC registrations allocated by the License Pool Manager Server.
 - "SBC-SIGNALING": Number of SBC signaling sessions allocated by the License Pool Manager Server.

The following displays an example of the indication of SBC licenses allocated by the License Pool Manager Server in the License Key page:

```

SBC Sessions Capability:
Local License: 5 SBC Sessions
Pool License: 7 SBC Sessions (from License Pool Manager)
Total (Actual): 12 SBC Sessions

Key features:
Board Type: Mediant 800
Coders: G723 G729 G728 NETCODER GSM-FR GSH-EFR AMR EVRC-QCELP G727 ILBC EVRC-B AMR-WB G722 EG711 MS_RTA_NB /
QOE features: VoiceQualityMonitoring MediaEnhancement
Security: IPSEC MediaEncryption StrongEncryption EncryptControlProtocol
Channel Type: RTP DspCh=100
HA
DATA features:
DSP Voice features:
IP Media: CALEA
T1Trunks=1
FXSPorts=4
FXOPorts=4
Control Protocols: TDMtoSBC TestCall=500 MGCP SIP SASurvivability SBC=5
Default features:
Coders: G711 G726

LicensePool features:
SBC=7 CODER-TRANSCODING=0 FEU=0 SBC-SIGNALING=0

```

If communication with the License Pool Manager Server is lost for a long duration, the device discards the allocated SBC license (i.e., expires) and resets with its initial, "local" SBC license. This mechanism prevents misuse of SBC licenses allocated by the License Pool Manager Server.

The following SNMP alarms relate to the allocation/de-allocation of SBC licenses by the License Pool Manager Server:

- acLicensePoolInfraAlarm (1.3.6.1.4.1.5003.9.10.1.21.2.0.106):
 - Sent when the device receives a new SBC license from the License Pool Manager Server and a device reset is required.
 - Sent when the device is unable to access the License Pool Manager Server.
 - Sent when the SBC license allocated by the License Pool Manager Server is about to expire (e.g., when communication with the License Pool Manager Server is lost)
- acLicensePoolApplicationAlarm (1.3.6.1.4.1.5003.9.10.1.21.2.0.107):

- Sent when the device receives an SBC license from the License Pool Manager Server that exceeds the maximum SBC session capacity that can be supported by the device.
- Sent when the device resets with an SBC license allocated by the License Pool Manager Server that exceeds the maximum SBC session capacity that can be supported by the device. The device sets the capacity to its maximum (and values beyond the device's capability are not applied)

Note:

- No configuration is required on the device; the License Pool Manager Server controls the allocation/de-allocation of its resource pool to the managed devices. For more information on the License Pool Manager Server, refer to *the EMS User's Manual*.
- The allocation/de-allocation of SBC licenses to the device by the License Pool Manager Server is service affecting and requires a device reset.
- For HA systems, the License Pool Manager Server automatically allocates an equal number of SBC licenses (sessions) to both the active and redundant devices. For example, if the License Pool Manager Server allocates 200 sessions to the active device, it also allocates 200 to the redundant. Thus, it is important to take this into consideration when ordering a license pool.
- If the device is restored to factory defaults, the SBC license allocated by the License Pool Manager Server is deleted.
- If the device is allocated an SBC license by the License Pool Manager Server that exceeds the maximum number of sessions that it can support, the device sets the number of sessions to its maximum supported.



38.4 Software Upgrade Wizard

The Web interface's Software Upgrade wizard lets you easily upgrade the device's software version (.cmp file). You can also use the wizard to load an *ini* file and Auxiliary files (e.g., CPT file). However, you can only use the wizard if you at least load a .cmp file. Once loaded, you can select other file types to load.

You can also use the wizard to upgrade devices in High Availability (HA) mode. You can choose between two optional HA upgrade methods:

- **System Reset Upgrade (non-Hitless):** Both active and redundant devices are upgraded simultaneously. Therefore, this method is traffic-affecting and terminates current calls during the upgrade process. The process is as follows:
 1. The active (current) device loads the .cmp file.
 2. The active device sends the .cmp file to the redundant device.
 3. Both active and redundant devices install and burn the file to flash memory with a reset. In other words, no HA switchover occurs.
- **Hitless Upgrade:** The devices are upgraded without disrupting traffic (i.e., current calls are maintained). The process is as follows:
 1. The active (current) device loads the .cmp file.
 2. The active device sends the .cmp file to the redundant device.
 3. The redundant device installs and burns the file to its flash memory with a reset. The redundant device now runs the new software version.
 4. An HA switchover occurs from active to redundant device. Therefore, current calls are maintained and now processed by the previously redundant device, which is now the active device.

5. The previously active device (now in redundant mode) installs and burns the file to flash memory with a reset. Therefore, both devices now run the new software version.
6. An HA switchover occurs from active device (i.e., the initial redundant device) to redundant device (i.e., the initial active device) to return the devices to their original HA state. Only the initial redundant device undergoes a reset to return to redundant state.

**Note:**

- You can obtain the latest software files from AudioCodes Web site at <http://www.audiocodes.com/downloads>.
- You can upgrade the device to the latest software version as specified in the installed License Key. If you attempt to upgrade the device to a version that is later than the one specified in the License Key, the device remains at the current software version. For more information, contact your AudioCodes sales representative.
- When upgrading Mediant VE SBC from Version 7.0 to any later version, please refer to the post-upgrade procedure described in Post-Upgrade from Version 7.0 Procedure on page 610.
- When you start the wizard, the rest of the Web interface is unavailable. After the files are successfully installed with a device reset, access to the full Web interface is restored.
- If you upgraded your firmware (.cmp file) and the "SW version mismatch" message appears in the Syslog or Web interface, your License Key does not support the new .cmp file version. If this occurs, contact AudioCodes support for assistance.
- Instead of manually upgrading the device, you can use the device's Automatic Update feature for automatic provisioning (see "Automatic Provisioning" on page 615).

The following procedure describes how to load files using the Web interface's Software Upgrade Wizard. Alternatively, you can load files using the CLI:

- cmp file:
copy firmware from <URL>
 - ini or Auxiliary file:
copy <ini file or auxiliary file> from <URL>
 - CLI script file:
copy cli-script from <URL>
 - HA devices:
 - Hitless Software Upgrade:
copy firmware from <URL and file name>
 - Non-Hitless Software Upgrade:
copy firmware from <URL and file name> non-hitless
- **To upgrade the device using the Software Upgrade wizard:**
1. Make sure that you have installed a License Key that is compatible with the software version to be installed (see "License Key" on page 597).
 2. It is recommended to enable the Graceful Lock feature (see "Locking and Unlocking the Device" on page 581). The wizard resets the device at the end of the upgrade process, thereby causing current calls to be untimely terminated. To minimize traffic

disruption, the Graceful Lock feature prevents the establishment of new calls.

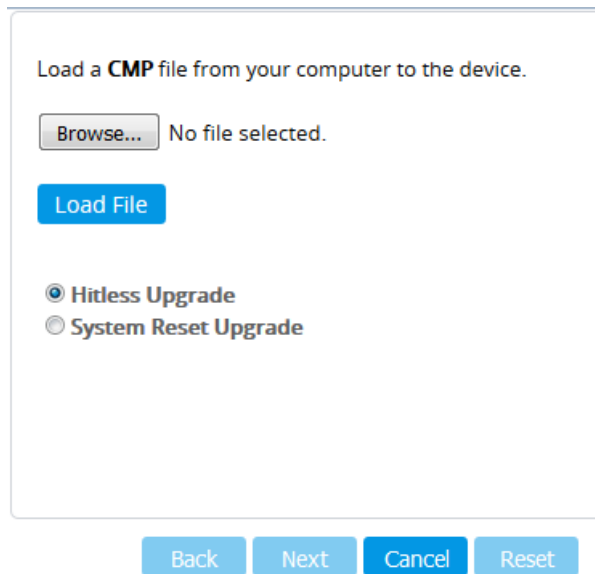
3. It is recommended to backup the device's configuration to your computer. If an upgrade failure occurs, you can restore your configuration by uploading the backup file to the device. For more information, see "Backing Up and Loading Configuration File" on page 613.
4. Open the Software Upgrade wizard:
 - **Toolbar:** From the **Actions** drop-down menu, choose **Software Upgrade**.
 - **Navigation tree:** **Setup** menu > **Administration** tab > **Maintenance** folder > **Software Upgrade**.

Figure 38-9: Starting Software Upgrade Wizard

Software Upgrade



5. Click **Start Software Upgrade**; the wizard starts, prompting you to load a .cmp file:



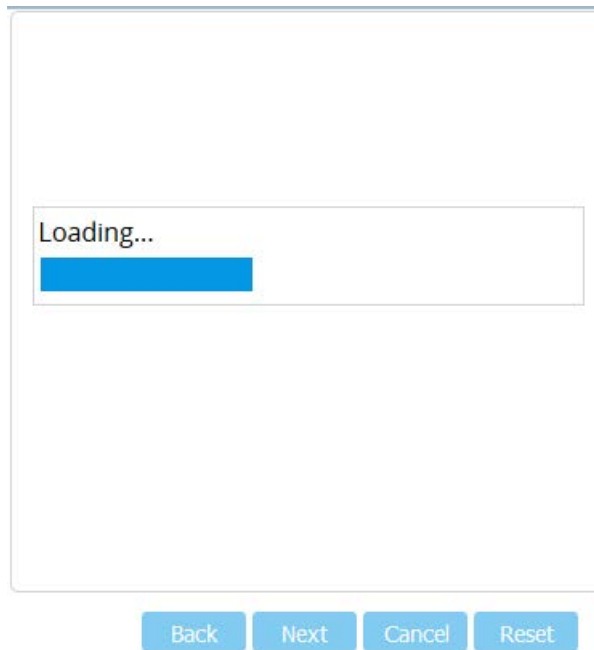
Note:

- The Hitless Upgrade and System Reset Upgrade options appear only if the device is configured for HA.
- At this stage, you can quit the Software Upgrade wizard without having to reset the device, by clicking **Cancel**. However, if you continue with the wizard and start loading the cmp file, the upgrade process must be completed with a device reset.

6. Click **Browse**, and then navigate to and select the .cmp file.

- Click **Load File**; the device begins to install the .cmp file and a progress bar displays the status of the loading process:

Figure 38-10: CMP File Loading Progress Bar



When the file is loaded, a message is displayed to inform you.

- If your device is in HA mode, select one of the following upgrade options:
 - Hitless Upgrade (default)
 - System Reset Upgrade

See the description of these methods in the beginning of this section.



Note: If you select the Hitless Upgrade option, the wizard can only be used to upload a .cmp file; Auxiliary and ini files cannot be uploaded.

- To load additional files, use the **Next** and **Back** buttons to navigate through the wizard to the desired file-load wizard page; otherwise, skip to the next step to load the .cmp file only.

The wizard page for loading an *ini* file lets you do one of the following:

- Load a new ini file:**
 - Click **Browse**, and then navigate to and select the new ini file.
 - Click **Load File**; the device loads the *ini* file.
- Restore configuration to factory defaults:** Clear the 'Use existing configuration' check box.

- **Retain the existing configuration (default):** Select the 'Use existing configuration' check box.

Figure 38-11: Load an INI File in the Software Upgrade Wizard

Load an *ini* file from your computer to the device.

No file selected.

Use existing configuration

Warning: 1. If you choose to load an ini file, parameters that are omitted from the file, revert to default settings. Therefore, make sure that the ini file contains all required configuration (e.g. IP networking parameters).
 2. The device restores to factory default settings if you clear the Use Existing Configuration check box and don't select a file to load.



Note: 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) and thereby, overwrite values previously configured for these parameters.

10. Click **Reset**; a progress bar is displayed, indicating the progress of saving the files to flash and device reset.

Figure 38-12: Progress Bar Indicating Burning Files to Flash

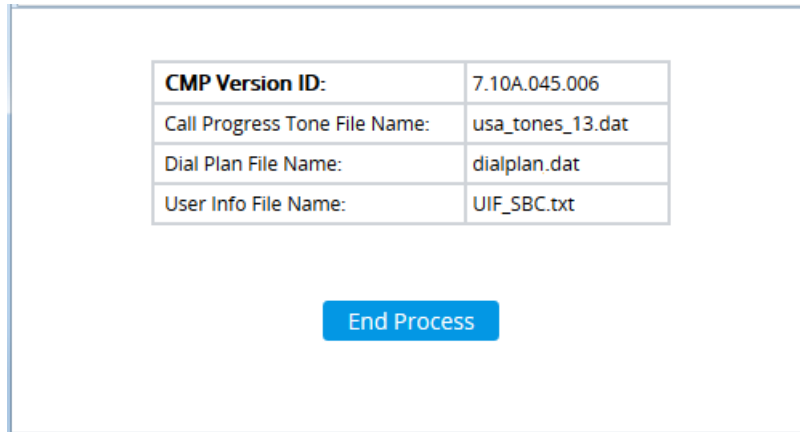
Burn and reset in progress...



Note: Device reset may take a few minutes (even up to 30 minutes), depending on .cmp file version.

When the device finishes the installation process and resets, the wizard displays the following, which lists the installed .cmp software version and other files that you may also have installed:

Figure 38-13: Software Upgrade Process Completed (Example)



11. Click **End Process** to close the wizard; the Web Login page appears, allowing you to log in to your upgraded device.

38.4.1 Post-Upgrade from Version 7.0 Procedure

If you have upgraded the Mediant VE SBC **from Version 7.0** to any later version, you must add the following configuration parameter and settings to each virtual machine (VM) running the Mediant VE SBC to ensure high performance is maintained:

- Parameter name: **monitor_control.halt_desched**
- Parameter value: **FALSE**

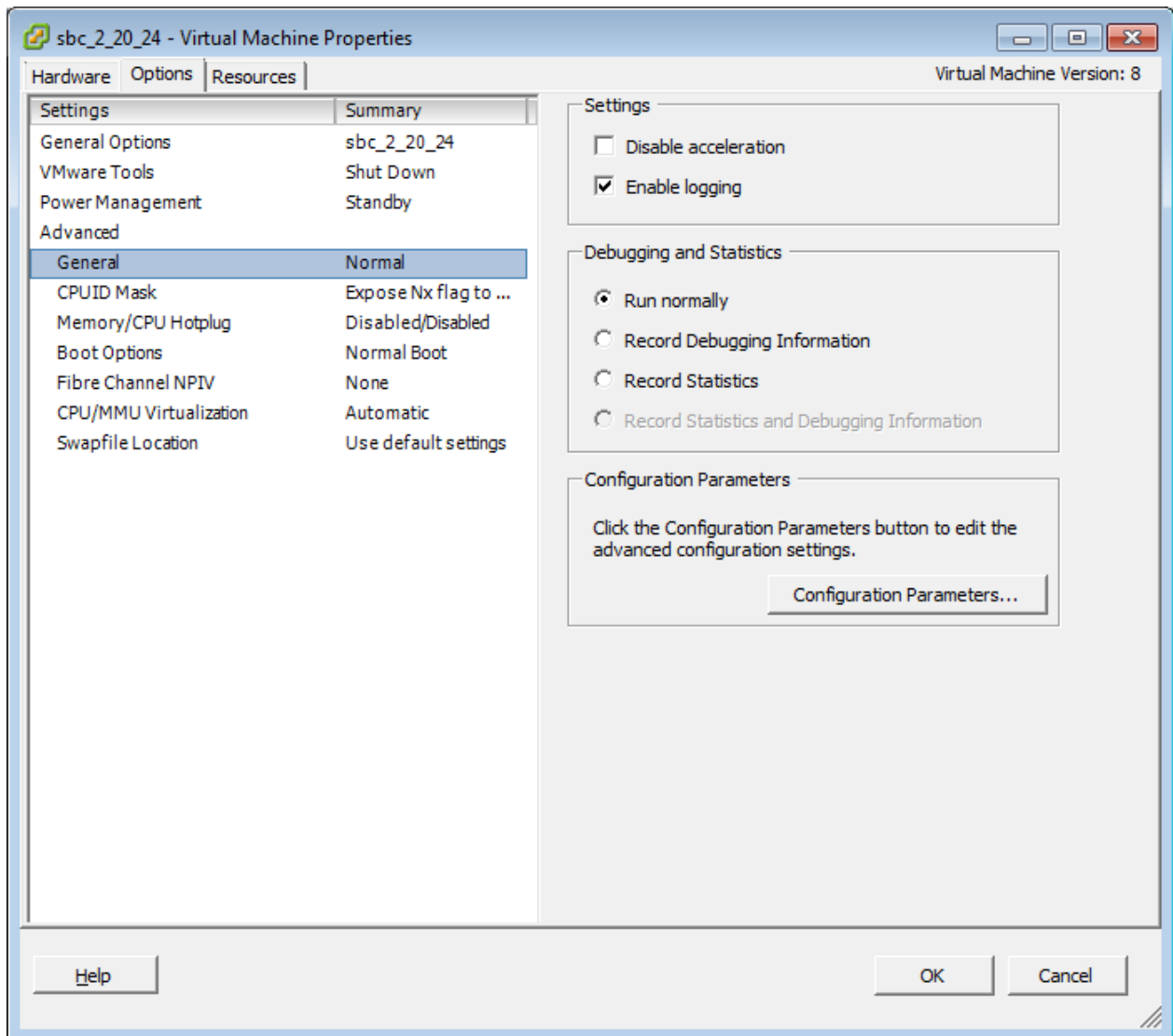
The following procedure provides an example of how to do this using the VMware vSphere Client program.

➤ **To ensure performance when upgrading from Version 7.0:**

1. Upgrade the device's (virtual machine's) software from Version 7.0 (see "Software Upgrade Wizard" on page 604).
2. Access the host server running the virtual machines (using, for example, VMware vSphere Client).
3. Power off the virtual machine: In the list of virtual machines running on the host, right-click the name of the required virtual machine, and then from the shortcut menu, choose **Power Off**.
4. Add the parameter:
 - a. Right-click the required virtual machine again, and then from the shortcut menu, choose **Edit Settings**.

- b. Click the **Options** tab; the following appears:

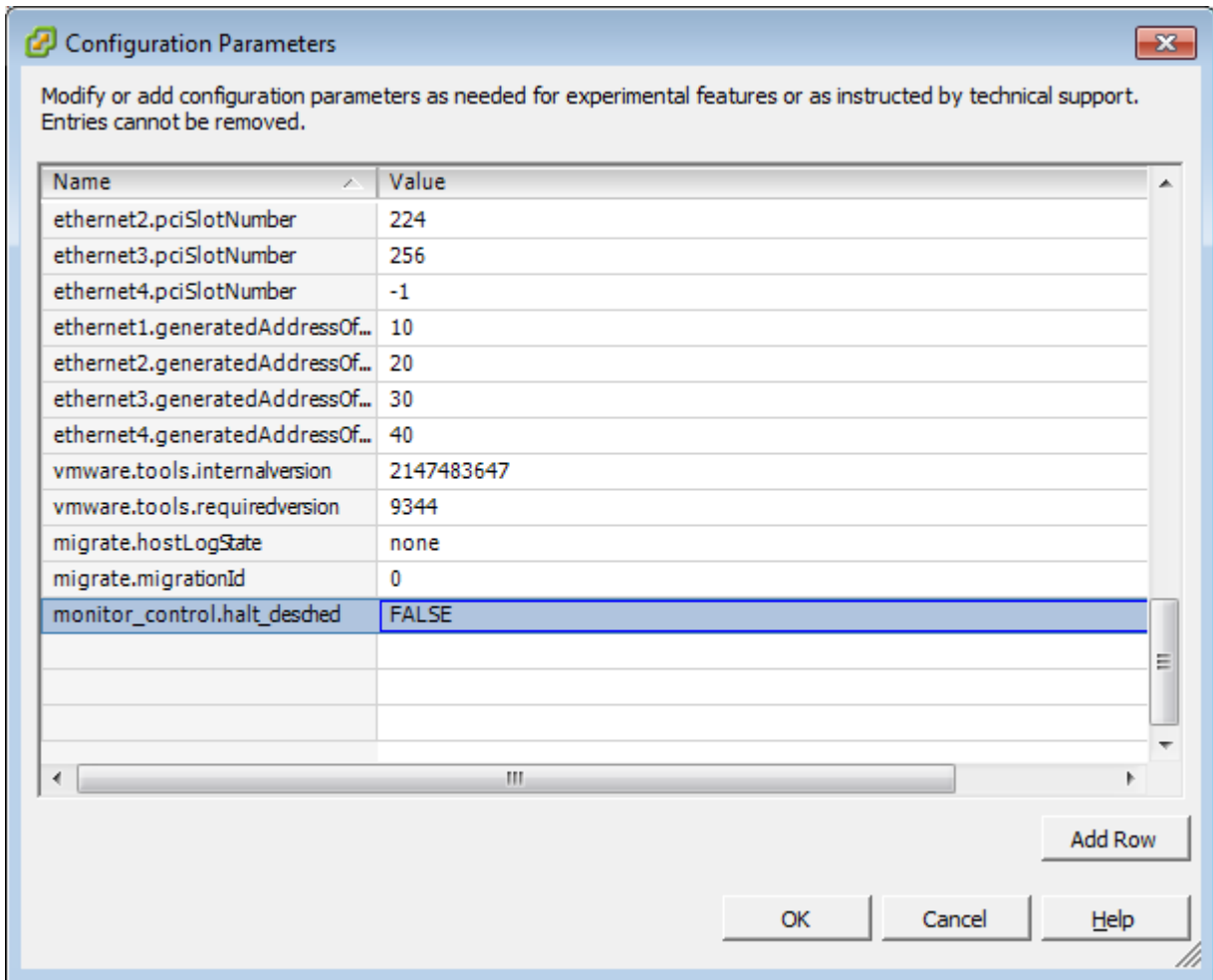
Figure 38-14: Adding Parameter to VM - Options Tab (Example)



- c. In the left pane, select **General** under the **Advanced** folder.

- d. Click the **Configuration Parameters** button; the following dialog box appears:

Figure 38-15: Adding Parameter to VM - Configuration Parameters (Example)



- e. Click the **Add Row** button, and then add a parameter with the following settings:
 - ◆ Name: **monitor_control.halt_desched**
 - ◆ Value: **FALSE**
 - f. Click **OK**, and then click **OK** in all opened dialog boxes until you return to the main window listing all the virtual machines.
 - g. Power on the virtual machine: Right-click the name of the required virtual machine, and then from the shortcut menu, choose **Power On**.
5. Repeat the above steps for each virtual machine.

39 Backing Up and Loading Configuration File

You can save a copy of the device's current configuration settings as a file on a local PC (ini file), remote server. This can be used as a backup file for your configuration. If needed, you can then load the file to the device to restore your configuration settings. The saved file includes only parameters that were modified and parameters with other than default values.

You can also save (create) the current configuration as a configuration file on the device's flash memory and then send it to a user-defined URL of a remote server (TFTP or HTTP/S). The configuration settings in the file are based only on CLI commands. This is done through CLI:

- Creating a Configuration file and saving it on a remote server:

```
# write-and-backup to <URL path with file name>
```

For example:

```
# write-and-backup to tftp://192.168.0.3/config-device1.txt
```



Warning:

- When loading an *ini* file using the Configuration File page, parameters excluded from the *ini* file **return to default settings**. If want to keep the device's current configuration settings and apply the settings specified in the ini file, load the file through the Auxiliary Files page, as described in "Loading Auxiliary Files through Web Interface" on page 586.
- When loading an ini file, the device resets for the settings to take effect.

➤ To save or load an ini file:

1. Open the Configuration File page:
 - **Toolbar:** From the **Actions** drop-down menu, choose **Configuration File**.
 - **Navigation tree:** **Setup** menu > **Administration** tab > **Maintenance** folder > **Configuration File**.
2. To save the *ini* file on your computer:
 - a. Click the **Save INI File** button; a dialog box appears.
 - b. Select the 'Save File' option, and then click **OK**.

Figure 39-1: Saving Configuration File using Configuration File Page

SAVE THE **INI** FILE TO THE PC.

Save INI File

3. To load an *ini* file to the device:
 - a. Click the **Browse** button, navigate to and select the file, and then click **Open**; the file name is displayed next to the **Browse** button.

- b. Click the **Load INI File** button, and then at the prompt, click **OK**; the device uploads the file and then resets. Once complete, the Web Login screen appears, requesting you to enter your username and password.

Figure 39-2: Loading ini File using Configuration File Page

LOAD THE **INI** FILE TO THE DEVICE.

No file selected.

Load INI File

The device will perform a reset after loading the **INI** file.

40 Automatic Provisioning

This chapter describes the device's automatic provisioning mechanisms.

40.1 Automatic Configuration Methods

The table below summarizes the automatic provisioning methods supported by the device:

Table 40-1: Automatic Provisioning Methods

BootP / TFTP	DHCP		Automatic Update Methods				SNMP (EMS)
	67	66	HTTP/S	TFTP	FTP	NFS	
No	No	No	Yes	Yes	Yes	No	Yes

40.1.1 DHCP-based Provisioning

A third-party DHCP server can be configured to automatically provide each device, acting as a DHCP client, with a temporary IP address so that individual MAC addresses are not required. The DHCP server can provide additional networking parameters such as subnet mask, default gateway, primary and secondary DNS server, and two SIP server addresses. These network parameters have a time limit, after which the device must 'renew' its lease from the DHCP server.

The device can use a host name in the DHCP request. The host name is set to `acl_nnnnn`, where `nnnnn` denotes the device's serial number. The serial number is the last six digits of the MAC address converted to decimal representation. In networks that support this feature and if the DHCP server registers this host name to a DNS server, you can access the device (through a Web browser) using the URL, `http://acl_<serial number>` (instead of using the device's IP address). For example, if the device's MAC address is 00908f010280, the DNS name is `acl_66176`.



Note:

- When using DHCP to acquire an IP address, the IP Interfaces table, VLANs and other advanced configuration options are disabled.
- For additional DHCP parameters, see "DHCP Parameters" on page 753.

➤ **To enable the device as a DHCP client:**

1. Open the Network Settings page (**Setup** menu > **IP Network** tab > **Advanced** folder > **Network Settings**).
2. From the "Enable DHCP" drop-down list, select **Enable**.

Figure 40-1: Enabling DHCP Client Functionality



3. Click **Apply**.
4. To activate the DHCP process, reset the device.

The following shows an example of a configuration file for a 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;
    }
}
```

Note:

- If, during operation, the device's IP address is changed as a result of a DHCP renewal, the device automatically resets.
- If the DHCP server denies the use of the device's current IP address and specifies a different IP address (according to RFC 1541), the device must change its networking parameters. If this occurs while calls are in progress, they are not automatically rerouted to the new network address. Therefore, administrators are advised to configure DHCP servers to allow renewal of IP addresses.
- If the device's network cable is disconnected and then reconnected, a DHCP renewal is performed (to verify that the device is still connected to the same network). The device also includes its product name in the DHCP Option 60 Vendor Class Identifier. The DHCP server can use this product name to assign an IP address accordingly.
- After power-up, the device performs two distinct DHCP sequences. Only in the second sequence is DHCP Option 60 included. If the device is software reset (e.g., from the Web interface or SNMP), only a single DHCP sequence containing Option 60 is sent.



40.1.2 HTTP-based Provisioning

An HTTP or HTTPS server can be located in the network in which the device is deployed, storing configuration and software files for the device to download. This does not require additional servers and is NAT-safe.

For example, assume the core network HTTPS server is <https://www.corp.com>. A master configuration ini file can be stored 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 device can be configured to periodically check the HTTP server for file updates. 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 only configuration required is to preconfigure the device(s) with the URL of the initial (master) ini file. This can be done using one of the following methods:

- DHCP, as described in "DHCP-based Provisioning" on page 615 or via TFTP at a staging warehouse. The URL is configured using the IniFileURL parameter.
- Private labeling (preconfigured during the manufacturing process).
- 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`

For more information on HTTP-based provisioning, see "HTTP/S-Based Provisioning using the Automatic Update Feature" on page 617.

40.1.3 FTP-based Provisioning

The Automatic Update feature provides limited support for FTP/FTPS connectivity. Periodic polling for updates is not possible since these protocols do not support conditional fetching (i.e., updating files only if they are changed on the server).

The only difference between FTP-based provisioning and those described in "HTTP-based Provisioning" on page 616 is that the protocol in the URL is "ftp" (instead of "http").

40.1.4 Provisioning using AudioCodes EMS

AudioCodes EMS server functions as a core-network provisioning server. The device's SNMP Manager should be configured with the IP address of the EMS server, using one of the methods detailed in the previous sections. As soon as a registered device contacts the EMS server through SNMP, the EMS server handles all required configuration automatically, upgrading software as needed. This alternative method doesn't require additional servers at the customer premises, and is NAT-safe.

40.2 HTTP/S-Based Provisioning using the Automatic Update Feature

The Automatic Update feature can be used for automatic provisioning of the device through HTTP/S. 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 device may be preconfigured during the manufacturing process (commonly known as private labeling). Typically, a two-stage configuration process is implemented whereby initial configuration includes only basic configuration, while the final configuration is done only when the device is deployed in the live network.



Warning: If you use the IniFileURL parameter for the Automatic Update feature, do not use the Web interface to configure the device. If you do configure the device through the Web interface 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 need to re-load the ini file (using the Web interface or BootP) with the correct IniFileURL settings. As a safeguard to an unintended save-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 parameters, see "Automatic Update Parameters" on page 743 or refer to the CLI Reference Guide.
- 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>.

40.2.1 Files Provisioned by Automatic Update

You can use the Automatic Update feature to update the device with any of the following files:

- Software file (*cmp*)
- Auxiliary files (e.g., Call Progress Tones, SSL Certificates, SSL Private Key)
- Configuration file:
 - ini File: Contains only ini file parameters and configures all the device's functionalities.
 - CLI Script File: Contains only CLI commands and configures all the device's functionalities (except commands such as show, debug or copy). The file updates the device's configuration only according to the configuration settings in the file. The device's existing configuration settings (not included in the file) are retained. The device does not undergo a reset and therefore, this file typically contains configuration settings that do not require a device reset. If a reset is required, for example, to apply certain settings, you must include the following CLI command (root level) at the end of the file:

```
# reload if-needed
```

To configure the URL of the server where the file is located, use the AUPDCliScriptURL ini file parameter or CLI command, configure system > automatic-update > cli-script <URL>.

40.2.2 File Location for Automatic Update

The files for updating the device can be stored on any standard Web (HTTP/S), TFTP, or FTP, server. The files can be loaded periodically to the device using HTTP/S, TFTP, or FTP, . This mechanism can be used even when the device is installed behind NAT and firewalls. The Automatic Update feature is done per file and configured by specifying the file name and URL address of the provisioning server where the file is located. For a description of the parameters used to configure URLs per file, see "Automatic Update Parameters" on page 743.

Below are examples for configuring the file names and their URLs for Automatic Update:

- ini File:

```
IniFileURL = 'http://www.corp.com/configuration.ini'
CptFileURL = 'http://www.corp.com/call_progress.dat'
AutoCmpFileUrl = 'http://www.corp.com/SIP_F7.00A.008.cmp'
FeatureKeyURL = 'https://www.company.com/License_Key.txt'
```

■ CLI:

```
# configure system
(config-system)# automatic update
(automatic-update)# cli-script https://company.com/cli/<MAC>
(automatic-update)# voice-configuration http://www.company.com/configuration.ini
(automatic-update)# call-progress-tones http://www.company.com/call_progress.dat
(automatic-update)# feature-key http://www.company.com/License_Key.txt
(automatic-update)# auto-firmware http://www.company.com/SIP_F7.00A.008.cmp
```



Note: For configuration files, the file name in the URL can automatically contain the device's MAC address for enabling the device to download a file unique to the device. For more information, see "MAC Address Placeholder in Configuration File Name" on page 619.

40.2.3 MAC Address Placeholder in Configuration File Name

You can configure the file name of the configuration file in the URL to automatically include the MAC address of the device. As described in "File Location for Automatic Update" on page 618, the file name is included in the configured URL of the provisioning server where the file is located.

Including the MAC address in the file name is useful if you want the device to download a file that is unique to the device. This feature is typically implemented in mass provisioning of devices where each device downloads a specific configuration file. In such a setup, the provisioning server stores configuration files per device, where each file includes the MAC address of a specific device in its file name.

To support this feature, you need to include the MAC address placeholder, "<MAC>" anywhere in the configured file name of the URL, for example:

```
IniFileURL = 'https://www.company.com/config_<MAC>.ini'
(automatic-update)# cli-script
https://company.com/files/cli_script_<MAC>.txt
```

The device automatically replaces the string with its hardware MAC address, resulting in a file name request that contains the device's MAC address, for example, config_00908F033512.ini. Therefore, you can configure all the devices with the same URL and file name.



Note: If you write the MAC address placeholder string in lower case (i.e., "<mac>"), the device adds the MAC address in lower case to the file name (e.g., config_<mac>.ini results in config_00908f053736e); if in upper case (i.e., "<MAC>"), the device adds the MAC address in upper case to the file name (e.g., config_<MAC>.ini results in config_00908F053736E).

40.2.4 File Template for Automatic Provisioning

To facilitate automatic provisioning setup, you can use a single template to define the files to download during automatic provisioning. The template uses special keywords to denote the different file types to download and in the URL address of the provisioning server it uses a placeholder for the file names which is replaced by hardcoded file names and extensions according to file type, as described in more detail below.



Note:

- Unlike the parameters that define specific URLs for Auxiliary files (e.g., CptFileURL), the file template feature always retains the URLs after each automatic update process. Therefore, with the file template the device always attempts to download the files upon each automatic update process.
- If you configure a parameter used to define a URL for a specific file (e.g., CptFileURL), the settings of the TemplateUrl parameter is ignored for the specific file type (e.g., CPT file).
- Additional placeholders can be used in the file name in the URL, for example, <MAC> for MAC address (see "MAC Address Placeholder in Configuration File Name" on page 619).

➤ To use a file template for automatic provisioning:

1. Define the file **types** to download by the file template, using the AupdFilesList parameter. Use the keywords listed in the table below to specify each file type. For example, to specify ini, License Key, and CPT files:

- ini File:

```
AupdFilesList = 'ini', 'fk', 'cpt'
```

- CLI:

```
# configure system
(config-system)# automatic update
(automatic-update)# template-files-list ini,fk,cpt
```

2. Define the URL address of the provisioning server on which the files (specified in Step 1) are located for download, using the TemplateUrl parameter. When you configure the URL, you must include the file type placeholder, "<FILE>", which represents the file name. For each file type specified in Step 1, the device sends an HTTP request to the server, where the placeholder in the URL is replaced with the filename and extension, as listed in the below table. For example, if you configure the AupdFilesList parameter as in Step 1 and the TemplateUrl parameter to:

- ini File:

```
TemplateUrl = 'http://10.8.8.20/Site1_<FILE>'
```

- CLI:

```
# configure system
(config-system)# automatic update
(automatic-update)# template-url http://10.8.8.20/Site1_<FILE>
```

The device sends HTTP requests to the following URLs:

- http://10.8.8.20/Site1_ **device.ini**
- http://10.8.8.20/Site1_ **fk.ini**
- http://10.8.8.20/Site1_ **cpt.data**

3. Place the files to download on the provisioning server. Make sure that their file names and extensions are based on the hardcoded string values specific to the file type for the <FILE> placeholder (e.g., "Site1_device.ini" for the ini file), as shown in the table

below.

Table 40-2: File Template Keywords and Placeholder Values per File Type

File Type	Keywords for Template File	Value Replacing <FILE> Placeholder
ini file	ini	device.ini
CLI Script file	cli	cliScript.txt
CMP file based on timestamp	acmp	autoFirmware.cmp
User Info file	usrinf	userInfo.txt
CMP file	cmp	firmware.cmp
License Key file	fk	fk.ini
Call Progress Tone (CPT) file	cpt	cpt.dat
Prerecorded Tones (PRT) file	prt	prt.dat
Dial Plan file	dpln	dialPlan.dat
Answering Machine Detection (AMD) file	amd	amd.dat
SSL/TLS Private Key file	sslp	pkey.pem pkey<ID>.pem (for multi-certificate system)
SSL/TLS Root Certificate file	sslr	root.pem root<ID>.pem (for multi-certificate system)
SSL/TLS Certificate file	sslc	cert.pem cert<ID>.pem (for multi-certificate system)

40.2.5 Triggers for Automatic Update

The Automatic Update feature can be triggered by the following:

- Upon device startup (reset or power up). To disable this trigger, run the following CLI command:


```
(config-system)# automatic-update
(automatic-update)# run-on-reboot off
```
- Periodically:
 - Specified time of day (e.g., 18:00), configured by the ini file parameter AutoUpdatePredefinedTime or CLI command `configure system > automatic-update > predefined-time`.
 - Interval between Automatic Updates (e.g., every 60 minutes), configured by the ini file parameter AutoUpdateFrequency or CLI command `configure system > automatic-update > update-frequency`.
- Centralized provisioning server request:
 - Upon receipt of an SNMP request from the provisioning server.


- Upon receipt of a special SIP NOTIFY message from the provisioning server. The NOTIFY message includes an Event header with the AudioCodes proprietary value, "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
```

To enable the feature:

- Open the Gateway Advanced Settings page (**Setup** menu > **Signaling & Media** tab > **Gateway** folder > **Gateway Advanced Settings**).
- From the 'Remote Management by Notify' (EnableSIPRemoteReset) drop-down list, select **Enable**:

Figure 40-2: Resetting Device by SIP NOTIFY



- Click **Apply**.

To enable through CLI: configure voip > sip-definition advanced-settings > sip-remote-reset.

40.2.6 Access Authentication with HTTP Server

You can configure the device to authenticate itself with the HTTP/S server. The device authenticates itself by providing the HTTP/S server with its authentication username and password. You can configure one of the following HTTP authentication schemes:

- **Basic Access Authentication:** The device provides its username and password to the HTTP server. The username and password is configured in the URL that you define for downloading the file:
 - ini file:


```
AutoCmpFileUrl = 'https://<username>:<password>@<IP address or domain name>/<file name>'
```
 - CLI:


```
# configure system
(config-system)# automatic update
(automatic-update)# auto-firmware https://<username>:<password>@<IP address or domain name>/<file name>
```
- **Digest Access Authentication:** The authentication username and password is negotiated between the device and HTTP/S server, using digest MD5 cryptographic hashing. This method is safer than basic access authentication. The digest authentication username and password are configured using the AUPDDigestUsername and AUPDDigestPassword parameters, respectively.

40.2.7 Querying Provisioning Server for Updated Files

Each time the Automatic Update feature is triggered, for each file and its configured URL the device does the following:

1. If you have configured the device to authenticate itself to the HTTP/S server for secure access, the device sends the access authentication username and password to the HTTP/S server (for more information, see "Access Authentication with HTTP Server" on page 622). If authentication succeeds, Step 2 occurs.
2. The device establishes an HTTP/S connection with the URL host (provisioning

server). If the connection is HTTPS, the device verifies the certificate of the provisioning server, and presents its own certificate if requested by the server.

3. The device queries the provisioning server for the requested file by sending an HTTP Get request. This request contains the HTTP User-Agent Header, which identifies the device to the provisioning server. By default, the header includes the device's model name, MAC address, and currently installed software and configuration versions. Based on its own dynamic applications for logic decision making, the provisioning server uses this information to check if it has relevant files available for the device and determines which files must be downloaded (working in conjunction with the HTTP If-Modified-Since header, described further on in this section).

You can configure the information sent in the User-Agent header, using the `AupdHttpUserAgent` parameter or CLI command, `configure system > http-user-agent`. The information can include any user-defined string or the following supported string variable tags (case-sensitive):

- **<NAME>**: product name, according to the installed License Key
- **<MAC>**: device's MAC address
- **<VER>**: software version currently installed on the device, e.g., "7.00.200.001"
- **<CONF>**: configuration version, as configured by the ini file parameter, `INIFileVersion` or CLI command, `configuration-version`

The device automatically populates these tag variables with actual values in the sent header. By default, the device sends the following in the User-Agent header:

```
User-Agent: Mozilla/4.0 (compatible; AudioCodes;
<NAME>; <VER>; <MAC>; <CONF>)
```

For example, if you set `AupdHttpUserAgent = MyWorld-<NAME>;<VER>(<MAC>)`, the device sends the following User-Agent header:

```
User-Agent: MyWorld-Mediant;7.00.200.001(00908F1DD0D3)
```



Note: If you configure the `AupdHttpUserAgent` parameter with the `<CONF>` variable tag, you must reset the device with a save-to-flash for your settings to take effect.

4. If the provisioning server has relevant files available for the device, the following occurs, depending on file type and configuration:

- **File Download upon each Automatic Update process:** This is applicable to software (.cmp) and configuration files. In the sent HTTP Get request, the device uses the HTTP If-Modified-Since header to determine whether to download these files. The header contains the date and time (timestamp) of when the device last downloaded the file from the specific URL. This date and time is regardless of whether the file was installed or not on the device. An example of an If-Modified-Since header is shown below:

```
If-Modified-Since: Mon, 1 January 2014 19:43:31 GMT
```

If the file on the provisioning server was unchanged (not modified) since the date and time specified in the header, the server replies with an HTTP 304 response and the file is not downloaded. If the file was modified, the provisioning server sends an HTTP 200 OK response with the file in the body of the HTTP response. The device downloads the file and compares the version of the file with the currently installed version on its flash memory. If the downloaded file is of a later version, the device installs it after the device resets (which is only done after the device completes all file downloads); otherwise, the device does not reset and does not install the file.

To enable the automatic software (.cmp) file download method based on this timestamp method, use the ini file parameter, `AutoCmpFileUrl` or CLI command,

configure system > automatic-update > auto-firmware <URL>. The device uses the same configured URL to download the .cmp file for each subsequent Automatic Update process.

You can also enable the device to run a CRC on the downloaded configuration file to determine whether the file has changed in comparison to the previously downloaded file. Depending on the CRC result, the device can install or discard the downloaded file. For more information, see "Cyclic Redundancy Check on Downloaded Configuration Files" on page 626.



Note:

- When this method is used, there is typically no need for the provisioning server to check the device's current firmware version using the HTTP-User-Agent header.
- The Automatic Update feature assumes that the 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 ini file parameter AutoUpdateFrequency or CLI command configure system > automatic update > update-frequency.

- **One-time File Download:** This is applicable to software (.cmp) and Auxiliary (e.g., License Key, CPT and Dial Plan) files. The device downloads these files only **once**, regardless of how many times the device may repeat the Automatic Update process. Once they are downloaded, the device discards their configured URLs. To update these files again, you need to configure their URL addresses and filenames again. Below is an example of how to configure URLs for some of these files:

Auxiliary Files:

- ◆ ini:

```
CptFileURL =
'https://www.company.com/call_progress.dat '
FeatureKeyURL =
'https://www.company.com/License_Key.txt '
```

- ◆ CLI:

```
(config-system)# automatic-update
(automatic-update)# call-progress-tones
http://www.company.com/call_progress.dat
(automatic-update)# tls-root-cert https://company.com/root.pem
```

Software (.cmp) File:

- ◆ ini:

```
CmpFileUrl =
'https://www.company.com/device/v.7.20A.000.038.cmp '
```

- ◆ CLI:

```
(config-system)# automatic-update
(automatic-update)# firmware
https://www.company.com/device/v.7.20A.000.038.cmp
```


**Note:**

- For one-time file download, the HTTP Get request sent by the device does not include the If-Modified-Since header. Instead, the HTTP-User-Agent header can be used in the HTTP Get request to determine whether firmware update is required.
- When downloading SSL certificate files, it is recommended to use HTTPS with mutual authentication for secure transfer of the SSL Private Key.
- After the device downloads the License Key file (FeatureKeyURL), it checks that the serial number in the file ("S/N <serial number>") is the same as that of the device. If the serial number is the same and the license key is different to the one currently installed on the device, it applies the new License Key. For devices in HA mode, the License Key is applied to both active and redundant units.

5. If the device receives an HTTP 301/302/303 redirect response from the provisioning server, it establishes a connection with the new server at the redirect URL and re-sends the HTTP Get request.

40.2.8 File Download Sequence

Whenever the Automatic Update feature is triggered (see "Triggers for Automatic Update" on page 621), the device attempts to download each file from the configured URLs, in the following order:

1. ini file
2. CLI Script file
3. Periodic software file (.cmp) download
4. One-time software file (.cmp) download
5. Auxiliary file(s)

The following files automatically instruct the device to reset:

- Periodic software file (.cmp)
- One-time software file (.cmp)

When multiple files requiring a reset are downloaded, the device resets only **after** it has downloaded and installed **all** the files. However, you can explicitly instruct the device to immediately reset for the following files:

- ini file: Use the ResetNow in file parameter
- CLI Script file: Use the reload if-needed CLI command



Warning: If you use the ResetNow parameter in an ini file for periodic automatic provisioning with non-HTTP (e.g., TFTP) and without CRC, the device resets after every file download. Therefore, use the parameter with caution and only if necessary for your deployment requirements.

**Note:**

- For ini file downloads, by default, parameters not included in the file are set to defaults. To retain the current settings of these parameters, set the SetDefaultOnINIFileProcess parameter to 0.
- If you have configured one-time software file (.cmp) download (configured by the ini file parameter CmpFileURL or CLI command configure system > automatic-update > firmware), the device will only apply the file if one-time software updates are enabled. This is disabled by default to prevent unintentional software upgrades. To enable one-time software upgrades, set the ini file parameter AutoUpdateCmpFile to 1 or CLI command, configure system > automatic-update > update-firmware on.
- If you need to update the device's software and configuration, it is recommended to first update the software. This is because the current ("old") software (before the upgrade) may not be compatible with the new configuration. However, if both files are available for download on the provisioning server(s), the device first downloads and applies the new configuration, and only then does it download and install the new software. Therefore, this is a very important issue to take into consideration.
- If more than one file needs to be updated - CLI Script and cmp: The device downloads and applies the CLI Script file on the currently ("old") installed software version. It then downloads and installs the cmp file with a reset. Therefore, the CLI Script file MUST have configuration compatible with the "old" software version.

40.2.9 Cyclic Redundancy Check on Downloaded Configuration Files

You can enable the device to perform cyclic redundancy checks (CRC) on downloaded configuration files during the Automatic Update process. The CRC checks whether the content (raw data) of the downloaded file is different to the content of the previously downloaded file from the previous Automatic Update process. The device compares the CRC check value (code) result with the check value of the previously downloaded file. If the check values are identical, it indicates that the file has no new configuration settings, and the device discards the file. If the check values are different, it indicates that the downloaded file is different (i.e., includes updates), and the device installs the downloaded file and applies the new configuration settings.

CRC is useful, for example, when the service provider replaces a file, on the provisioning server, with another file whose contents are the same. When the device sends an HTTP Get request during the Automatic Update process, the provisioning server sends the new file to the device. This occurs as the timestamp between the previously downloaded file and this new file is different (determined by the HTTP If-Modified-Since header in the Get request). Therefore, the CRC feature can be used to prevent the device from installing such files.

For enabling CRC, use the ini file parameter AUPDCheckIfIniChanged or CLI command, configure system > automatic-update > crc-check regular. By default, CRC is disabled. For more information on the parameter, see "Automatic Update Parameters" on page 743.

40.2.10 Automatic Update Configuration Examples

This section provides a few examples on configuring the Automatic Update feature.

40.2.10.1 Automatic Update for Single Device

This simple example describes how to configure the Automatic Update feature for updating a single device. In this example, the device queries the provisioning server for software, configuration and Auxiliary files every 24 hours.

➤ **To set up Automatic Provisioning for single device (example):**

1. Set up an HTTP Web server (e.g., <http://www.company.com>) and place all the required configuration files on this server.
2. Configure the device with the IP address of the DNS server for resolving the domain name (e.g., <http://www.company.com>) that is used in the URL of the provisioning server. You configure this in the IP Interfaces table:

- ini File:

```
[ InterfaceTable ]
FORMAT InterfaceTable_Index =
InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_VlanID, InterfaceTable_InterfaceName,
InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress,
InterfaceTable_UnderlyingDevice;
InterfaceTable 0 = 6, 10, 10.15.7.95, 16, 10.15.0.1, 1,
"Voice", 80.179.52.100, 0.0.0.0, "vlan 1";
[ \InterfaceTable ]
```

- CLI:

```
# configure network
(config-network)# interface network-if 0
(network-if-0)# primary-dns 80.179.52.100
```

3. Configure the device with the following Automatic Update settings:

- a. Automatic Update is done every 24 hours (1440 minutes):

- ◆ ini File:

```
AutoUpdateFrequency = 1440
```

- ◆ CLI:

```
# configure system
(config-system)# automatic update
(automatic-update)# update-frequency 1440
```

- b. Automatic Update of software file (.cmp):

- ◆ ini File:

```
AutoCmpFileUrl = 'https://www.company.com/sw.cmp'
```

- ◆ CLI:

```
# configure system
(config-system)# automatic update
(automatic-update)# auto-firmware 'http://www.company.com/sw.cmp'
```

- c. Automatic Update of Call Progress Tone file:

- ◆ ini File:

```
CptFileURL =
'https://www.company.com/call_progress.dat'
```

- ◆ CLI:

```
# configure system
(config-system)# automatic update
(automatic-update)# call-progress-tones
'http://www.company.com/call_progress.dat'
```

- d. Automatic Update of ini configuration file:

- ◆ ini File:

```
IniFileURL = 'https://www.company.com/config.ini'
```

- ◆ CLI:

```
# configure system
(config-system)# automatic update
(automatic-update)# voice-configuration
'http://www.company.com/config.ini'
```

- e. Enable Cyclical Redundancy Check (CRC) on downloaded ini file:

- ◆ ini File:

```
AUPDCheckIfIniChanged = 1
```

- ◆ CLI:

```
# configure system
(config-system)# automatic update
(automatic-update)# crc-check regular
```

4. Power down and then power up the device.

40.2.10.2 Automatic Update from Remote Servers

This example describes how to configure the Automatic Update feature where files are stored and downloaded from different file server types. The example scenario includes the following:

- FTPS server at ftpserver.corp.com for storing the License Key file. The login credentials to the server are username "root" and password "wheel".
- HTTP server at www.company.com for storing the configuration file.
- DNS server at 80.179.52.100 for resolving the domain names of the provisioning servers (FTPS and HTTP).

➤ To set up Automatic Provisioning for files stored on different server types (example):

1. License Key file:

- a. Set up an FTPS server and copy the License Key file to the server.
- b. Configure the device with the URL path of the License Key file:

- ◆ ini File:

```
FeatureKeyURL =
'ftps://root:wheel@ftpserver.corp.com/license_key.txt'
```

- ◆ CLI:

```
# configure system
(config-system)# automatic update
(automatic-update)# feature-key
'ftps://root:wheel@ftpserver.corp.com/license_key.txt'
```

2. Software (.cmp) and ini files:

- a. Set up an HTTP Web server and copy the .cmp and configuration files to the server.
- b. Configure the device with the URL paths of the .cmp and ini files:

- ◆ ini File:

```
AutoCmpFileUrl =
'http://www.company.com/device/sw.cmp'
IniFileURL = 'http://www.company.com/device/inifile.ini'
```

◆ CLI:

```
# configure system
(config-system)# automatic update
(automatic-update)# auto-firmware 'http://www.company.com/sw.cmp'
```

3. Configure the device with the IP address of the DNS server for resolving the domain names of the FTPS and HTTP servers:

```
[ InterfaceTable ]
FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_VlanID, InterfaceTable_InterfaceName,
InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress,
InterfaceTable_UnderlyingDevice;
InterfaceTable 0 = 6, 10, 10.15.7.95, 16, 10.15.0.1, 1,
"Voice", 80.179.52.100, 0.0.0.0, "vlan 1";
[ \InterfaceTable ]
```

4. Configure the device to perform the Automatic Update process daily at 03:00 (3 a.m):

- ini File:

```
AutoUpdateFrequency = '03:00'
```

- CLI:

```
# configure system
(config-system)# automatic update
(automatic-update)# update-frequency 03:00
```

40.2.10.3 Automatic Update for Mass Deployment

This example describes how to configure the Automatic Update feature for updating multiple devices (i.e., mass deployment) using an HTTP provisioning server. In this example, all the devices are configured to download the same "master" configuration file. This file serves as the configuration template and instructs the devices which files to download and how often to perform the Automatic Update process. In addition, the master file also instructs each device to download an ini configuration file whose file name contains the MAC address of the device.

The example scenario is as follows:

- All devices download a "master" configuration file that contains the following:
 - Common configuration shared by all device's.
 - Specific configuration that instructs each device to download a specific configuration file based on the device's MAC address, using the special string "<MAC>" in the URL, as described in "MAC Address Placeholder in Configuration File Name" on page 619.
- Device queries the provisioning server daily at 24:00 (midnight) for software, configuration and Auxiliary files.
- HTTP-based provisioning server at www.company.com for storing the files.
- DNS server at 80.179.52.100 for resolving the domain name of the provisioning server.

➤ **To set up automatic provisioning for mass provisioning (example):**

1. Create a "master" configuration file template named "master_configuration.ini" with the following settings:

- Common configuration for all devices:

- ◆ ini file:

```
AutoUpdatePredefinedTime = '24:00'
CptFileURL = 'https://www.company.com/call_progress.dat'
AutoCmpFileUrl = 'https://www.company.com/sw.cmp'
```

- ◆ CLI:

```
# configure system
(config-system)# automatic update
(automatic-update)# update-frequency 24:00
(automatic-update)# call-progress-tones
https://www.company.com/call_progress.dat
(automatic-update)# auto-firmware https://www.company.com/sw.cmp
```

- Configuration per device based on MAC address:

- ◆ ini file:

```
IniFileURL = 'http://www.company.com/config_<MAC>.ini'
```

- ◆ CLI:

```
# configure system
(config-system)# automatic update
(automatic-update)# cli-script
https://company.com/files/cli_script_<MAC>.txt
(automatic-update)# voice-configuration
http://www.company.com/config_<MAC>.ini
```

2. Copy the master configuration file that you created in Step 1 as well as the CPT and .cmp files to the HTTP-based provisioning server.

3. Configure **each** device with the following:

- a. URL of the master configuration file:

- ◆ ini File:

```
IniFileURL =
'http://www.company.com/master_configuration.ini'
```

- ◆ CLI:

```
# configure system
(config-system)# automatic update
(automatic-update)# voice-configuration
http://www.company.com/master_configuration.ini
(automatic-update)# cli-script
https://company.com/files/master_startup.txt
```

- b. Configure the device with the IP address of the DNS server for resolving the domain name (e.g., http://www.company.com) that is used in the URL for the provisioning server. This is done in the IP Interfaces table:

- ◆ ini File:

```
[ InterfaceTable ]
FORMAT InterfaceTable_Index =
InterfaceTable_ApplicationTypes,
InterfaceTable_InterfaceMode, InterfaceTable_IPAddress,
InterfaceTable_PrefixLength, InterfaceTable_Gateway,
InterfaceTable_VlanID, InterfaceTable_InterfaceName,
InterfaceTable_PrimaryDNSServerIPAddress,
InterfaceTable_SecondaryDNSServerIPAddress,
InterfaceTable_UnderlyingDevice;
InterfaceTable 0 = 6, 10, 10.15.7.95, 16, 10.15.0.1, 1,
```

```
"Voice", 80.179.52.100, 0.0.0.0, "vlan 1";  
[ \InterfaceTable ]
```

◆ CLI:

```
# configure network  
(config-network)# interface network-if 0  
(network-if-0)# primary-dns 80.179.52.100
```

4. Power down and then power up the device.

This page is intentionally left blank.

41 Restoring Factory Defaults

This section describes how to restore the device's configuration to factory defaults.

41.1 Restoring Factory Defaults through CLI

You can restore the device to factory defaults through CLI, as described in the following procedure.

➤ **To restore factory defaults through 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
```

41.2 Restoring Factory Defaults through Web Interface

You can restore the device to factory defaults through the Web interface.



Note: When restoring to factory defaults, you can preserve your IP network settings that are configured in the IP Interfaces table (see "Configuring IP Network Interfaces" on page 130), as described in the procedure below. This may be important, for example, to maintain connectivity with the device (through the OAMP interface) after factory defaults have been applied.

➤ **To restore factory defaults through Web interface:**

1. Open the Configuration File page:
 - **Toolbar:** From the **Actions** drop-down menu, choose **Configuration File**.
 - **Navigation tree:** **Setup** menu > **Administration** tab > **Maintenance** folder > **Configuration File**.

Figure 41-1: Restoring Factory Defaults through Web

RESTORE THE DEFAULT CONFIGURATION OF THE DEVICE.

Restore Defaults

Preserve Network configuration.

2. To keep your current IP network settings, select the **Preserve Network Configuration** check box. To overwrite all your IP network settings with the default IP network interface, clear the **Preserve Network Configuration** check box.
3. Click the **Restore Defaults** button; a message appears requesting you to confirm.
4. Click **OK** to confirm or **Cancel** to return to the page.
5. Once the device is restored to factory defaults, reset the device for the settings to take effect.

41.3 Restoring Defaults through ini File

You can restore the device to factory defaults, 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 613). If the *ini* file includes parameter settings, 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) LAN IP address and the Web interface's login username and password.

Part IX

Status, Performance Monitoring and Reporting

42 System Status

This section describes how to view various system statuses.

42.1 Viewing Device Information

You can view hardware and software information about the device on the Device Information page. The page also lists Auxiliary files that have been installed on the device and allows you to remove them (see "Deleting Auxiliary Files" on page 587).

➤ **To view device information:**

- Open the Device Information page (**Monitor** menu > **Monitor** menu > **Summary** tab > **Device Information**).

Figure 42-1: Viewing Device Information (Example)

GENERAL SETTINGS		LOADED FILES	
MAC Address:	00908f3b463f	Loaded Call Progress Tones:	Default Progress Tones
Serial Number:	3884606	User Info File Name:	userInfoSBC3000.txt Delete
Board Type:	Mediant		
Device Up Time:	1d:21h:52m:18s:12th		
Device Administrative State:	Unlocked		
Device Operational State:	Enabled		
Flash Size [Mbytes]:	252		
RAM Size [Mbytes]:	4015		
CPU Speed [MHz]:	1250		

VERSIONS	
Version ID:	7.10A.045.002
DSP Type:	1
DSP Software Version:	72013
DSP Software Name:	5039AE3_R
Flash Version:	560

42.2 Viewing Device Status on Monitor Page

The Web interface's Monitor page provides basic status and information on the device. The page is useful in that it allows you to easily obtain an overview of the device's operating status at a single glance.

➤ **To view device status and information on the Monitor home page:**

- On the Menu bar, click **Monitor** or if you are already in the Monitor menu's Navigation tree, click [🏠 Monitor](#).

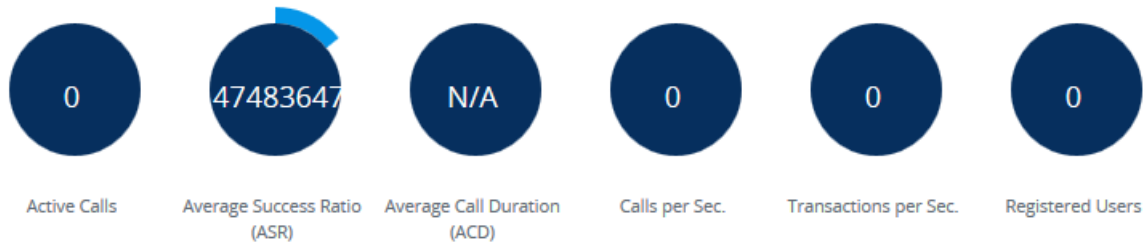
The Monitor page displays the following groups of information:

- **Device Information pane:**

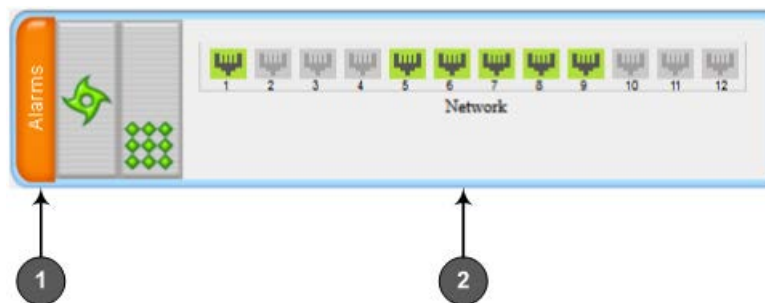
- 'Address': IP address of the device's OAMP interface

- 'Firmware': Software version currently running on the device
 - 'Type': Name of the device
 - 'HA Status': High-Availability (HA) status of the device, if configured for HA. For more information, see Viewing HA Status on Monitor Web Page on page 558.
- SBC Call Statistics:
- Active Calls: Total number of SBC calls. The corresponding SNMP performance monitoring MIB is PM_gwInINVITEDialogs.
 - Average Success Rate (ASR): Number of successfully answered calls out of the total number of attempted calls. The corresponding SNMP performance monitoring MIB is PM_gwSBCASR.
 - Average Call Duration (ACD): Average call duration in seconds of established calls. The value is refreshed every 15 minutes and therefore, this value reflects the average duration of all established calls made within a 15 minute period. The corresponding SNMP performance monitoring MIB is PM_gwSBCACD.
 - Calls per Sec: Total number of new calls per second (CPS).
 - Transactions per Sec: Total number of new SIP transactions per second (out-of-dialog transactions such as INVITE and REGISTER, or in-dialog transactions such as UPDATE and BYE). The corresponding SNMP performance monitoring MIB is PM_gwActiveSIPTransacionsPerSecond. The counter is applicable to SBC and Gateway calls.
 - Registered Users: Number of users registered with the device. The corresponding SNMP performance monitoring MIB is PM_gwSBCRegisteredUsers.

Figure 42-2: Viewing Call Statistics on Monitor Page





- Graphical display of the device with color-coded status icons, as shown in the figure below and described in the subsequent table:



Note: For a description of the Monitor page when the device is in High Availability (HA) mode, see HA Status Display on Monitor Web Page on page 558.

Table 42-1: Description of Graphical Display of Device

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 643).</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 663).</p>

This page is intentionally left blank.

43 Reporting DSP Utilization through SNMP MIB

You can obtain information on the percentage of DSP resources utilized by the device, through the SNMP MIB table, `acPMDSPUsage`. You can also configure low and high DSP utilization thresholds for this MIB, that if crossed, the SNMP trap event, `acPerformanceMonitoringThresholdCrossing` is sent by the device. For more information on this MIB, refer to the *SNMP Reference Guide*.

This page is intentionally left blank.

44 Viewing Carrier-Grade Alarms

This section describes how to view SNMP alarms raised by the device.

44.1 Viewing Active Alarms

You can view current (active) alarms in the Web interface that have been raised by the device. If an alarm is cleared, it is moved into the History Alarms table (see "Viewing History Alarms" on page 644).



Note:

- The alarms in the table are deleted upon a device reset.
- For more information on SNMP alarms, refer to the *SNMP Reference Guide* document.

➤ **To view active alarms:**

- Open the Active Alarms table, by doing one of the following:
 - Navigation tree: **Monitor** menu > **Monitor** tab > **Summary** folder > **Active Alarms**.
 - Monitor home page: Click the "Alarms" area on the graphical display of the device (see "Viewing Device Status on Monitor Page" on page 637).

SEQUENTIAL #	SEVERITY	SOURCE	DESCRIPTION	TIME
1	Major	Board#1	Network element admin state change alarm. Gateway is locked	27/11/2010, 12:22:53
2	Minor	Board#1/EthernetLink#2	Ethernet link alarm. LAN port number 2 is down.	27/11/2010, 12:22:55
3	Minor	Board#1/EthernetLink#3	Ethernet link alarm. LAN port number 3 is down.	27/11/2010, 12:22:55
4	Minor	Board#1/EthernetLink#4	Ethernet link alarm. LAN port number 4 is down.	27/11/2010, 12:22:55

Table 44-1: Active Alarms Table Description

Field	Description
Sequential Number	The number of the alarm. The alarms are numbered sequentially as they are raised by the device. The numbering resets to 1 immediately after a device reset (i.e., the first alarm raised after a reset is assigned the number #1).
Severity	Severity level of the alarm: <ul style="list-style-type: none"> ▪ Critical (red) ▪ Major (orange) ▪ Minor (yellow)
Source	Component of the device from which the alarm was raised.
Description	Brief description of the alarm.
Date	Date (DD/MM/YYYY) and time (HH:MM:SS) the alarm was raised.

44.2 Viewing History Alarms

You can view all SNMP alarms, in the Web interface's Alarms History table, that have been raised (active alarms) as well as cleared (resolved). One of the benefits of this is that you can view alarms that may have been raised and then cleared on a continuous basis. For example, such an alarm may be raised due to an Ethernet cable that is not securely attached to the device's Ethernet port, causing the Ethernet link to be sometimes up and sometimes down. This alarm would not be listed in the Active Alarms table due to it being cleared. The Alarms History table displays both the cleared alarm and the alarm for which it was cleared adjacent to one another, as shown in the figure below for alarms #9 and #10.

To configure the maximum number of alarms that can be displayed in the table, use the AlarmHistoryTableMaxSize ini file parameter. If the maximum is reached and a new alarm is added to the table, the oldest alarm is removed from the table to accommodate the new alarm.



Note:

- The alarms in the table are deleted upon a device reset.
- For more information on SNMP alarms, refer to the *SNMP Reference Guide* document.

➤ **To view history alarms:**

- Open the Alarms History table (**Monitor** menu > **Monitor** tab > **Summary** folder > **Alarms History**).

Figure 44-1: Viewing Alarms History Table

SEQUENTIAL #	SEVERITY	SOURCE	DESCRIPTION	TIME
1	Major	Board#1	Network element admin state change alarm. Gateway is locked	27/11/2010, 12:22:53
2	Minor	Board#1/EthernetLink#2	Ethernet link alarm. LAN port number 2 is down.	27/11/2010, 12:22:55
3	Minor	Board#1/EthernetLink#3	Ethernet link alarm. LAN port number 3 is down.	27/11/2010, 12:22:55
4	Minor	Board#1/EthernetLink#4	Ethernet link alarm. LAN port number 4 is down.	27/11/2010, 12:22:55
7	Major	Board#1/ProxyConnection#0	Proxy Set Alarm Proxy Set 0: Proxy lost. looking for another pro:	17/03/2010, 16:30:01
8	Cleared	Board#1/ProxyConnection#0	Alarm cleared: Proxy Set Alarm Proxy Set 0: Proxy lost. looking	17/03/2010, 16:30:01
9	Major	Board#1/ProxyConnection#1	Proxy Set Alarm Proxy Set 1: Proxy lost. looking for another pro:	17/03/2010, 16:30:01
10	Cleared	Board#1/ProxyConnection#1	Alarm cleared: Proxy Set Alarm Proxy Set 1: Proxy lost. looking	17/03/2010, 16:30:01

Table 44-2: Alarms History Table Description

Field	Description
Sequential Number	The number of the alarm. The alarms are numbered sequentially as they are raised by the device. The numbering resets to 1 immediately after a device reset (i.e., the first alarm raised after a reset is assigned the number #1).
Severity	Severity level of the alarm: <ul style="list-style-type: none"> ▪ Critical (red) ▪ Major (orange) ▪ Minor (yellow) ▪ Cleared (green)
Source	Component of the device from which the alarm was raised.
Description	Brief description of the alarm.

Field	Description
Date	Date (DD/MM/YYYY) and time (HH:MM:SS) the alarm was raised.

➤ **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.

This page is intentionally left blank.

45 Viewing Management User Activity Logs

If you have enabled the reporting of management user activities performed in the device's management interfaces (see "Configuring Reporting of Management User Activities" on page 705), you can view the logged activities in the Web interface, as described in the procedure below.

➤ **To view management user activity logs:**

- Open the Activity Log table (**Monitor** menu > **Monitor** tab > **Summary** folder > **Activity Log**).

Figure 45-1: Viewing Management User Activity Log

ID ↕	TIME	DESCRIPTION	USER	INTERFACE	CLIENT
7	11/29/2010, 11:44:45	CLI: 'enable'	Admin	Telnet	10.13.2.3
6	11/29/2010, 11:44:43	User login succeeded	Admin	Telnet	10.13.2.3
5	11/29/2010, 11:40:38	System configuration has be	Admin	WEB	10.13.2.3
4	11/29/2010, 11:40:27	WEB: Successful login at 10	Admin	WEB	10.13.2.3
3	11/29/2010, 11:40:24	WEB: User logout	Admin	WEB	10.13.2.3
2	11/29/2010, 11:40:16	SRTP Tunneling Authenticati	Admin	WEB	10.13.2.3
1	11/29/2010, 11:39:58	System configuration has be	Admin	WEB	10.13.2.3

Table 45-1: Activity Log Table Description

Parameter	Description
Time	Date (mm/dd/yyyy) and time (hh:mm:ss) that the activity was performed.
Description	Description of the activity.
User	Username of the user account that performed the activity.
Interface	Protocol used for connecting to the management interface (e.g., Telnet, SSH, Web, or HTTP).
Client	IP address of the client PC from where the user accessed the management interface.

This page is intentionally left blank.

46 Viewing Performance Monitoring

This section describes how to view performance monitoring in the device's Web interface.

46.1 Viewing Call Success and Failure Ratio

You can view success and failure ratio of SIP dialogs in the Web interface's Success/Failure Ratio page. You can filter the display by a specific SRD or IP Group, and by call direction and type of SIP dialog (e.g., INVITEs only). The information is displayed in the following pie charts:

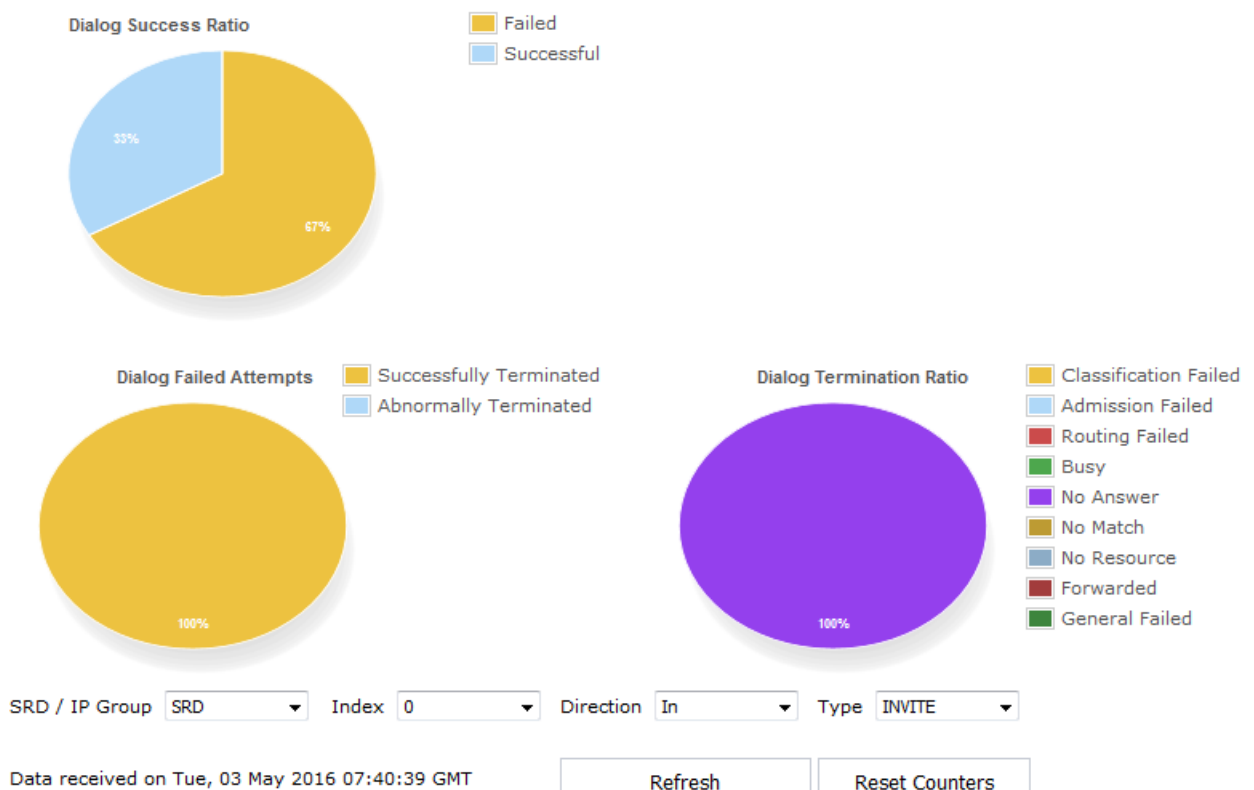
- **Dialog Success Ratio:** Displays the SIP call and subscribe (SUBSCRIBE) dialog success-failed ratio.
- **Dialog Failed Attempts:** Displays failed SIP dialog attempts. This includes the number of calls and subscribes which were successfully and abnormally terminated.
- **Dialog Termination Ratio:** Displays SIP dialog termination by reason (e.g., due to no answer).

➤ **To view success and failed call ratio:**

1. Open the Success/Failure Ratio page (**Monitor** menu > **Monitor** tab > **Performance Monitoring** folder > **Success / Failure Ratio**).

Figure 46-1: Viewing Success/Failure Ratio

Success/Failure Ratio



2. From the 'SRD/IP Group' drop-down list, select whether you want to view statistic for an SRD or IP Group.
3. From the 'Index' drop-down list, select the SRD or IP Group index.

4. From the 'Direction' 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

If there is no data for the charts, the chart appears gray and "No Data" is displayed to the right of the chart.

➤ **To refresh the charts:**

- Click **Refresh**.

➤ **To reset the counters:**

- Click **Reset Counters**.

46.2 Viewing Average Call Duration

You can view the number of currently active calls and the average call duration (ACD) in the Web interface's Average Call Duration page. You can filter display by a specific SRD or IP Group. The page displays the following two graphs:



- **Upper graph:** Displays the number of currently active calls (INVITEs). The x-axis indicates the time (hh:mm:ss) and the y-axis the number of calls.
- **Lower graph:** Displays the ACD. The x-axis indicates the time (hh:mm:ss) and the y-axis the average call duration. The ACD is refreshed every 15 minutes and therefore, this value reflects the average duration of all established calls made within a 15 minute period.

- **To view number of active calls and average call duration:**
- 1. Open the Average Call Duration page (**Monitor** menu > **Monitor** tab > **Performance Monitoring** folder > **Average Call Duration**).

Figure 46-2: Viewing Average Call Duration



2. From the 'SRD / IP Group' drop-down list, select the configuration entity (SRD or IP Group).
3. From the 'Index' drop-down list, select the specific 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 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.

46.3 Configuring Performance Profiles

The Performance Profile table lets you configure up to 6,303 Performance Profile rules. A Performance Profile rule defines thresholds of performance monitoring call metrics for Major and Minor severity alarms. If the threshold is crossed, the device raises the corresponding severity alarm. You can configure a Performance Profile rule for all calls (*globally*), or per SRD or IP Group.

You can configure the alarm thresholds for the following call metrics:

- **Answer Success Ratio or ASR (also known as Answer Seizure Ratio):** The number (in percentage) of answered calls (i.e. number of seizures resulting in an answer signal) out of the total number of attempted calls (seizures). The metric is calculated for the outgoing call leg. The metric includes the following SNMP performance monitoring MIBs:
 - PM_gwSBCASR: ASR for all (global) entities (i.e., all IP Groups and SRDs)

- PM_gwSBCIPGroupASR: ASR per IP Group
- PM_gwSBCSRDASR: ASR per SRD

If the configured ASR minor or major thresholds are crossed, the device raises the SNMP alarm, acASRThresholdAlarm (OID 1.3.6.1.4.1.5003.9.10.1.21.2.0.111).

To view ASR in the Web interface, see "Viewing Call Success and Failure Ratio" on page 649.

- **Network Effectiveness Ratio (NER):** The number (in percentage) of successfully connected calls out of the total number of attempted calls (seizures). The metric measures the ability of the network to deliver a call to the called terminal. In addition to answered calls, the following SIP response codes are regarded as successfully connected calls: 408 (Request Timeout), 480 (Temporarily Unavailable), and 486 (Busy Here). The metric is calculated for the outgoing call leg. The metric includes the following SNMP performance monitoring MIBs:

- PM_gwSBCNER: NER for all (global) entities (i.e., all IP Groups and SRDs)
- PM_gwSBCIPGroupNER: NER per IP Group
- PM_gwSBCSRDNER: NER per SRD

If the configured NER minor or major thresholds are crossed, the device raises the SNMP alarm, AcNERThresholdAlarm (OID 1.3.6.1.4.1.5003.9.10.1.21.2.0.113).

- **Average Call Duration (ACD):** The ACD plus the session disconnect time (SDD) is the duration from when the SIP 200 OK is received to when the SIP Bye message is sent. The metric is calculated for both incoming and outgoing call legs. The metric includes the following SNMP performance monitoring MIBs:

- PM_gwSBCACD: ACD for all (global) entities (i.e., all IP Groups and SRDs)
- PM_gwSBCIPGroupACD: ACD per IP Group
- PM_gwSBCSRDACD: ACD per SRD

If the configured ACD minor or major thresholds are crossed, the device raises the SNMP alarm, acACDThresholdAlarm (OID 1.3.6.1.4.1.5003.9.10.1.21.2.0.112).

To view ACD in the Web interface, see "Viewing Average Call Duration" on page 650.

At any given time during a call, a voice metric can be in one of the following color-coded quality states (as displayed by SEM):

- **Green:** Indicates good call quality
- **Yellow:** Indicates fair call quality
- **Red:** Indicates poor call quality

When the threshold of a voice metric is crossed, the device changes the alarm severity and corresponding color-coded quality state of the call:

- **Minor Threshold (Yellow):** Lower threshold that indicates changes from Green or Red to Yellow.
- **Major Threshold (Red):** Higher threshold that indicates changes from Green or Yellow to Red.

The device also uses hysteresis to determine whether the threshold has indeed being crossed. Hysteresis defines the amount of fluctuation from the threshold in order for the threshold to be considered as crossed (i.e., change in color state). Hysteresis is used to avoid false reports being sent by the device. Hysteresis is used only for threshold crossings toward a lesser severity (i.e., from Red to Yellow, Red to Green, or Yellow to Green).

The following example is used to explain how the device considers threshold crossings. The example is based on the ASR of a call, where the Major threshold is configured to 70%, the Minor threshold to 90% and the hysteresis for both thresholds to 2%:

Figure 46-3: Example of Threshold Crossings (ASR)

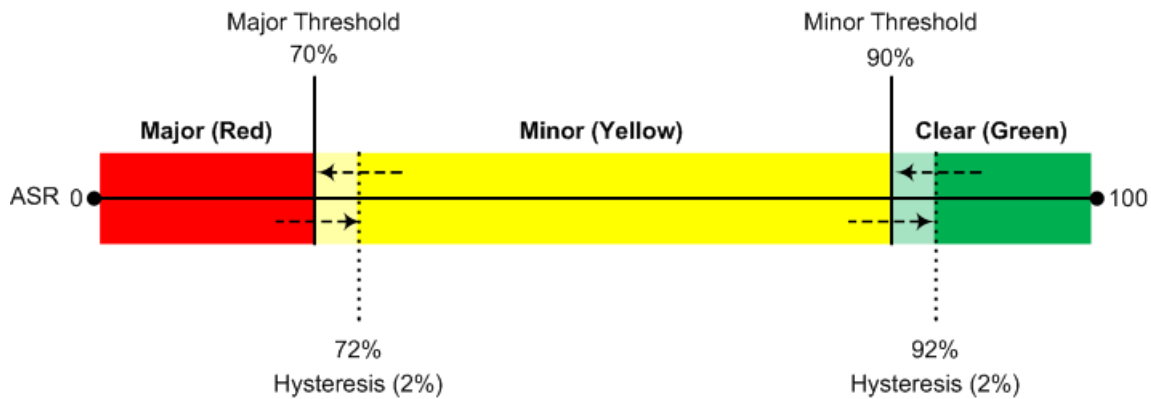


Table 46-1: Threshold Crossings based on Threshold and Hysteresis

Threshold Crossing	Calculation	Threshold based on Example
Green to Yellow (Minor alarm)	The change occurs if the measured metric crosses the configured Minor threshold only (i.e., hysteresis is not used).	90%
Green to Red (Major alarm)	The change occurs if the measured metric crosses the configured Major threshold only (i.e., hysteresis is not used).	70%
Yellow to Red (Major alarm)	The change occurs if the measured metric crosses the configured Major threshold only (i.e., hysteresis is not used).	70%
Red to Yellow (Minor alarm)	The change occurs if the measured metric crosses the configured Major threshold with hysteresis.	72% (i.e., 70 + 2)
Red to Green (alarm cleared)	The change occurs if the measured metric crosses the configured Minor threshold with hysteresis.	92 (i.e., 90 + 2)
Yellow to Green (alarm cleared)	The change occurs if the measured metric crosses the configured Minor threshold with hysteresis.	92 (i.e., 90 + 2)



Note:

- Forwarded calls are not considered in the calculation for ASR and NER.
- If you don't configure thresholds for a specific metric, the device still provides current performance monitoring values of the metric, but does not raise any threshold alarms for it.
- You can configure the device to perform certain actions, for example, reject calls to the IP Group for a user-defined duration, if a threshold is crossed. For more information, see "Configuring Quality of Service Rules" on page 300.

The following procedure describes how to configure Performance Profile rules through the Web interface. You can also configure it through ini file (PerformanceProfile) or CLI (configure system > performance-profile).

➤ **To configure a Performance Profile rule:**

1. Open the Performance Profile table (**Monitor** menu > **Monitor** tab > **Performance Monitoring** folder > **Performance Profile**).
2. Click **New**; the following dialog box appears:

Figure 46-4: Performance Profile Table - Dialog Box

MATCH		ACTION	
Index	2	Minor Threshold	0
Entity	Global	Major Threshold	0
IP Group	#1 [ITSP] View	Hysteresis	0
SRD	-- View	Minimum Samples	10
PM Type	ASR	Window Size [min]	5

3. Configure the rule according to the parameters described in the table below.
4. Click **Apply**.

Table 46-2: Performance Profile Table Parameter Descriptions

Parameter	Description
Index [PerformanceProfile_Index]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
Match	
Entity entity [PerformanceProfile_Entity]	Defines a configuration entity type to which you want to apply the rule. <ul style="list-style-type: none"> ▪ [0] Global = (Default) The device calculates call metrics for all calls. ▪ [1] SRD = Assigns an SRD. To specify the SRD, use the 'SRD' parameter (see below). ▪ [2] IP Group = Assigns an IP Group. To specify the IP Group, use the 'IP Group' parameter (see below).
IP Group ip-group-name [PerformanceProfile_IPGroupName]	Assigns an IP Group to the rule. Note: The parameter is applicable only if you configure the 'Entity' parameter to IP Group .
SRD srd-name [PerformanceProfile_SRDName]	Assigns an SRD to the rule. Note: The parameter is applicable only if you configure the 'Entity' parameter to SRD .
PM Type	Defines the type of performance monitoring metric for which you want to configure thresholds.

Parameter	Description
pmtype [PerformanceProfile_PMType]	<ul style="list-style-type: none"> ▪ [16] ASR (Default) ▪ [17] ACD ▪ [18] NER
Action	
Minor Threshold minor-threshold [PerformanceProfile_MinorThreshold]	<p>Defines the Minor threshold (in percentage) of the selected performance monitoring metric, which is the lower threshold located between the Yellow and Green states.</p> <p>To consider a threshold crossing:</p> <ul style="list-style-type: none"> ▪ Increase in severity (i.e., Green to Yellow): Only this value is used. ▪ Decrease in severity (Red to Green, or Yellow to Green): This value is used with the hysteresis, configured by the 'Hysteresis' parameter (see below). <p>The valid range is 0 to 100. The default is 0.</p>
Major Threshold major-threshold [PerformanceProfile_MajorThreshold]	<p>Defines the Major threshold (in percentage) of the selected performance monitoring metric, which is the upper threshold located between the Yellow and Red states.</p> <p>To consider a threshold crossing:</p> <ul style="list-style-type: none"> ▪ Increase in severity (i.e., Yellow to Red, or Green to Red): Only this value is used. ▪ Decrease in severity (Red to Yellow): This value is used with the hysteresis, configured by the 'Hysteresis' parameter (see below). <p>The valid range is 0 to 100. The default is 0.</p>
Hysteresis hysteresis [PerformanceProfile_Hysteresis]	<p>Defines the amount of fluctuation (hysteresis) from the configured threshold in order for the threshold to be considered as crossed. Hysteresis is used to avoid false reports being sent by the device. Hysteresis is used only when the severity level decreases (i.e., from Red to Yellow, Yellow to Green, or Red to Green).</p> <p>The valid value is 0 to 15 (in percentage). The default is 5.</p> <p>For example, if you configure the 'Major Threshold' parameter to 70% and the 'Hysteresis' parameter to 2%, the device considers a threshold crossing from Red to Yellow only if the ASR crosses 72% (i.e., 70% + 2%).</p>
Minimum Samples minimum-samples [PerformanceProfile_MinimumSample]	<p>Defines the minimum number of call sessions (sample) that is required for the device to calculate the performance monitoring metrics (per window size). If the number of call sessions is less than the configured value, no calculation is done.</p> <p>The default is 10 calls.</p> <p>Note: The calculation also depends on the configured sampling window size (see 'Window Size' parameter). For example, if the parameter is configured to 10 calls, but only 5 calls were processed during the configured sampling window, no calculation is done.</p>
Window Size window-size	<p>Defines the time interval (in minutes) during which the device calculates the performance monitoring metrics. For example, if the parameter is configured to five minutes, the calculation</p>

Parameter	Description
[PerformanceProfile_WindowSize]	<p>is done for the last five minutes. The default is 5 minutes.</p> <p>Note: The calculation depends on the configured minimum samples (see 'Minimum Samples' parameter). For example, if the parameter is configured to five minutes, but the number of calls during the interval is less than the configured minimum samples, no calculation is done.</p>

47 Viewing VoIP Status

This section describes how to view VoIP-related status.

47.1 Viewing SBC Registered Users

You can view SBC users that are registered with the device. For each user, the Address of Record (AOR) and the corresponding contacts are shown. An 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. A contact is a SIP URI that can be used to contact that specific instance of the user agent for subsequent requests.

➤ **To view registered SBC users:**

- Web: SBC Registered Users page (**Monitor** menu > **Monitor** tab > **VoIP Status** folder > **SBC Registered Users**).

Figure 47-1: Viewing Registered SBC Users

ADDRESS OF RECORD	CONTACT
-------------------	---------

Table 47-1: SBC Registered Users Table Description

Parameter	Description
Address of Record	AOR (e.g., 1000@10.8.5.71)
Contact	<p>Contacts corresponding to the AOR, for example:</p> <pre><sip:1000@10.8.5.71:5060>;expires=180; Active status:1</pre> <p>The contact's registration status is displayed:</p> <ul style="list-style-type: none"> ■ "Active status:1": The contact has been successfully registered and calls can be routed to it. ■ "Active status:0": The device has recently received a REGISTER request from the contact, but the contact has yet to be registered. The device removes the contact from the database if no response is received within 10 seconds from the proxy/registrar server.

- CLI:
 - SBC users:
show voip register db sbc list
 - SBC contacts of a specified AOR:
show voip register db sbc user <Address Of Record>

47.2 Viewing Call Routing Status

You can view information on the current call routing method used by the device. The information includes the IP address (or FQDN) of the Proxy server with which the device routes the call.

➤ **To view call routing status:**

- Open the Call Routing Status table (**Monitor** menu > **Monitor** tab > **VoIP Status** folder > **Call Routing Status**).

Figure 47-2: Viewing Call Routing Status

Call-Routing Method Proxy Set

Active Proxy Sets Status

ID	IP ADDRESS	STATE
0	Not Used (-)	--
1	10.10.9.200 (10.10.9.200)	OK
2	192.168.10.200 (192.168.10.200)	OK
3	10.10.9.200 (10.10.9.200)	OK
4	192.168.0.111 (192.168.0.111)	OK
5	192.168.0.111 (192.168.0.111)	OK
6	10.10.10.200 (10.10.10.200)	OK
7	Not Used (-)	--
8	Not Used (-)	--

Table 47-2: Call Routing Status Table Description

Parameter	Description
Call-Routing Method	Displays the method used to route the call: <ul style="list-style-type: none"> ▪ "Proxy Set": Call is routed using a Proxy server (i.e., Proxy Set). To configure Proxy Sets, see "Configuring Proxy Sets" on page 341. ▪ "Routing Table": Call is routed using a routing rule: <ul style="list-style-type: none"> ✓ SBC IP-to-IP Routing table (Configuring SBC IP-to-IP Routing Rules on page 470)
IP Address	Displays the call destination IP address: <ul style="list-style-type: none"> ▪ "Not Used": Proxy server is not used to route the call. ▪ IP address (or FQDN) of the Proxy server with which the device currently operates.
State	Displays the connectivity of the device with the Proxy server: <ul style="list-style-type: none"> ▪ "N/A": Proxy server isn't configured. ▪ "OK": Connectivity with the Proxy server exists. ▪ "Fail": No response from any of the configured Proxies.

47.3 Viewing Registration Status

You can view the registration status of the device's SIP Accounts.

➤ **To view registration status:**

- Open the Registration Status table (**Monitor** menu > **Monitor** tab > **VoIP Status**

folder > **Registration Status**).

Accounts Registration Status

INDEX	GROUP TYPE	GROUP NAME	STATUS
1	IP Group		NOT REGISTERED

Table 47-3: Registration Status Table Description

Parameter	Description
Accounts Registration Status	<p>Displays the status registration per Account, as configured in the Accounts table (see "Configuring Registration Accounts" on page 355).</p> <ul style="list-style-type: none"> ▪ Group Type: Served IP Group ▪ Group Name: Name of served IP Group, if applicable ▪ Status: "REGISTERED" or "NOT REGISTERED"

47.4 Viewing CDR Test Calls

You can view Call Detail Records (CDR) of SBC test calls, configured in "Configuring Test Call Endpoints" on page 713. These CDRs are stored on the device's non-volatile memory. When a new CDR is generated, the device adds it to the top of the table and all existing entries are shifted one row down in the table. The table displays the last 4,096 CDRs. If the table reaches maximum capacity of entries and a new CDR is added, the last CDR entry is removed from the table.



Note: If the device is reset, all CDRs are deleted from memory and from the table.

➤ **To view CDRs of test calls:**

- **Web:** Open the Test Call CDR History table (**Monitor** menu > **Monitor** tab > **VoIP Status** folder > **Test Call CDR History**).

Figure 47-3: Viewing CDRs of Test Calls

CALL END TIME	END POINT	CALLER	CALLEE	DIRECTION	REMOTE IP	DURATION	TERMINATION REASON	SESSION ID
<< << Page 1 of 0 >> >> 20								No records to view

■ **CLI:**

- All CDR history:
show voip calls history test
- CDR history for a specific SIP session ID:
show voip calls history test <session ID>

Table 47-4: Test Call CDR History Table

Field	Description
Call End Time	Displays the time at which the call ended. The time is displayed in the format, hh:mm:ss, where <i>hh</i> is the hour, <i>mm</i> the minutes and <i>ss</i> the

Field	Description
	seconds (e.g., 15:06:36).
End Point	Indicates that this is test call.
Caller	Displays the URI (user or user@host) of the test endpoint (caller).
Callee	Displays the destination (called) URI (user@host).
Direction	Displays the direction of the call: <ul style="list-style-type: none"> ▪ "Incoming" ▪ "Outgoing"
Remote IP	Displays the IP address of the call party. For an "Incoming" call, this is the source IP address; for an "Outgoing" call, this is the destination IP address.
Duration	Displays the duration of the call, displayed in the format hh:mm:ss, where <i>hh</i> is hours, <i>mm</i> minutes and <i>ss</i> seconds. For example, 00:01:20 denotes 1 minute and 20 seconds.
Termination Reason	Displays the reason for the call being released (ended). For example, "NORMAL_CALL_CLEAR" indicates a normal termination.
Session ID	Displays the SIP session ID of the call.

47.5 Viewing SBC CDR History

You can view historical Call Detail Records (CDR) of SBC calls in a table. History CDRs are stored on the device's memory. When a new CDR is generated, the device adds it to the top of the table and all existing entries are shifted one down in the table. The table displays the last 4,096 CDRs. If the table reaches maximum capacity of entries and a new CDR is added, the last CDR entry is removed from the table.



Note: If the device is reset, all CDRs are deleted from memory and from the table.

➤ **To view SBC CDR history:**

- **Web:** Open the SBC CDR History table (**Monitor** menu > **Monitor** tab > **VoIP Status** folder > **SBC CDR History**).

Figure 47-4: SBC CDR History Table

CALL END TIME	IP GROUP	CALLER	CALLEE	DIRECTION	REMOTE IP	DURATION	TERMINATION REASON	SESSION ID
<< Page 1 of 0 >>								No records to view

■ **CLI:**

- All CDR history:
show voip calls history sbc
- CDR history for a specific SIP session ID:
show voip calls history sbc <session ID>

Table 47-5: SBC CDR History Table

Field	Description
Call End Time	Displays the time at which the call ended. The time is displayed in the format, hh:mm:ss, where <i>hh</i> is the hour, <i>mm</i> the minutes and <i>ss</i> the seconds (e.g., 15:06:36).
IP Group	Displays the IP Group of the leg for which the CDR was generated.
Caller	Displays the phone number (source URI user@host) of the party who made the call.
Callee	Displays the phone number (destination URI user@host) of the party to whom the call was made.
Direction	Displays the direction of the call: <ul style="list-style-type: none"> ▪ "Incoming" ▪ "Outgoing"
Remote IP	Displays the IP address of the call party. For an "Incoming" call, this is the source IP address; for an "Outgoing" call, this is the destination IP address.
Duration	Displays the duration of the call, displayed in the format hh:mm:ss, where <i>hh</i> is hours, <i>mm</i> minutes and <i>ss</i> seconds. For example, 00:01:20 denotes 1 minute and 20 seconds.
Termination Reason	Displays the reason for the call being released (ended). For example, "NORMAL_CALL_CLEAR" indicates a normal termination.
Session ID	Displays the SIP session ID of the call.

This page is intentionally left blank.

48 Viewing Network Status

This section describes how to view network-related status.

48.1 Viewing Active IP Interfaces

You can view the device's active IP interfaces that are configured in the IP Interfaces table (see "Configuring IP Network Interfaces" on page 130).

➤ **To view active IP network interfaces:**

- Open the IP Interface Status page (**Monitor** menu > **Monitor** tab > **Network Status** folder > **IP Interface Status**).

INDEX	APPLICATION TYPE	IP ADDRESS	INTERFACE MODE	PREFIX LENGTH	DEFAULT GATEWAY	INTERFACE NAME	PRIMARY DNS SERVER IP ADDRESS	SECONDARY DNS SERVER IP ADDRESS	UNDERLYING DEVICE	ADDRESS STATE
0	O+M+C	10.15.7.96	IPv4 Manual	16	10.15.0.1	O+M+C	0.0.0.0	0.0.0.0	vlan 1	Permanent
NA	Internal	169.253.254.254	IPv4 Manual	16	0.0.0.0	Internalif 2	0.0.0.0	0.0.0.0	Internalif 2	Permanent

48.2 Viewing Ethernet Device Status

You can view the status of configured Ethernet Devices that have been successfully applied. To configure Ethernet Devices, see "Configuring Underlying Ethernet Devices" on page 128.

➤ **To view Ethernet Device status:**

- Open the Ethernet Device Status page (**Monitor** menu > **Monitor** tab > **Network Status** folder > **Ethernet Device Status**).

INDEX	VLAN ID	UNDERLYING INTERFACE	NAME
0	1	GROUP_1	vlan 1
1	2	GROUP_2	vlan 2

48.3 Viewing Ethernet Port Information

You can view status information of the device's Ethernet ports. To configure Ethernet ports, see "Configuring Underlying Ethernet Devices" on page 128



Note: If the device is operating in High-Availability mode, you can also view Ethernet port information of the redundant device, by opening the Redundant Ethernet Port Information page (Monitor menu > Monitor tab > Network Status folder > Redundant Ethernet Port Information).

➤ **To view Ethernet port information:**

- Open the Ethernet Port Information table, by doing one of the following:
 - Navigation tree: **Monitor** menu > **Monitor** tab > **Network Status** folder > **Ethernet Port Information**.
 - Monitor home page: Click an Ethernet port on the graphical display of the device (see "Viewing Device Status on Monitor Page" on page 637).

	PORT NAME	ACTIVE	SPEED	DUPLEX MODE	STATE	GROUP MEMBER
1	GE_1	Yes	1 Gbps	Full Duplex	Forwarding	GROUP_1
2	GE_2	Yes	1 Gbps	Full Duplex	Forwarding	GROUP_2

Table 48-1: Ethernet Port Information Table Description

Parameter	Description
Port Name	Displays the name of the port.
Active	Displays whether the port is active ("Yes") or not ("No").
Speed	Displays the speed 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"> ▪ "Forwarding": Active port (data is being transmitted and received) ▪ "Disabled": Redundancy port
Group Member	Displays the Ethernet Group to which the port belongs.

48.4 Viewing Static Routes Status

You can view the status of static IP routes, configured in the Static Routes table (see "Configuring Static IP Routing" on page 138) and routes through the Default Gateway.

The status of the static routes can be one of the following:

- "Active": Static route is used by the device.
- "Inactive": Static route is not used. 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".

➤ To view the status of static IP routing:

- Open the Static Route Status table (**Monitor** menu > **Monitor** tab > **Network Status** folder > **Static Route Status**).

Figure 48-1: Viewing Static Route Status

INDEX	DESTINATION IP ADDRESS	PREFIX LENGTH	GATEWAY IP ADDRESS	METRIC	DEVICE NAME	STATUS	DESCRIPTION
NA	10.15.0.0	16	0.0.0.0	0	vlan 1	Active	
NA	10.13.0.0	16	0.0.0.0	0	vlan 2	Active	
NA	0.0.0.0	0	10.15.0.1	1	vlan 1	Active	

49 Reporting Information to External Party

This section describes features for reporting various information to an external party.

49.1 Configuring 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 (Quality of Experience). RTCP XR information publishing is implemented in the device according to RFC 6035. The 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. 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 through SNMP.



Note:

- The RTCP XR feature is available only if the device is installed with a License Key that includes this feature. For installing a License Key, see "License Key" on page 597.
- If the RTCP XR feature is unavailable (not licensed or disabled), the R-factor VoIP metrics are not provided in CDRs (CDR fields, Local R Factor and Remote R Factor) generated by the device. Instead, these CDR fields are sent with the value 127, meaning that information is unavailable.

You can configure the device to send RTCP XR to a specific IP Group. In addition, you can configure the stage of the call at which you want the device to send RTCP XR:

- End of the call.
- Periodically, according to a user-defined interval between consecutive reports.

The device sends RTCP XR in SIP PUBLISH messages. The PUBLISH message contains the following RTCP XR related header values:

- From and To: Telephone extension number of the user.
- Request-URI: IP address and port of the SEM server.
- Event: "vq-rtcpxr"
- Content-Type: "application/vq-rtcpxr"

The type of RTCP XR report event (VQReportEvent) supported by the device is VQSessionReport (SessionReport). The device can include local and remote metrics in the RTCP XR. Local metrics are generated by the device while remote metrics are provided by the remote endpoint. The following table lists the supported voice metrics (parameters) published in the RTCP XR.

Table 49-1: RTCP XR Published VoIP Metrics

Metric	Parameter	Description
CallID	-	Call ID - call ID from the SIP dialog
LocalID	-	Local ID - identifies the reporting endpoint for the media session

Metric	Parameter	Description
RemoteID	-	Remote ID - identifies the remote endpoint of the media session
OrigID	-	Originating ID - Identifies the endpoint which originated the session
LocalAddr	-	Local Address - IP address, port, and SSRC of the endpoint/UA which is the receiving end of the stream being measured
RemoteAddr	-	Remote Address - IP address, port, and SSRC of the the source of the stream being measured
LocalGroup	-	Local Group ID - identification for the purposes of aggregation for the local endpoint
RemoteGroup	-	Remote Group ID - identification for the purposes of aggregation for the remote endpoint
LocalMAC	-	Media Access Control (MAC) address of the local SIP device
Timestamps	START	Start time of the media session
	STOP	End time of the media session
SessionDesc	PT	Payload Type - 'payload type' parameter in the RTP packets (i.e., the codec).
	PD	Payload Description - description of the codec
	SR	Sample Rate - rate at which the voice was sampled
	FD	Frame Duration (msec) - packetization rate
	FO	Frame Octets - number of octets in each frame per RTP packet
	FPP	Frames per Packets - number of frames per RTP packet
	PLC	Packet Loss Concealment - indicates whether a PLC algorithm was used for the session ("0" - unspecified; "1" - disabled; "2" - enhanced; "3" - standard)
	SSUP	Silence Suppression State - indicates whether silence suppression, also known as Voice Activity Detection (VAD) is enabled ("on" or "off")
JitterBuffer	JBA	Jitter Buffer Adaptive - indicates the jitter buffer in the endpoint ("0" - unknown; "1" - reserved; "2" - non-adaptive; "3" - adaptive)
	JBR	Jitter Buffer Rate
	JBN	Jitter Buffer Nominal
	JBM	Jitter Buffer Max
	JBX	Jitter Buffer Abs Max
PacketLoss	NLR	Network Packet Loss Rate
	JDR	Jitter Buffer Discard Rate
BurstGapLoss	BLD	Burst Loss Density
	BD	Burst Duration
	GLD	Gap Loss Density
	GD	Gap Duration
	GMIN	Minimum Gap Threshold

Metric	Parameter	Description
Delay	RTD	Round Trip Delay (msec)
	ESD	End System Delay (msec)
	OWD	One Way Delay (msec)
	IAJ	Inter-Arrival Jitter (msec)
	MAJ	Mean Absolute Jitter (msec)
Signal	SL	Signal Level (dB) - ratio of the signal level to a 0 dBm0 reference
	NL	Noise Level (dB) - ratio of the silent period background noise level to a 0 dBm0 reference
	RERL	Residual Echo Return Noise (dB) - ratio between the original signal and the echo level as measured after echo cancellation or suppression has been applied.
QualityEst	RLQ	Listening Quality R - listening quality expressed as an R factor (0-95 for narrowband calls and 0-120 for wideband calls)
	RLQEstAlg	RLQ Est. Algorithm - name (string) of the algorithm used to estimate RLQ
	RCQ	Conversational Quality R - cumulative measurement of voice quality from the start of the session to the reporting time (R is 0-95 for narrowband calls and 0-120 for wideband calls)
	RCQEstAlg	RCQ Est. Algorithm - name (string) of the algorithm used to estimate RCQ
	EXTRI	External R In - voice quality as measured by the local endpoint for incoming connection on "other" side (R is 0-95 for narrowband calls and 0-120 for wideband calls)
	ExtRIEstAlg	Ext. R In Est. Algorithm - name (string) of the algorithm used to estimate EXTRI
	EXTRO	External R Out - value is copied from RTCP XR received from the remote endpoint on the "other" side of this endpoint (R is 0-95 for narrowband calls and 0-120 for wideband calls)
	ExtROEstAlg	Ext. R Out Est. Algorithm - name (string) of the algorithm used to estimate EXTRO
	MOSLQ	MOS-LQ - estimated mean opinion score for listening voice quality on a scale from 1 to 5, in which 5 represents excellent and 1 represents unacceptable
	MOSLQEstAlg	MOS-LQ Est. Algorithm - name (string) of the algorithm used to estimate MOSLQ
	MOSCQ	MOS-CQ - estimated mean opinion score for conversation voice quality on a scale from 1 to 5, in which 5 represents excellent and 1 represents unacceptable
	MOSCQEstAlg	MOS-CQ Est. Algorithm - name (string) of the algorithm used to estimate MOSCQ
	QoEEstAlg	QoE Est. Algorithm - name (string) of the algorithm used to estimate all voice quality metrics

Metric	Parameter	Description
DialogID		Identification of the SIP dialog with which the media session is related

Below shows an example of a SIP PUBLISH message sent with RTCP XR and QoE information:



```
PUBLISH sip:172.17.116.201 SIP/2.0
Via: SIP/2.0/UDP 172.17.116.201:5060;branch=z9hG4bKac2055925925
Max-Forwards: 70
From: <sip:172.17.116.201>;tag=1c2055916574
To: <sip:172.17.116.201>
Call-ID: 20559160721612201520952@172.17.116.201
CSeq: 1 PUBLISH
Contact: <sip:172.17.116.201:5060>
Allow:
REGISTER,OPTIONS,INVITE,ACK,CANCEL,BYE,NOTIFY,PRACK,REFER,INFO,SUBSCRIBE,UPDATE
Event: vq-rtcpxr
Expires: 3600
User-Agent: device/v.7.20A.000.038
Content-Type: application/vq-rtcpxr
Content-Length: 1066
VQSessionReport
CallID=20328634741612201520943@172.17.116.201
LocalID: <sip:1000@172.17.116.201>
RemoteID: <sip:2000@172.17.116.202;user=phone>
OrigID: <sip:1000@172.17.116.201>
LocalAddr: IP=172.17.116.201 Port=6000 SSRC=0x54c62a13
RemoteAddr: IP=172.17.116.202 Port=6000 SSRC=0x243220dd
LocalGroup:
RemoteGroup:
LocalMAC: 00:90:8f:57:d9:71
LocalMetrics:
Timestamps: START=2015-12-16T20:09:45Z STOP=2015-12-16T20:09:52Z
SessionDesc: PT=8 PD=PCMA SR=8000 FD=20 PLC=3 SSUP=Off
JitterBuffer: JBA=3 JBR=0 JBN=7 JBM=10 JBX=300
PacketLoss: NLR=0.00 JDR=0.00
BurstGapLoss: BLD=0.00 BD=0 GLD=0.00 GD=6325 GMIN=16
Delay: RTD=0 ESD=11
Signal: SL=-34 NL=-67 RERL=17
QualityEst: RLQ=93 MOSLQ=4.1
MOSQ=4.10
RemoteMetrics:
Timestamps: START=2015-12-16T20:09:45Z STOP=2015-12-16T20:09:52Z
JitterBuffer: JBA=3 JBR=0 JBN=0 JBM=0 JBX=300
PacketLoss: NLR=0.00 JDR=0.00
BurstGapLoss: BLD=0.00 BD=0 GLD=0.00 GD=0 GMIN=16
Delay: RTD=65535 ESD=0
QualityEst:
DialogID: 20328634741612201520943@172.17.116.201;to-tag=1c1690611502;from-tag=1c2032864069
```

➤ **To configure RTCP XR:**

1. Open the RTP/RTCP Settings page (**Setup** menu > **Signaling & Media** tab > **Media** folder > **RTP/RTCP Settings**).


2. Under the RTCP-XR group, configure the following:
 - 'Enable RTCP XR' (*VQMonEnable*) - enables voice quality monitoring and RTCP XR.
 - '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*.
 - '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.
 - 'Minimum Gap Size' (*VQMonGMin*) - defines the voice quality monitoring minimum gap size (number of frames).

Figure 49-1: Enabling and Configuring RTCP XR

RTCP-XR	
Enable RTCP XR	Enable Fully  
RTCP XR Packet Interval	0
Disable RTCP XR Interval Randomization	Disable 
Burst Threshold	-1
Delay Threshold	-1
R-Value Delay Threshold	-1
Minimum Gap Size	16

3. Under the RTCP-XR Collection Server group, configure the following:
 - 'SBC RTCP XR Report Mode' (*SBCRtcpXrReportMode*) - enables the sending of RTCP XR reports of QoE metrics at the end of each call session (i.e., after a SIP BYE).

Figure 49-2: Configuring RTCP XR Collection Server

RTCP-XR COLLECTION SERVER	
SBC RTCP XR Report Mode	Disable 

4. Using the *PublicationIPGroupID* ini file parameter, define the IP Group to where you want to send the RTCP XR.
5. Click **Apply**, and then reset the device with a save-to-flash for your settings to take effect.

49.2 Generating Call Detail Records

Call Detail Records (CDR) contains vital statistic information on calls made from the device. The device can generate and report CDRs at various stages of the call - end of call,

or only at the start and end of call. In addition, CDRs can be generated for SIP signaling and/or media. The device can send CDRs to any of the following:

- Syslog server. The CDR Syslog message complies with RFC 3164 and is identified by Facility 17 (local1) and Severity 6 (Informational).
- RADIUS server. For CDR in RADIUS format, see "Configuring RADIUS Accounting" on page 685. To configure RADIUS servers for CDR reporting, see "Configuring RADIUS Servers" on page 219.



Note: To view SBC CDRs stored on the device's memory, see Viewing SBC CDR History on page 660.

49.2.1 CDR Field Description

This section describes the default CDR fields that are generated by the device.



Note: You can customize the default CDR fields if desired. For customizing SBC-related CDRs, see Customizing CDRs for SBC Calls on page 678.

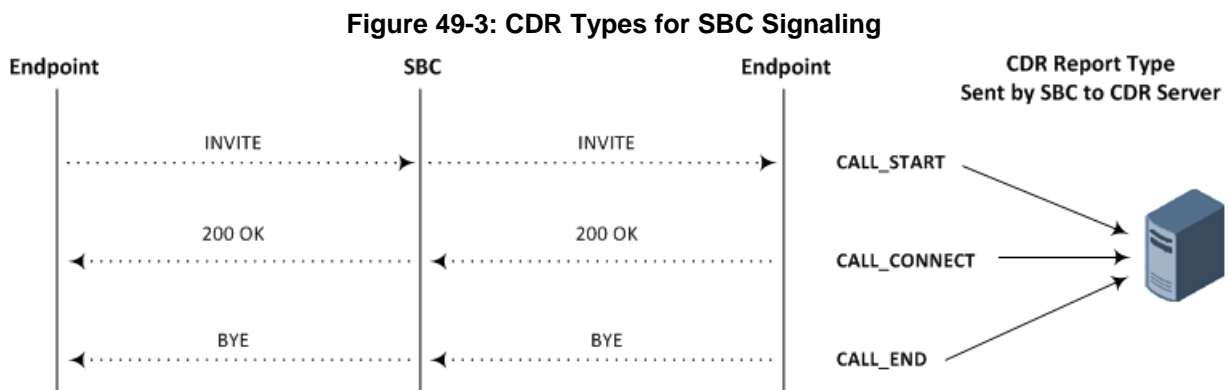
49.2.1.1 CDR Fields for SBC Signaling

The default CDR fields for SBC signaling are listed in the following table.

A typical SBC session consists of two SBC legs. Each leg generates its own signaling CDRs. Each leg generates three different CDR types (SBCReportType), which are sent to the CDR server at different stages of the SIP dialog:

- "CALL_START": CDR is sent upon an INVITE message.
- "CALL_CONNECT": CDR is sent upon a 200 OK response (i.e., call is established).
- "CALL_END": CDR is sent upon a BYE message (i.e., call ends)

The CDR types for SBC signaling and the SIP dialog stages are shown in the following figure:



CDRs belonging to the same SBC session (both legs) have the same Session ID (SessionId CDR field). CDRs belonging to the same SBC leg have the same Leg ID (LegId CDR field)

For billing applications, the CDR that is sent when the call ends (CALL_END) is usually sufficient. Billing may be based on the following:

- Leg ID (LegId CDR field)
- Source URI (SrcURI CDR field)
- Destination URI (DstURI CDR field)
- Call originator (Orig CDR field) - indicates the call direction (caller)
- Call duration (Durat CDR field) - call duration (elapsed time) from call connect
- Call time is based on SetupTime, ConnectTime and ReleaseTime CDR fields

Table 49-2: Default CDR Fields for SBC Signaling

CDR Field	Description	CDR Report Type (SBCReportType)	Format
SBCReportType	Report type: <ul style="list-style-type: none"> ■ "CALL_START": CDR sent upon an INVITE message. ■ "CALL_CONNECT": CDR sent upon a 200 OK response. ■ "CALL_END": CDR sent upon a BYE message. ■ "DIALOG_START" ■ "DIALOG_END" 	-	String
EPTyp	Endpoint type: "SBC"	All	String
SIPMethod	SIP message type	All	String (up to 10 characters)
SIPCallId	Unique ID of call	All	String (up to 50 characters)
SessionId	Unique Session ID	All	String (up to 10 characters)
LegId	Unique ID number of the call leg within a specific call session. A basic call consists of two legs (incoming leg and outgoing leg) and thus, two leg IDs are generated for the session, one for each leg. For each new call, the device assigns leg ID "1" to the first leg. The device then increments the leg ID for subsequent legs according to the leg sequence in the call session. For example, the device generates leg ID "1" for the incoming leg and leg ID "2" for the outgoing leg. If the call is transferred, the device generates leg ID "3" for the leg belonging to the call transfer target. Another example is a call forking session where the leg ID sequence may be as follows: incoming leg is "1", outgoing leg to user's office phone is "2" and outgoing leg to the user's mobile phone is "3". If the call is then transferred, the leg ID for the transfer leg is "4".	"CALL_START", "CALL_CONNECT" and "CALL_END"	String (decimal)
Orig	Call originator:	All	String

CDR Field	Description	CDR Report Type (SBCReportType)	Format
	<ul style="list-style-type: none"> ▪ "LCL": local ▪ "RMT": remote 		
SourceIp	Source IP address	All	String (up to 20 characters)
SourcePort	Source UDP port	All	String (up to 10 characters)
DestIp	Destination IP address	All	String (up to 20 characters)
DestPort	Destination UDP port	All	String (up to 10 characters)
TransportType	Transport type: <ul style="list-style-type: none"> ▪ "UDP" ▪ "TCP" ▪ "TLS" 	All	String
SrcURI	Source URI	All	String (up to 41 characters)
SrcURIBeforeMap	Source URI before manipulation	All	String (up to 41 characters)
DstURI	Destination URI	All	String (up to 41 characters)
DstURIBeforeMap	Destination URI before manipulation	All	String (up to 41 characters)
Durat	Call duration (in seconds)	"CALL_END"	String (up to 5 characters)
TrmSd	Termination side: <ul style="list-style-type: none"> ▪ "LCL": local ▪ "RMT": remote 	"CALL_END"	String
TrmReason	Termination reason	"CALL_END"	String (up to 40 characters)
TrmReasonCategory	Termination reason category: Calls with duration 0 (i.e., not connected): <ul style="list-style-type: none"> ▪ NO_ANSWER: <ul style="list-style-type: none"> ✓ "GWAPP_NORMAL_CALL_CLEAR" ✓ "GWAPP_NO_USER_RESPONDING" ✓ "GWAPP_NO_ANSWER_FROM_USER_ALERTED" ▪ BUSY: <ul style="list-style-type: none"> ✓ "GWAPP_USER_BUSY" ▪ NO_RESOURCES: <ul style="list-style-type: none"> ✓ "GWAPP_RESOURCE_UNAVAILABLE_UNSPECIFIED" ✓ "RELEASE_BECAUSE_NO_CONFERENCE" 	"CALL_END"	String (up to 17 characters)

CDR Field	Description	CDR Report Type (SBCReportType)	Format
	<p>RENCE_RESOURCES_LEFT"</p> <ul style="list-style-type: none"> ✓ "RESOURCE_BECAUSE_NO_TRANSCODING_RESOURCES_LEFT" ✓ "RELEASE_BECAUSE_GW_LOCKED" <ul style="list-style-type: none"> ▪ NO_MATCH: <ul style="list-style-type: none"> ✓ "RELEASE_BECAUSE_UNMATCHED_CAPABILITIES" ▪ FORWARDED: <ul style="list-style-type: none"> ✓ "RELEASE_BECAUSE_FORWARD" ▪ GENERAL_FAILED: Any other reason <p>Calls with duration:</p> <ul style="list-style-type: none"> ▪ NORMAL_CALL_CLEAR: <ul style="list-style-type: none"> ✓ "GWAPP_NORMAL_CALL_CLEAR" ✓ "ABNORMALLY_TERMINATED": Anything else <p>N/A - Reasons not belonging to above categories.</p>		
SetupTime	Call setup time	All	String (up to 35 characters)
ConnectTime	Call connect time	"CALL_CONNECT" and "CALL_END"	String (up to 35 characters)
ReleaseTime	Call release time	"CALL_END"	String (up to 35 characters)
RedirectReason	Redirect reason	"CALL_END"	String (up to 15 characters)
RedirectURINum	Redirection URI	"CALL_END"	String (up to 41 characters)
RedirectURINumBeforeMap	Redirect URI number before manipulation	"CALL_END"	String (up to 41 characters)
TxSigIPDiffServ	Signaling IP DiffServ	All	String (up to 15 characters)
IPGroup	IP Group ID and name	All	String (up to 40 characters)
SrdId	SRD ID and name	All	String (up to 29 characters)
SIPInterfaceId	SIP Interface ID	All	String (up to 15 characters)
ProxySetId	Proxy Set ID	All	String (up to 15 characters)
IpProfileId	IP Profile ID and name	All	String (up to 34 characters)

CDR Field	Description	CDR Report Type (SBCReportType)	Format
MediaRealmId	Media Realm ID and name	All	String (up to 55 characters)
DirectMedia	Direct media or traversing SBC: <ul style="list-style-type: none"> ▪ "yes" ▪ "no" 	All	String
SIPTrmReason	SIP call termination reason (BYE, CANCEL, or SIP error codes, e.g., 404)	"CALL_END"	String (up to 12 characters)
SipTermDesc	Description of SIP termination reason: <ul style="list-style-type: none"> ▪ SIP Reason header, if exists, for example: SIP ;cause=200 ;text="Call completed elsewhere". ▪ 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". ▪ If no reason text exists in the SIP response code, the description is 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. 	"CALL_END"	String (up to 26 characters)
Caller	Name of caller	All	String (up to 36 characters)
Callee	Name of called party	All	String (up to 36 characters)

Below shows an example of an SBC signaling CDR sent at the end of a call (call was terminated normally):

```
[S=40] |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 |SIPTermDesc |Caller |Callee
[S=41] |CALL_END |SBC |20767593291410201017029@10.33.45.80
|1871197419|LCL |10.33.45.80 |5060 |10.33.45.72 |5060 |UDP
|9001@10.8.8.10 |9001@10.8.8.10 |6001@10.33.45.80
|6001@10.33.45.80 |15 |LCL |GWAPP_NORMAL_CALL_CLEAR
|NORMAL_CALL_CLEAR |17:00:29.954 UTC Thu Oct 14 2014
|17:00:49.052 UTC Thu Oct 14 2014 |17:01:04.953 UTC Thu Oct 14
2014 |-1 | | |40 |1 |0 (SRD_GW) |1 |1 |1 ( ) |0 (MR_1) |no |BYE
|Q.850 ;cause=16 ;text="loc |user 9928019 |
```

49.2.1.2 CDR Fields for SBC Media

The default CDR fields for SBC media are listed in the following table. 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.

There are three different CDR types (SBCReportType), which are sent to the CDR server at different stages of the SIP dialog session:

- "MEDIA_START": CDR is sent upon an INVITE message.
- "UPDATE": CDR is sent upon a re-INVITE message (e.g., the established call is placed on hold by one of the call parties).
- "END": CDR is sent upon a BYE message (i.e., call ends)

The CDR types for SBC media and the SIP dialog stages are shown in the following figure:

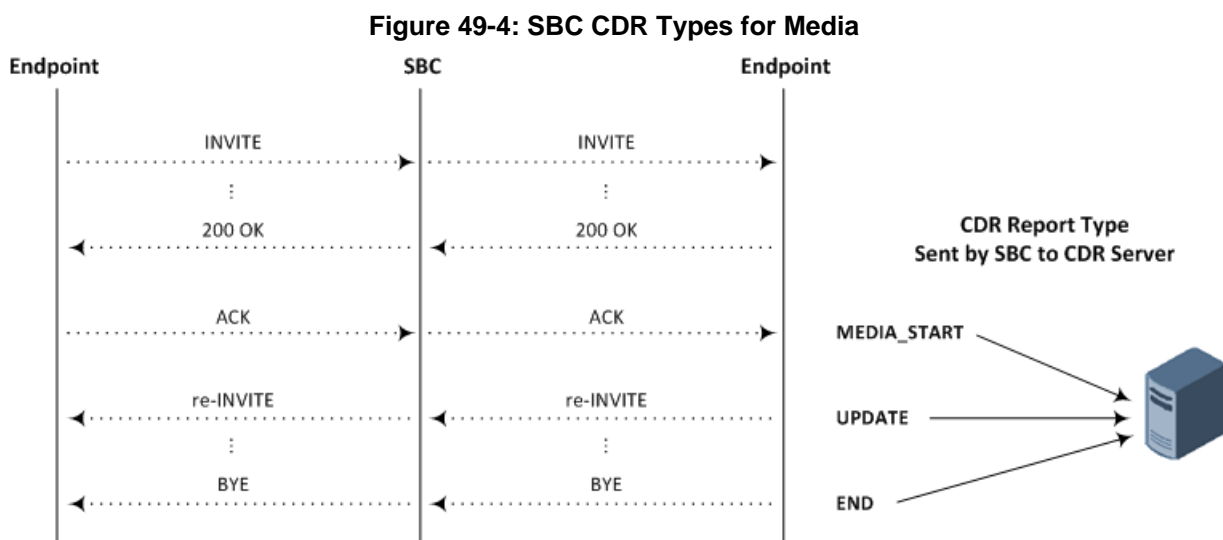


Table 49-3: Default CDR Fields for SBC Media

CDR Field	Range	Description
MediaReportType		Report type: <ul style="list-style-type: none"> ■ "MEDIA_START": CDR is sent upon 200 OK response or early media ■ "UPDATE": CDR is sent upon a re-INVITE message ■ "END": CDR sent is upon a BYE message
SIPCallId		Unique call ID
LegId		Unique ID number of the call leg within a specific call session. The field is included in all Report Types (MediaReportType). A basic call consists of two legs (incoming leg and outgoing leg) and thus, two leg IDs are generated for the session, one for each leg. For each new call, the device assigns leg ID "1" to the first leg. The device then

CDR Field	Range	Description
		increments the leg ID for subsequent legs according to the leg sequence in the call session. For example, the device generates leg ID "1" for the incoming leg and leg ID "2" for the outgoing leg. If the call is transferred, the device generates leg ID "3" for the leg belonging to the call transfer target. Another example is a call forking session where the leg ID sequence may be as follows: incoming leg is "1", outgoing leg to user's office phone is "2" and outgoing leg to the user's mobile phone is "3". If the call is then transferred, the leg ID for the transfer leg is "4".
Cid		Channel CID
MediaType		Media type (audio, video, or text)
Coder		Coder name
PacketInterval	10 to 200 ms	Coder packet interval
LocalRtpIp		Local RTP IP address
LocalRtpPort	0 to 0xFFFF	Local RTP port
RemoteRtpIp		Remote RTP IP address
RemoteRtpPort	0 to 0xFFFF	Remote RTP port
InPackets	0 to 0xFFFFFFFF	Number of packets received by the device (local)
OutPackets	0 to 0xFFFFFFFF	Number of packets sent by the device (local)
LocalPackLoss	0 to 0xFFFFFFFF	Number of packet loss of the entire stream (local)
RemotePackLoss	0 to 0xFFFF (-1 if information is unavailable)	Remote packet loss
RTPdelay	0 to 10000 ms (-1 if information is unavailable)	Average RTP delay of the entire stream
RTPjitter	0 to 40000 samples (-1 if unavailable)	RTP jitter
TxRTPSSRC	0 to 0xFFFFFFFF	Tx RTP SSRC
RxRTPSSRC	0 to 0xFFFFFFFF	Local RTP SSRC
LocalRFactor	0 to 120 (127 if information is unavailable)	Local conversation quality Note: If the RTCP XR feature is unavailable (not licensed or disabled), this R-factor VoIP metric is not provided. Instead, the device sends the CDR field with the value 127, meaning that information is unavailable.
RemoteRFactor	0 to 120 (127 if information is	Remote conversation quality

CDR Field	Range	Description
	unavailable)	Note: If the RTCP XR feature is unavailable (not licensed or disabled), this R-factor VoIP metric is not provided. Instead, the device sends the CDR field with the value 127, meaning that information is unavailable.
LocalMosCQ	10 to 46 (127 if information is unavailable)	Local MOS for conversation
RemoteMosCQ	10 to 46 (127 if information is unavailable)	Remote MOS for conversation
TxRTPIPDiffServ	0 to 63	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	0 to 0xFFFF	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.
LatchedT38lp		Latching of a new T.38 stream - new IP address
LatchedT38Port	0 to 0xFFFF	Latching of a new T.38 stream - new port

49.2.1.3 CDR Fields for SBC Local Storage

The CDR fields for SBC calls that are stored locally (history) on the device are listed in the table below. For storing CDRs locally, see "Storing CDRs on the Device" on page 683.

Table 49-4: Default CDR Fields for Locally Stored (History) CDRs

CDR Field	Title
Report Type	SBCReportType
Endpoint Type	EPTyp
Call Id	SIPCallId
Session ID	SessionId
Leg ID	LegId
Call Orig	Orig
Source IP	SourceIp
Source Port	SourcePort
Destination IP	DestIp
Destination Port	DestPort
Transport Type	TransportType

CDR Field	Title
Source URI	SrcURI
Source URI Before Manipulation	SrcURIBeforeMap
Destination URI	DstURI
Destination URI Before Manipulation	DstURIBeforeMap
Call Duration	Durat
Termination Side	TrmSd
Termination Reason	TrmReason
Termination Reason Category	TrmReasonCategory
Setup Time	SetupTime
Connect Time	ConnectTime
Release Time	ReleaseTime
Redirect Reason	RedirectReason
Redirect URI	RedirectURINum
Redirect URI Before Manipulation	RedirectURINumBeforeMap
Signaling IP DiffServ	TxSigIPDiffServ
IP Group Name	IPGroup
SRD Name	SrdId
SIP Interface Name	SIPInterfaceld
Proxy Set Name	ProxySetId
IP Profile Name	IpProfileId
Media Realm Name	MediaRealmId
Direct Media	DirectMedia
SIP Termination Reason	SIPTrmReason
SIP Termination Description	SIPTermDesc
Caller Display ID	Caller
Callee Display ID	Callee

49.2.2 Customizing CDRs for SBC Calls

The SBC CDR Format table lets you customize SBC-related CDRs that are generated by the device for the following:

- CDRs (media and SIP signaling) sent in Syslog messages. For CDRs sent in Syslog messages, you can customize the name of the CDR field. The table lets you configure up to 128 Syslog CDR customization rules.
- CDRs related to RADIUS accounting and sent in RADIUS accounting request messages. For RADIUS accounting CDRs, you can customize the RADIUS Attribute's prefix name and RADIUS Attribute's ID, for standard RADIUS Attributes and vendor-specific RADIUS Attributes (VSA). For example, instead of the default VSA name, "h323-connect-time" with RADIUS Attribute ID 28, you can change the name to "Call-

Connect-Time" with ID 29. The table lets you configure up to 40 RADIUS-accounting CDR customization rules. For more information on RADIUS accounting, see "Configuring RADIUS Accounting" on page 685.

- CDRs stored locally on the device. For local storage of CDRs, you can customize the name of the CDR field. The table lets you configure up to 64 locally-stored CDR customization rules. For more information on storing CDRs on the device, see Storing CDRs on the Device on page 683.

If you do not configure a CDR customization rule for a specific CDR, the device generates the CDR in a predefined default CDR format (see "CDR Field Description" on page 670).



Note:

- The following standard RADIUS Attributes cannot be customized: 1 through 6, 18 through 20, 22, 23, 27 through 29, 32, 34 through 39, 41, 44, 52, 53, 55, 60 through 85, 88, 90, and 91.
- If the RTCP XR feature is unavailable (not licensed or disabled), the R-factor VoIP metrics are not provided in CDRs (CDR fields, Local R Factor and Remote R Factor) generated by the device. Instead, these CDR fields are sent with the value 127, meaning that information is unavailable.

The following procedure describes how to customize SBC-related CDRs through the Web interface. You can also configure it through ini file (SBCCDRFormat) or CLI (configure troubleshoot > cdr > cdr-format sbc-cdr-format).

➤ **To customize SBC-related CDRs:**

1. Open the SBC CDR Format table (**Troubleshoot** menu > **Troubleshoot** tab > **Call Detail Record** folder > **SBC CDR Format**).
2. Click **New**; the following dialog box appears:

Figure 49-5: SBC CDR Format Table - Add Dialog Box

3. Configure the CDR according to the parameters described in the table below.
4. Click **Apply**.

Examples of configured CDR customization rules are shown below:

Figure 49-6: Examples of SBC CDR Customization Rules

INDEX ↕	CDR TYPE	FIELD TYPE	TITLE	RADIUS ATTRIBUTE TYPE	RADIUS ATTRIBUTE ID
0	Syslog SBC	Source IP	"Source IP Address"	Standard	0
1	RADIUS SBC	Release Time	disconnect-time=	Vendor Specific	29
2	Local Storage SBC	Call Duration	Lenght of Call	Standard	0

Table 49-5: SBC CDR Format Table Parameter Descriptions

Parameter	Description
Index [SBCCDRFormat_Index]	<p>Defines an index number for the new table row.</p> <p>Note: Each row must be configured with a unique index.</p>
CDR Type cdr-type [SBCCDRFormat_CDRTYPE]	<p>Defines the application type for which you want to customize CDRs.</p> <ul style="list-style-type: none"> ▪ [1] Syslog SBC = (Default) Customizes CDR fields for SIP signaling-related CDRs sent in Syslog messages. ▪ [3] Syslog Media = Customizes CDR fields for media-related CDRs sent in Syslog messages. ▪ [5] Local Storage SBC = Customizes CDR fields that are stored locally on the device. Only signaling-related CDRs are stored locally on the device. ▪ [7] RADIUS SBC = Customizes CDR fields (i.e., RADIUS Attributes) for CDRs sent in RADIUS accounting request messages.
Field Type col-type [SBCCDRFormat_FieldType]	<p>Defines the CDR field (column) that you want to customize. The applicable CDR field depends on the settings of the 'CDR Type' parameter:</p> <ul style="list-style-type: none"> ▪ For all types: [300] CDR Type (default); [301] Call ID; [302] Session ID; [303] Report Type; [304] Media Type; [305] Accounting Status Type; [306] H323 ID; [307] RADIUS Call ID; [308] Blank; [309] Global Session ID; [310] Leg ID. ▪ Syslog SBC, Local Storage SBC, and RADIUS SBC: [400] Endpoint Type; [401] Call Orig; [402] Source IP; [403] Destination IP; [404] Remote IP; [405] Source Port; [406] Dest Port; [407] Remote Port; [408] Call Duration; [409] Termination Side; [410] Termination Reason; [411] Setup Time; [412] Connect Time; [413] Release Time; [414] Redirect Reason; [415] Was Call Started; [416] IP Group ID; [417] IP Group Name; [418] SRD ID; [419] SRD Name; [420] SIP Interface ID; [421] Transport Type; [422] Signaling IP DiffServ; [423] Termination Reason Category; [424] Proxy Set ID; [425] IP Profile ID; [426] IP Profile Name; [427] Media Realm ID; [428] Media Realm Name; [429] SIP Termination Reason; [430] SIP Termination Description; [431] Caller Display ID; [432] Callee Display ID; [433] SIP Interface Name; [434] Call Orig RADIUS; [435] Termination Side RADIUS; [436] Termination Side Yes No; [437] Termination Reason Value; [438] Proxy Set Name; [439] Trigger. ▪ Syslog Media and RADIUS SBC: [600] Channel ID; [601] Coder Type; [602] Packet Interval; [603] Payload Type; [604] Local Input Packets; [605] Local Output Packets; [606] Local Input Octets; [607] Local Output Octets; [608] Local Packet Loss; [609] Local Round Trip Delay; [610] Local Jitter; [611] Local SSRC Sender; [612] Remote Input Packets; [613] Remote Output Packets; [614] Remote Input Octets; [615] Remote Output

Parameter	Description
	<p>Octets; [616] Remote Packet Loss; [617] Remote Round Trip Delay; [618] Remote Jitter; [619] Remote SSRC Sender; [620] Local RTP IP; [621] Local RTP Port; [622] Remote RTP IP; [623] Remote RTP Port; [624] RTP IP DiffServ; [625] Local R Factor; [626] Remote R Factor; [627] Local MOS CQ; [628] Remote MOS CQ; [629] AMD Decision; [630] AMD Decision Probability; [631] Latched RTP IP; [632] Latched RTP Port; [633] Latched T38 IP; [634] Latched T38 Port.</p> <ul style="list-style-type: none"> ▪ Syslog SBC, Local Storage SBC, and RADIUS SBC: [800] Source URI; [801] Destination URI; [802] Source URI Before Manipulation; [803] Destination URI Before Manipulation; [804] Redirect URI; [805] Redirect URI Before Manipulation; [806] SIP Method; [807] Direct Media; [808] Source Username; [809] Destination Username; [810] Source Username Before Manipulation; [811] Destination Username Before Manipulation; [812] Source Host; [813] Destination Host; [814] Source Host Before Manipulation; [815] Destination Host Before Manipulation; [816] Source Dial Plan Tags; [817]; Destination Dial Plan Tags.
<p>Title title [SBCCDRFormat_Title]</p>	<p>Defines a new name for the CDR field (for Syslog or local storage) or for the RADIUS Attribute prefix name (for RADIUS accounting) that you selected in the 'Column Type' parameter.</p> <p>You can configure the name to be enclosed by apostrophes (single or double). For example, if you want the CDR field name to appear as 'Phone Duration', you must configure the parameter to 'Phone Duration'. You can also configure the CDR field name with an equals (=) sign, for example "call-connect-time=".</p> <p>Note:</p> <ul style="list-style-type: none"> ▪ For VSA's that do not require a prefix name, leave the parameter undefined. ▪ The parameter's value is case-sensitive. For example, if you want the CDR field name to be Phone-Duration, you must configure the parameter to "Phone-Duration" (i.e., upper case "P" and "D").
<p>RADIUS Attribute Type radius-type [SBCCDRFormat_RadiusType]</p>	<p>Defines whether the RADIUS Attribute of the CDR field is a standard or vendor-specific attribute.</p> <ul style="list-style-type: none"> ▪ [0] Standard = (Default) For standard RADIUS Attributes. ▪ [1] Vendor Specific = For vendor-specific RADIUS Attributes (VSA). <p>Note: The parameter is applicable only for RADIUS accounting (i.e., 'CDR Type' parameter configured to RADIUS SBC).</p>
<p>RADIUS Attribute ID radius-id [SBCCDRFormat_RadiusID]</p>	<p>Defines an ID for the RADIUS Attribute. For VSAs, this represents the VSA ID; for standard Attributes, this represents the Attribute ID (first byte of the Attribute).</p> <p>The valid value is 0 to 255 (one byte). The default is 0.</p> <p>Note:</p> <ul style="list-style-type: none"> ▪ The parameter is applicable only for RADIUS accounting (i.e., 'CDR Type' parameter configured to RADIUS SBC). ▪ For VSA's (i.e., 'RADIUS Attribute Type' parameter configured to Vendor Specific), the parameter must be configured to any value other than 0. ▪ For standard RADIUS Attributes (i.e., 'RADIUS Attribute Type'

Parameter	Description
	<p>parameter configured to Standard), the value must be a "known" RADIUS ID (per RFC for RADIUS). However, if you configure the ID to 0 (default) for any of the RADIUS Attributes (configured in the 'Column Type' parameter) listed below and then apply your rule (Click Apply), the device automatically replaces the value with the RADIUS Attribute's ID according to the RFC:</p> <ul style="list-style-type: none"> ✓ Destination Username: 30 ✓ Source Username: 31 ✓ Accounting Status Type: 40 ✓ Local Input Octets: 42 ✓ Local Output Octets: 43 ✓ Call Duration: 46 ✓ Local Input Packets: 47 ✓ Local Output Packets: 48 <p>If you configure the value to 0 and the RADIUS Attribute is not any of the ones listed above, the configuration is invalid.</p>

49.2.3 Configuring CDR Reporting

To enable and configure CDR reporting, perform the following procedure. For detailed descriptions of the parameters, see "Syslog, CDR and Debug Parameters" on page 758.

➤ **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 "Enabling Syslog" on page 703.
2. Open the Call Detail Record Settings page (**Troubleshoot** menu > **Troubleshoot** tab > **Call Detail Record** folder > **Call Detail Record Settings**).

Figure 49-7: CDR Parameters in Advanced Parameters Page

CDR REPORTS

CDR Server IP Address	<input style="width: 90%;" type="text" value="0.0.0.0"/>
CDR Report Level	<input style="width: 90%;" type="text" value="None"/> ▼
Media CDR Report Level	<input style="width: 90%;" type="text" value="None"/> ▼
CDR Syslog Sequence Number	<input style="width: 90%;" type="text" value="Enable"/> ▼

3. Configure the following parameters:
 - In the 'CDR Server IP Address' field (CDRSyslogServerIP), enter the IP address of the server to where you want the CDRs sent.
 - From the 'CDR Report Level' drop-down list (CDRReportLevel), select the stage of the call at which you want CDRs to be generated and sent.
 - (Applicable only to SBC) From the 'Media CDR Report Level' drop-down list (MediaCDRReportLevel), select the stage of the call at which you want CDRs to be generated and sent.

- From the 'CDR Syslog Sequence Number' drop-down list (CDRSyslogSeqNum), enable or disable the inclusion of the sequence number (S=) in CDR Syslog messages.
4. Click **Apply**.

**Note:**

- If you do not configure an IP address for a CDR server, the device sends CDRs to the Syslog server, as configured in 'Enabling Syslog' on page 703.
- The device sends CDRs only for dialog-initiating INVITE messages (call start), 200 OK responses (call connect) and BYE messages (call end). For SBC calls only: If you want to enable the generation of CDRs for non-call SIP dialogs (such as SUBSCRIBE, OPTIONS, and REGISTER), use the EnableNonCallCdr parameter.

49.2.4 Storing CDRs on the Device

The CDRs generated by the device can also be stored locally on the device (hard disk of server platform).

You can specify the calls (configuration entities) for which you wish to create CDRs and store locally. This is done using Logging Filter rules in the Logging Filters table. For example, you can configure a rule to create CDRs for traffic belonging only to IP Group 2 and store the CDRs locally.

The locally stored CDRs are saved in a comma-separated values file (*.csv), where each CDR is shown on a dedicated row. An example of a CSV file with two CDRs are shown below:

- CSV file viewed in Excel:

	A	B	C	D	E	F	G	H
1	3b463e:215:1	CALL_END	4	14:34:40.000 UTC Wed Dec 16 2015	14:34:35.000 UTC Wed Dec 16 2015	14:34:33.000 UTC Wed Dec 16 2015	RMT	GWAPP_NORMAL
2	3b463e:215:1	CALL_END	4	14:34:40.000 UTC Wed Dec 16 2015	14:34:35.000 UTC Wed Dec 16 2015	14:34:33.000 UTC Wed Dec 16 2015	LCL	GWAPP_NORMAL
3								

- CSV file viewed in a text editor (Notepad):

Figure 49-8: CSV File of CDRs in Text Editor (Notepad)

1	3b463e:215:1,CALL_END,4,14:34:40.000 UTC Wed Dec 16 2015,14:34:35.000 UTC Wed Dec 16 2015,14:34:33.000 UTC Wed Dec 16 2015,RMT,GWAPP_NORMAL
2	3b463e:215:1,CALL_END,4,14:34:40.000 UTC Wed Dec 16 2015,14:34:35.000 UTC Wed Dec 16 2015,14:34:33.000 UTC Wed Dec 16 2015,LCL,GWAPP_NORMAL
3	

To view the CDR column headers corresponding to the CDR data in the CSV file, run the following CLI command:

- SBC CDRs:

```
(config-system)# cdr
(cdr)# cdr-format show-title local-storage-sbc
session id,report type,call duration, call end time, call
connect time,call start time, call originator, termination
reason, call id, srce uri, dest uri
```

You can do the following with locally saved CDR files (*.csv), through the CLI (root menu):

- View stored CDR files:

- View all stored CDR files:


```
# show storage-history
```
- View all stored, unused CDR files:

```
# show storage-history unused
```

- Delete stored CDR files:

- Delete all stored files:

```
# clear storage-history cdr-storage-history all
```

- Delete all stored, unused CDR files:

```
# clear storage-history cdr-storage-history unused
```

- Save stored CDR files to an external destination:

```
# copy storage-history cdr-storage-history <filename> to
<protocol://destination>
```

Where:

- *filename*: name you want to assign the file. Any file extension name can be used, but as the file content is in CSV format, it is recommended to use the .csv file extension.
- *protocol*: protocol over which the file is sent (tftp, http, or https).

For example:

```
copy storage-history cdr-storage-history my_cdrs.csv to
tftp://company.com/cdrs
```

The following procedure describes how to configure local CDR storage through the Web interface.

- **To configure local CDR storage:**

1. Open the Call Detail Record Settings page (**Troubleshoot** menu > **Troubleshoot** tab > **Call Detail Record** folder > **Call Detail Record Settings**).
2. Configure the following parameters:
 - 'Local Storage Max File Size' (CDRLocalMaxFileSize): Enter the maximum size (in kilobytes) of the CDR file. Once the file size is reached, the device creates a new file for subsequent CDRs, and so on.
 - 'Local Storage Max Number of Files' (CDRLocalMaxNomOfFiles): Enter the maximum number of CDR files. Once the maximum is reached, a subsequent CDR file replaces the oldest created file.
 - 'Local Storage File Creation Interval' (CDRLocalInterval): Enter the time (in minutes) for how often the device creates a new CDR file. For example, if configured to 60, it creates a new file every hour even if the maximum file size has not yet been reached.
 - For a detailed description of each parameter, see "Syslog, CDR and Debug Parameters" on page 758.

CDR LOCAL STORAGE	
Local Storage Max File Size [KB]	<input type="text" value="1024"/>
Local Storage Max Number of Files	<input type="text" value="5"/>
Local Storage File Creation Interval [minutes]	<input type="text" value="60"/>

3. Open the Logging Filters table (see "Configuring Log Filter Rules" on page 693), and then configure a log filtering rule with the following settings:
 - 'Filter Type' and 'Value': (as desired)
 - 'Log Destination': **Local Storage**
 - 'Log Type': **CDR Only**
 - 'Mode': **Enable**

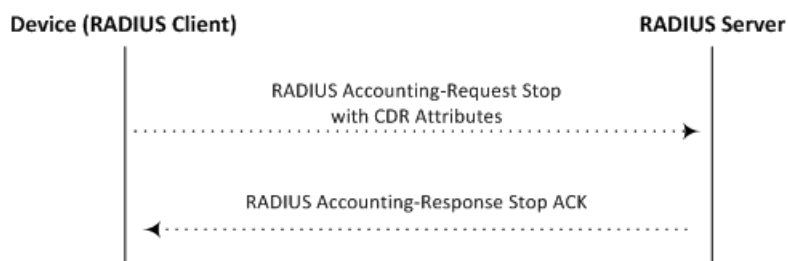
**Note:**

- If you have enabled the CDR storage feature and you later decide to change the maximum number of files (CDRLocalMaxNomOfFiles) to a lower value (e.g., from 50 to 10), the device stores the remaining files (e.g., 40) in its memory (i.e., unused files).
- When the device operates in High-Availability mode, stored CDRs are deleted upon device switchover.
- For customizing CDR fields for SBC calls, see Customizing CDRs for SBC Calls on page 678.

49.3 Configuring RADIUS Accounting

The device can send accounting data of SIP calls as call detail records (CDR) to a RADIUS Accounting server. CDR-based accounting messages can be sent upon call release, call connection and release, or call setup and release. This section lists the CDR attributes for RADIUS accounting.

The following figure shows the interface between the device and the RADIUS server, based on the RADIUS Accounting protocol. For each CDR that the device sends to the RADIUS server, it sends an Accounting-Request Stop with all the CDR attributes. When the RADIUS server successfully receives all the CDR attributes, it responds with an Accounting-Response Stop ACK message to the device. If the device does not receive the Accounting-Response ACK message, it can resend the Accounting-Request Stop with all CDR attributes again, up to a user-defined number of re-tries (see "Configuring RADIUS Packet Retransmission" on page 221).



There are two types of data that can be sent to the RADIUS server. The first type is the accounting-related attributes and the second type is the vendor specific attributes (VSA):

- **Standard RADIUS attributes (per RFC):** A typical standard RADIUS attribute is shown below. The RADIUS attribute ID depends on the attribute.

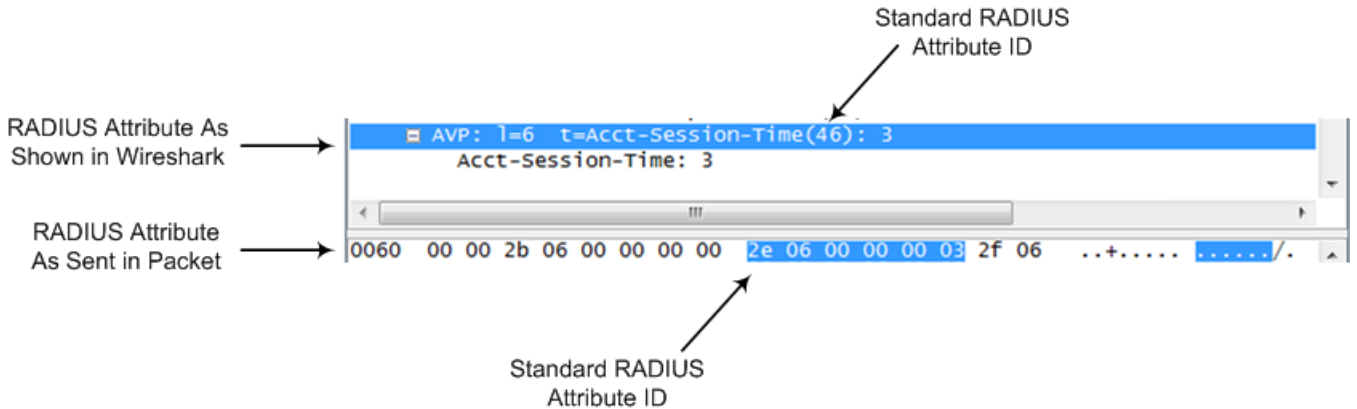
Figure 49-9: Typical Standard RADIUS Attribute

```

2e 06 00 00 00 03 --- Data
| |
| Length (including header)
RADIUS ID
  
```

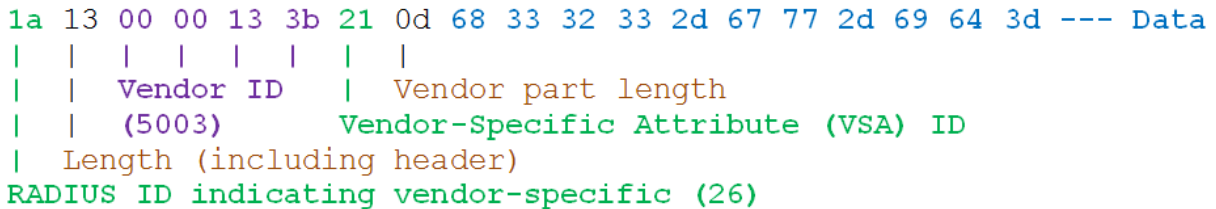
The following figure shows a standard RADIUS attribute collected by Wireshark. The bottom pane shows the RADIUS attribute information as sent in the packet; the upper pane is Wireshark's interpretation of the RADIUS information in a more readable format. The example shows the attribute in numeric format (32-bit number in 4 bytes).

Figure 49-10: Example of Standard RADIUS Attribute Collected by Wireshark



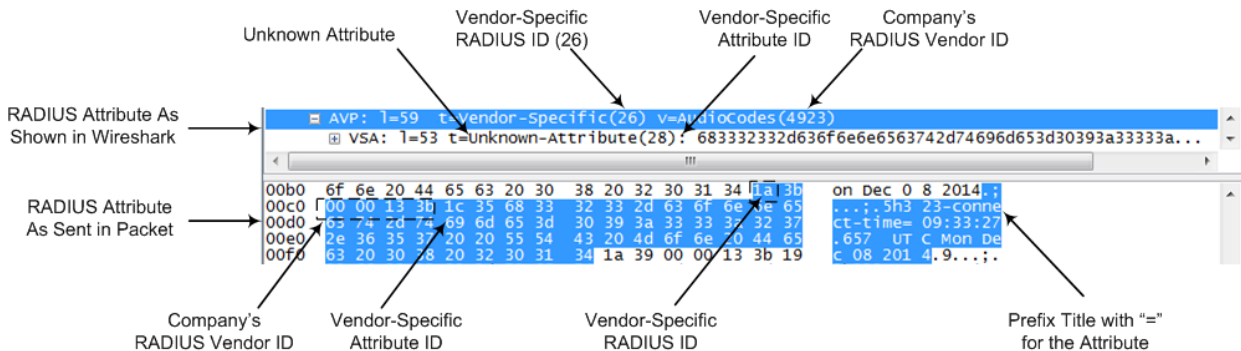
- Vendor-specific RADIUS attributes:** RADIUS attributes that are specific to the device (company) are referred to as Vendor-specific attributes (VSA). The CDR of VSAs are sent with a general RADIUS ID of 26 to indicate that they are vendor-specific (non-standard). In addition, the company's registered vendor ID (as registered with the Internet Assigned Numbers Authority or IANA) is also included in the packet. The device's default vendor ID is 5003, which can be changed (see "Configuring the RADIUS Vendor ID" on page 222). The VSA ID is also included in the packet.

Figure 49-11: Example of a Vendor-Specific Attribute



The following figure shows a vendor-specific RADIUS attribute collected by Wireshark. The bottom pane shows the RADIUS attribute information as sent in the packet; the upper pane is Wireshark's interpretation of the RADIUS information in a more readable format. The example shows the attribute in string-of-characters format.

Figure 49-12: Example of Vendor-Specific RADIUS Attribute Collected by Wireshark



Note: You can customize the prefix title of the RADIUS attribute name and the ID. For more information, see Customizing CDRs for SBC Calls on page 678.

To configure the address of the RADIUS Accounting server, see "Configuring RADIUS Servers" on page 219. For all RADIUS-related configuration, see "RADIUS-based Services" on page 218.

➤ **To configure RADIUS accounting:**

1. Open the Call Detail Record Settings page (**Troubleshoot** menu > **Troubleshoot** tab > **Call Detail Record** folder > **Call Detail Record Settings**).
2. Configure the following parameters:
 - From the 'Enable RADIUS Access Control' drop-down list (EnableRADIUS), select **Enable**.
 - From the 'RADIUS Accounting Type' drop-down list (RADIUSAccountingType), select the stage of the call that RADIUS accounting messages are sent to the RADIUS accounting server.
 - From the 'AAA Indications' drop-down list (AAAIndications), select whether you want Authentication, Authorization and Accounting (AAA) indications.

For a detailed description of the parameters, see "RADIUS Parameters" on page 835.

Figure 49-13: Configuring RADIUS Accounting

RADIUS ACCOUNTING SETTING

Enable RADIUS Access Control	Disable ⚡
RADIUS Accounting Type	At Call Release
AAA Indications	None

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

The table below lists the RADIUS Accounting CDR attributes included in the communication packets transmitted between the device and a RADIUS server.

Table 49-6: Supported RADIUS Accounting CDR Attributes

Attribute ID	Attribute Name	Vendor-Specific Attribute (VSA) ID	Description	Value Format	Example	AAA
Request Attributes						
1	user-name	(Standard)	Account number or calling party number or blank	String up to 15 digits long	5421385747	Start Acc Stop Acc
4	nas-ip-address	(Standard)	IP address of the requesting device	Numeric	192.168.14.43	Start Acc Stop Acc
6	service-type	(Standard)	Type of service requested	Numeric	1: login	Start Acc Stop Acc
26	h323-	1	SIP call identifier	Up to	h323-incoming-	Start

Attribute ID	Attribute Name	Vendor-Specific Attribute (VSA) ID	Description	Value Format	Example	AAA
	incoming-conf-id			32 octets	conf-id=38393530	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	h323-setup-time=09:33:26.621 Mon Dec 2014	Start Acc Stop Acc
26	h323-call-origin	26	Originator of call: <ul style="list-style-type: none"> ▪ "answer": Call originated from the incoming leg ▪ "originate": Call originated from the outgoing leg 	String	h323-call-origin=answer	Start Acc Stop Acc
26	h323-call-type	27	Protocol type or family used on this leg of the call. The value is always "VOIP".	String	h323-call-type=VOIP	Start Acc Stop Acc
26	h323-connect-time	28	Connect time in NTP format	String	h323-connect-time=09:33:37.657 UTC Mon Dec 08 2015	Stop Acc
26	h323-disconnect-time	29	Disconnect time in NTP format	String	-	Stop Acc
26	h323-disconnect-cause	30	Disconnect cause code (Q.850)	Numeric	h323-disconnect-cause=16	Stop Acc
26	h323-gw-id	33	Name of the gateway	String	h323-gw-id=<SIP ID string>	Start Acc Stop Acc
26	sip-call-id	34	SIP Call ID	String	sip-call-id=abcde@ac.com	Start Acc Stop Acc
26	call-terminator	35	Terminator of the	String	call-terminator=yes	Stop

Attribute ID	Attribute Name	Vendor-Specific Attribute (VSA) ID	Description	Value Format	Example	AAA
			call: <ul style="list-style-type: none"> "yes": Call terminated by the outgoing leg "no": Call terminated by the incoming leg 			Acc
26	terminator	37	Terminator of the call: <ul style="list-style-type: none"> "answer": Call originated from the incoming leg "originate": Call originated from the outgoing leg 	String	terminator=originate	Stop Acc
30	called-station-id	(Standard)	Destination URI	String	8004567145	Start Acc
31	calling-station-id	(Standard)	Source URI	String	5135672127	Start Acc Stop Acc
40	acct-status-type	(Standard)	Account Request Type - start (1) or stop (2) Note: 'start' isn't supported on the Calling Card application.	Numeric	1	Start Acc Stop Acc
41	acct-delay-time	(Standard)	No. of seconds tried in sending a particular record	Numeric	5	Start Acc Stop Acc
42	acct-input-octets	(Standard)	Number of octets received for that call duration (applicable only if media anchoring)	Numeric	-	Stop Acc
43	acct-output-octets	(Standard)	Number of octets sent for that call duration (applicable only if media anchoring)	Numeric	-	Stop Acc
44	acct-session-id	(Standard)	A unique accounting identifier - match start & stop	String	34832	Start Acc Stop Acc

Attribute ID	Attribute Name	Vendor-Specific Attribute (VSA) ID	Description	Value Format	Example	AAA
46	acct-session-time	(Standard)	For how many seconds the user received the service	Numeric	-	Stop Acc
47	acct-input-packets	(Standard)	Number of packets received during the call	Numeric	-	Stop Acc
48	acct-oputput-packets	(Standard)	Number of packets sent during the call	Numeric	-	Stop Acc
61	nas-port-type	(Standard)	Physical port type of device on which the call is active	String	0: Asynchronous	Start Acc Stop Acc
Response Attributes						
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	(Standard)	A unique accounting identifier – match start & stop	String	-	Stop Acc

Below is an example of RADIUS Accounting, where 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
```

Part X

Diagnostics

50 Syslog and Debug Recording

For debugging and troubleshooting, you can use the device's Syslog and/or Debug Recording capabilities:

- **Syslog:** 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.
- **Debug Recording:** The device can send debug recording packets to a debug 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 server defined by IP address. The debug recording can be done for different types of traffic such as 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: You can include Syslog messages in debug recording (see "Configuring Log Filter Rules" on page 693).

50.1 Configuring Log Filter Rules

The Logging Filters table lets you configure up to 60 rules for filtering debug recording packets, Syslog messages, and Call Detail Records (CDR). The log filter determines the calls for which you want to generate debug recording packets, Syslog messages or CDRs. For example, you can add a rule to generate Syslog messages only for calls belonging to IP Groups 2 and 4, or for calls belonging to all IP Groups except IP Group 3. You can also configure log filters for generating CDRs only and saving them on the device (local storage). Debug recording log filters can include signaling information (such as SIP messages), Syslog messages, CDRs, media (RTP, RTCP, and T.38), and pulse-code modulation (PCM).

If you don't configure any rules in the Logging Filters table and you have globally enabled debug recording (by configuring the Debug Recording server's address - see Note below), Syslog (global parameter - see Note below), and/or CDR generation (global parameter for enabling Syslog - see Note below), logs are generated for all calls. Thus, the benefit of log filtering is that it allows you to create logs per specific calls, eliminating the need for additional device resources (CPU consumption) otherwise required when logs are generated for all calls.

You can enable and disable configured Log Filter rules. Enabling a rule activates the rule, whereby the device starts generating the debug recording packets, Syslog messages, or CDRs. Disabling a rule is useful, for example, if you no longer require the rule, but may need it in the future. Thus, instead of deleting the rule entirely, you can simply disable it.



Note:

- If you want to configure a Log Filter rule that logs Syslog messages to a Syslog server (i.e., not to a Debug Recording server), you must enable Syslog functionality, using the 'Enable Syslog' (EnableSyslog) parameter (see "Enabling Syslog" on page 703). Enabling Syslog functionality is not required for rules that include Syslog messages in the debug recording sent to the Debug Recording server.
- To configure the Syslog server's address, see "Configuring the Syslog Server Address" on page 703. To configure additional, global Syslog settings, see "Configuring Syslog" on page 698.
- To configure the Debug Recording server's address, see "Configuring the Debug Recording Server Address" on page 708.
- To configure additional, global CDR settings such as at what stage of the call the CDR is generated (e.g., start and end of call), see "Configuring CDR Reporting" on page 682.

The following procedure describes how to configure Log Filter rules through the Web interface. You can also configure it through ini file (LoggingFilters) or CLI (configure troubleshoot > logging logging-filters).

➤ **To configure a Log Filter rule:**

1. Open the Logging Filters table (**Troubleshoot** menu > **Troubleshoot** tab > **Logging** folder > **Logging Filters**).
2. Click **New**; the following dialog box appears:

Figure 50-1: Logging Filters Table - Add Dialog Box

3. Configure a Log Filtering rule according to the parameters described in the table below.
4. Click **Apply**.

Table 50-1: Logging Filters Table Parameter Descriptions

Parameter	Description
Index [LoggingFilters_Index]	Defines an index number for the new table row. Note: Each row must be configured with a unique index.

Parameter	Description
Filter Type filter-type [LoggingFilters_FilterType]	Defines the filter type criteria. <ul style="list-style-type: none"> ▪ [1] Any (default) ▪ [8] IP Group = Filters log by IP Group. To configure IP Groups, see "Configuring IP Groups" on page 329. ▪ [9] SRD = Filters log by SRD. To configure SRDs, see Configuring SRDs on page 311. ▪ [10] Classification = Filters log by Classification rule. To configure Classification rules, see Configuring Classification Rules on page 461. ▪ [11] IP-to-IP Routing = Filters log by IP-to-IP routing rule. To configure IP-to-IP routing rules, see Configuring SBC IP-to-IP Routing Rules on page 470. ▪ [12] User = Filters log by user. The user is defined by username or username@hostname in the Request-URI of the SIP Request-Line. For example, "2222@10.33.45.201", which represents the following INVITE: <pre style="background-color: #f0f0f0; padding: 5px;">INVITE sip:2222@10.33.45.201;user=phone SIP/2.0</pre> ▪ [13] IP Trace = Filters log by an IP network trace, Wireshark-like expression. For more information, see "Filtering IP Network Traces" on page 697. ▪ [14] SIP Interface = Filters log by SIP Interface. To configure SIP Interfaces, see Configuring SIP Interfaces on page 321.
Value value [LoggingFilters_Value]	Defines the value for the filtering type configured in the 'Filter Type' parameter. The value can include the following: <ul style="list-style-type: none"> ▪ A single value. ▪ A range, using a hyphen "-" between the two values. For example, to specify IP Groups 1, 2 and 3, configure the parameter to "1-3" (without apostrophes). ▪ Multiple, non-contiguous values, using commas "," between each value. For example, to specify IP Groups 1, 3 and 9, configure the parameter to "1,3,9" (without apostrophes). ▪ The exclamation (!) wildcard character can be used for excluding a specific configuration entity from the filter. For example, to include all IP Groups in the filter except IP Group ID 2, configure the 'Filter Type' parameter to IP Group and the 'Value' parameter to "!2" (without apostrophes). Note that a Logging Filter rule applies to the entire session, which is both legs (i.e., not per leg). For example, a call between IP Groups 1 and 2 are logged for both legs even if the 'Value' parameter is configured to "!2". ▪ Any to indicate all. Note: <ul style="list-style-type: none"> ▪ You can use the index number or string name to specify the configuration entity for the following 'Filter Types': IP Group, SRD, Classification, IP-to-IP Routing, or SIP Interface. For example, to specify IP Group at Index 2 with the name "SIP Trunk", configure the parameter to either "2" or "SIP Trunk" (without apostrophes). ▪ For IP trace expressions, see "Filtering IP Network Traces" on

Parameter	Description
	page 697.
Log Destination log-dest [LoggingFilters_LogDestination]	Defines where the device sends the log file. <ul style="list-style-type: none"> ▪ [0] Syslog Server = The device generates Syslog messages based on the configured log filter and sends them to a user-defined Syslog server. The Syslog messages can contain one of the following types of information, depending on the settings of the 'Log Type' parameter (described later): <ul style="list-style-type: none"> ✓ Not configured (default): Syslog messages include regular syslog information. ✓ CDR Only: Syslog messages include only CDRs (no system information and alerts). ▪ [1] Debug Recording Server = (Default) The device generates debug recording packets based on the configured log filter and sends them to a user-defined Debug Recording server. ▪ [2] Local Storage = The device generates CDRs based on the configured log filter and stores them locally on the device. For more information on local CDR storage, see Storing CDRs on the Device on page 683. <p>Note:</p> <ul style="list-style-type: none"> ▪ If the 'Filter Type' parameter is configured to IP Trace, you must configure the parameter to Debug Recording Server. ▪ If you configure the parameter to Local Storage, you must configure the 'Log Type' parameter to CDR Only. ▪ If you configure the parameter to Syslog Server and the debug level (GwDebugLevel) is configured to No Debug (see "Configuring Syslog Debug Level" on page 704), the Syslog messages include only system Warnings and Errors. ▪ If you configure the parameter to Debug Recording Server, you can also include Syslog messages in the debug recording packets sent to the debug recording server. To include Syslog messages, configure the 'Log Type' parameter (see below) to the relevant option.
Log Type log-type [LoggingFilters_CaptureType]	Defines the type of messages to include in the log file. <ul style="list-style-type: none"> ▪ [0] = (Default) Not configured. The option is applicable only for sending Syslog messages to a Syslog server (i.e., 'Log Destination' parameter is configured to Syslog Server). ▪ [1] Signaling = The option is applicable only to debug recording (i.e., 'Log Destination' parameter is configured to Debug Recording Server). The debug recording includes signaling information such as SIP signaling messages, Syslog messages, CDRs, and the device's internal processing messages. ▪ [2] Signaling & Media = The option is applicable only to debug recording (i.e., 'Log Destination' parameter is configured to Debug Recording Server). The debug recording includes signaling, Syslog messages, and media (RTP/RTCP/T.38). ▪ [3] Signaling & Media & PCM = The option is applicable only to debug recording (i.e., 'Log Destination' parameter is configured to Debug Recording Server). The debug recording includes signaling, Syslog messages, media, and PCM. ▪ [5] CDR Only = Only CDRs are generated. The option is applicable only if the 'Log Destination' parameter is configured to Syslog Server or Local Storage. When configured to Syslog

Parameter	Description
	<p>Server, only CDRs are included in the Syslog messages (excluding all system logs and alerts) sent to the Syslog server.</p> <p>Note:</p> <ul style="list-style-type: none"> ▪ If you configure the 'Log Destination' parameter to Local Storage, the 'Log Type' parameter must be configured to CDR Only. ▪ The parameter is not applicable when the 'Filter Type' parameter is configured to IP Trace. ▪ To include Syslog messages in debug recording, it is unnecessary to enable Syslog functionality.
Mode mode [LoggingFilters_Mode]	Enables and disables the rule. <ul style="list-style-type: none"> ▪ [0] Disable ▪ [1] Enable (default)

50.1.1 Filtering IP Network Traces

You can filter Syslog and debug recording messages for IP network traces, by configuring 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>). Network traces are typically used to record HTTP.

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:

Table 50-2: Supported Wireshark-like Expressions for 'Value' Parameter

Expression	Description
ip.src, ip.dst	Source and destination IP address
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' parameter is undefined, the device records all IP traffic types.
- You cannot use ip.addr or udp/tcp.port together with ip.src/dst or udp/tcp.srcport/dstport. For example, "ip.addr==1.1.1.1 and ip.src==2.2.2.2" is an invalid configuration value.

50.2 Configuring Syslog

This section describes how to configure Syslog. To filter Syslog messages, see "Configuring Log Filter Rules" on page 693.

50.2.1 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 "Enabling Syslog" on page 703).

Syslog includes two types of log messages:

- SIP call session logs: Logs relating to call sessions (e.g., call established). These logs are identified by a session ID ("SID"), described in detail in the table below. The following is an example of a SIP-session related Syslog message:

```
13:10:57.811 : 10.13.4.12 : NOTICE : [S=235][SID:2ed1c8:96:5]
(lgr_flow)(63) UdpTransportObject#0- Adding socket event for
address 10.33.2.42:5060 [Time: 04-19-2012@18:29:39]
```

- Board logs: Logs relating to the operation of the device (infrastructure) that are non-call session related (e.g., device reset or Web login). These logs are identified by a board ID ("BID"), described in detail in the table below. The following is an example of a board Syslog message:

```
10:21:28.037 : 10.15.7.95 : NOTICE : [S=872] [BID=3aad56:32]
Activity Log: WEB: Successful login at 10.15.7.95:80. User:
Admin. Session: HTTP (10.13.22.54)
```

The format of the Syslog message is described in the following table below:

Table 50-3: Syslog Message Format Description

Message Item	Description
Message Types	<p>Syslog generates the following types of messages:</p> <ul style="list-style-type: none"> ▪ ERROR: Indicates that a problem has been identified that requires immediate handling. ▪ WARNING: Indicates an error that might occur if measures are not taken to prevent it. ▪ NOTICE: Indicates that an unusual event has occurred. ▪ INFO: Indicates an operational message. ▪ DEBUG: Messages used for debugging.

Message Item	Description
	<p>Note:</p> <ul style="list-style-type: none"> The INFO and DEBUG messages are required only for advanced debugging and by default, they are not sent by the device. When viewing Syslog messages in the Web interface, these message types are color coded.
<p>Message Sequence Number [S=<number>]</p>	<p>By default, Syslog messages are sequentially numbered in the format [S=<number>], for example, "[S=643]". A skip in the number sequence of messages indicates a loss of message packets. For example, in the below Syslog, messages 238 through 300 were not received. In other words, 63 Syslog messages were lost (the sequential numbers are indicated below in bold font):</p> <pre>18:38:14. 52 : 10.33.45.72 : NOTICE: [S=235][SID:2ed1c8:96:5] (lgr_psbrdex)(619) rcv <-- 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=236][SID:2ed1c8:96:5] (lgr_flow)(620) #0:DIGIT_EV [File: Line:-1] 18:38:14. 83 : 10.33.45.72 : NOTICE: [S=237][SID:2ed1c8:96:5] (lgr_flow)(621) #0:DIGIT_EV [File: Line:-1] 18:38:14.958 : 10.33.45.72 : NOTICE: [S=301][SID:2ed1c8:96:5] (lgr_flow)(625) #0:DIGIT_EV [File: Line:-1]</pre> <p>You can disable the inclusion of the message sequence number in Syslog messages, by setting the 'CDR Syslog Sequence Number' parameter to Disable (see "Configuring Syslog" on page 703).</p>
<p>Log Number (lgr)(number)</p>	<p>Ignore this number; it has been replaced by the Message Sequence Number (described previously).</p>
<p>Session ID (SID)</p>	<p>Unique SIP call session and device identifier. The device identifier facilitates debugging by clearly identifying the specific device that sent the log message, especially useful in deployments consisting of multiple devices. In addition, the benefit of unique numbering is that it enables you to filter the information (such as SIP, Syslog, and media) according to device or session ID.</p> <p>The syntax of the session and device identifiers are as follows:</p> <p>[SID=<unique number generated during software installation>:<number of times device has reset>:<unique SID counter indicating the call session; increments consecutively for each new session; resets to 1 after a device reset>]</p> <p>For example:</p> <pre>14:32:52.028: 10.33.8.70: NOTICE: [S=9369] [SID=2ed1c8:96:5] (lgr_psbrdex)(274) rcv <-- OFF_HOOK Ch:4</pre> <p>Where:</p>

Message Item	Description
	<ul style="list-style-type: none"> ▪ <i>2ed1c8</i> is the device's MAC address. ▪ 96 is the number of times the device has reset. ▪ 5 is a unique SID session number (in other words, this is the fifth call session since the last device reset). ✓ ✓ A session includes both the outgoing and incoming legs, where both legs share the same session number. ✓ Forked legs and alternative legs share the same session number.
Board ID (BID)	<p>Unique non-SIP session related (e.g., device reset) and device identifier. The device identifier facilitates debugging by clearly identifying the specific device that sent the log message, especially useful in deployments consisting of multiple devices. In addition, the benefit of unique numbering is that it enables you to filter the information according to device.</p> <p>The syntax of the BID is as follows: [BID=<unique number generated during software installation>:<number of times device has reset>]</p> <p>For example: 14:32:52.062: 10.33.8.70: WARNING: [S=9399] [BID=2ed1c8:96] invalid Physical index</p> <p>Where:</p> <ul style="list-style-type: none"> ▪ <i>2ed1c8</i> is the device's MAC address. ▪ 96 is the number of times the device has reset.
Message Body	Describes the message.
Timestamp	When the Network Time Protocol (NTP) is enabled, a timestamp string [hour:minutes:seconds] is added to all Syslog messages.

50.2.1.1 Event Representation in Syslog Messages

The Syslog message events that the device sends are denoted by unique abbreviations. The following example shows an abbreviated event in a Syslog message indicating packet loss (PL):

```
Apr  4 12:00:12 172.30.1.14 PL:5 [Code:3a002] [CID:3294] [Time:20:17:00]
```

The table below lists the unique event abbreviations:

Table 50-4: Syslog Error Name Descriptions

Error Abbreviation	Error Name Description
AA	Invalid Accumulated Packets Counter
AC	Invalid Channel ID
AL	Invalid Header Length
AO	Invalid Codec Type

Error Abbreviation	Error Name Description
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

50.2.1.2 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 by IP address, you can filter messages by Facility level.

➤ **To configure the Facility level:**

- Configure the SyslogFacility ini file parameter to one of the following options:

Table 50-5: Syslog Facility Levels

Numerical Value	Facility Level
16 (default)	local use 0 (local0)
17	local use 1 (local1)
18	local use 2 (local2)
19	local use 3 (local3)
20	local use 4 (local4)
21	local use 5 (local5)
22	local use 6 (local6)
23	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)
```

50.2.1.3 Syslog Fields for Answering Machine Detection (AMD)

The Syslog message can include information relating to the Answering Machine Detection (AMD) feature. AMD is used to detect whether a human (including a fax machine), an answering machine, silence, or answering machine beeps have answered the call on the remote side.

- AMDSignal – the field can acquire one of the following values:
 - voice (V)
 - answer machine (A)
 - silence (S)
 - unknown (U)
- AMDDecisionProbability – probability (in %) success that correctly detects answering type

Below is an example of such a Syslog message with AMD information:

```
CallMachine:EVENT_DETECTED_EV - AMDSignal = <type - V/A/S/U>,
AMDDecisionProbability = <percentage> %
```

If there is no AMD detection, the AMDSignal field is shown empty (i.e. AMDSignal =).

For more information on the AMD feature, see "Answering Machine Detection (AMD)" on page 192.

50.2.1.4 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 50-6: Syslog Message Severity

ITU Perceived Severity (SNMP Alarm's Severity)	AudioCodes' Syslog Severity
Critical	RecoverableMsg
Major	RecoverableMsg
Minor	RecoverableMsg
Warning	Notice
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:

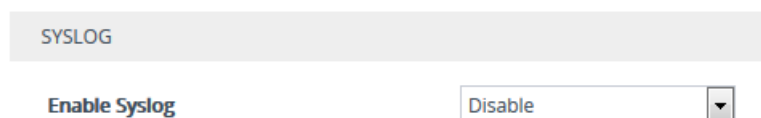
50.2.2 Enabling Syslog

The following procedure describes how to enable Syslog.

➤ **To enable Syslog:**

1. Open the Syslog Settings page (**Troubleshoot** menu > **Troubleshoot** tab > **Logging** folder > **Syslog Settings**).
2. From the 'Enable Syslog' drop-down list, select **Enable**.

Figure 50-2: Enabling Syslog



3. Click **Apply**.

50.2.3 Configuring the Syslog Server Address

The following procedure describes how to configure the Syslog server's address to where the device sends Syslog messages.

➤ **To configure the Syslog server address:**

1. Open the Syslog Settings page (**Troubleshoot** menu > **Troubleshoot** tab > **Logging** folder > **Syslog Settings**).
2. In the 'Syslog Server IP' field (SyslogServerIP), enter the IP address of the Syslog server.
3. In the 'Syslog Server Port' field, enter the port of the Syslog server.

Figure 50-3: Configuring the Syslog Server Address

Syslog server IP	0.0.0.0
Syslog Server Port	514

4. Click **Apply**.

50.2.4 Configuring Syslog Debug Level

You can configure the amount of information (debug level) to include in Syslog messages. You can also enable the device to send multiple Syslog messages bundled into a single packet, and enable a protection mechanism that automatically lowers the debug level when the device's CPU resources become low, ensuring sufficient CPU resources are available for processing voice traffic.

➤ **To configure the Syslog debug level:**

1. Open the Syslog Settings page (**Troubleshoot** menu > **Troubleshoot** tab > **Logging** folder > **Syslog Settings**).

Figure 50-4: Configuring Syslog Debug Level

Syslog CPU Protection	Enabled
Syslog Optimization	Disabled
Debug Level	No Debug

2. From the 'Debug Level' (GwDebugLevel) drop-down list, select the debug level of Syslog messages:
 - **No Debug:** Disables Syslog and no Syslog messages are sent.
 - **Basic:** Sends debug logs of incoming and outgoing SIP messages.
 - **Detailed:** Sends debug logs of incoming and outgoing SIP message as well as many other logged processes.
3. From the 'Syslog Optimization' (SyslogOptimization) drop-down list, select whether you want the device to accumulate and bundle multiple debug messages into a single UDP packet before sending it to a Syslog server. The benefit of the feature is that it reduces the number of UDP Syslog packets, thereby improving (optimizing) CPU utilization. The size of the bundled message is configured by the MaxBundleSyslogLength parameter.
4. From the 'Syslog CPU Protection' (SyslogCpuProtection) drop-down list, select whether you want to enable the protection feature for the device's CPU resources during debug reporting, ensuring voice traffic is unaffected. If CPU resources drop (i.e., high CPU usage) to a critical level (user-defined threshold), the device automatically lowers the debug level to free up CPU resources that were required for the previous debug-level functionality. When CPU resources become available again, the device increases the debug level to its' previous setting. For example, if you set the 'Debug Level' to **Detailed** and CPU resources decrease to the defined threshold, the device automatically changes the level to **Basic**, and if that is not enough, it

changes the level to **No Debug**. Once CPU resources are returned to normal, the device automatically changes the debug level back to its' original setting (i.e., **Detailed**). The threshold is configured by the DebugLevelHighThreshold parameter.

5. Click **Apply**.

50.2.5 Configuring Reporting of Management User Activities

The device can report operations (activities) performed in the device's management interfaces (e.g., Web and CLI) by management users, in Syslog messages. The Syslog message indicates these logs with the string "Activity Log". Each logged user activity includes the following information:

- Username (e.g., "Admin") of the user that performed the action
- IP address of the client PC from where the Web user accessed the management interface
- Protocol used for the session (e.g., SSH or HTTP)

The following example shows a Web-user activity log (indicating a login action) with the above-mentioned information:

```
14:07:46.300 : 10.15.7.95 : Local 0 :NOTICE : [S=3149]
[BID=3aad56:32] Activity Log: WEB: Successful login at
10.15.7.95:80. User: Admin. Session: HTTP (10.13.22.54)
```

The device can report the following user activities:

- Modifications of individual parameters, for example:


```
14:33:00.162 : 10.15.7.95 : Local 0 :NOTICE : [S=3403]
[BID=3aad56:32] Activity Log: Max Login Attempts was changed
from '3' to '2'. User: Admin. Session: HTTP (10.13.22.54)
```
- Modifications of table fields, and addition and deletion of table rows, for example:


```
14:42:48.334 : 10.15.7.95 : NOTICE : [S=3546] [BID=3aad56:32]
Activity Log: Classification - remove line 2. User: Admin.
Session: HTTP (10.13.22.54)
```
- Entered CLI commands (modifications of security-sensitive commands are logged without the entered value).
- Configuration file load (reported without per-parameter notifications).
- Auxiliary file load and software update.
- Device reset and burn to flash memory.
- Access to unauthorized Web pages according to the Web user's access level.
- Modifications of "sensitive" parameters.
- Login and logout.
- Actions that are not related to parameter changes (for example, file uploads, file delete, lock-unlock maintenance actions, LDAP clear cache, register-unregister, and start-stop trunk. In the Web, these actions are typically done by clicking a button (e.g., the LOCK button).

For more information on each of the above listed options, see "Syslog, CDR and Debug Parameters" on page 758.

The following procedure describes how to configure management user activity logging through the Web interface. You can also configure it through ini file (ActivityListToLog) or CLI (configure troubleshoot > activity-log).

➤ To configure reporting of Web user activities:

1. Open the Syslog Settings page (**Troubleshoot** tab > **Troubleshoot** menu > **Logging**

folder > **Syslog Settings**).

2. Under the Activity Types to Report group, select the Web actions to report to the Syslog server:

Figure 50-5: Configuring Web Activities to Report to Syslog

ACTIVITY TYPES TO REPORT	
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"/>
Non-Authorized Access	<input type="checkbox"/>
Sensitive Parameters Value Change	<input type="checkbox"/>
Login and Logout	<input type="checkbox"/>
CLI Activity	<input type="checkbox"/>
Action Executed	<input type="checkbox"/>

3. Click **Apply**.



Note:

- You can also view logged user activities in the Web interface (see "Viewing Web User Activity Logs" on page 647).
- Logging of CLI commands can only be configured through CLI or ini file.
- You can configure the device to send an SNMP trap each time a user performs a Web activity. For more information, see "Configuring SNMP Community Strings" on page 83.

50.2.6 Viewing Syslog Messages

You can receive and view Syslog messages generated by the device using any of the following Syslog server types:

- **Wireshark:** Third-party, network protocol analyzer (<http://www.wireshark.org>).



Note: When debug recording is enabled and Syslog messages are also included in the debug recording, to view Syslog messages using Wireshark, you must install AudioCodes' Wireshark plug-in (acsyslog.dll). Once the plug-in is installed, the Syslog messages are decoded as "AC SYSLOG" and displayed using the "acsyslog" filter (instead of the regular "syslog" filter). For more information on debug recording, see "Debug Recording" on page 707.

- **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.
- **Device's CLI Console:** The device sends error messages (e.g., Syslog messages) to the CLI as well as to the configured destination. Use the following commands:
 - To start debug recording:

```
debug log
```


- To stop debug recording:
no debug log
- To stop all debug recording:
no debug log all
- **Device's Web Interface:** The device provides an embedded Syslog server, which is accessed through the Web interface (**Troubleshoot** tab > **Troubleshoot** menu > **Message Log** ) . This provides limited Syslog server functionality.

Figure 50-6: Viewing Message Log in Web Interface

```

Log is Activated

17:17:11 Opening Log Web Page [Code:0x40529 File:RpCgi.cpp Line:2481]
17:17:11 Starting Log Session successfully [Code:0x40529 File:RpCgi.cpp Line:2482]
17:17:11 Opening Log Web Page [Code:0x40529 File:RpCgi.cpp Line:2481]
17:17:11 Starting Log Session successfully [Code:0x40529 File:RpCgi.cpp Line:2482]
17:17:17 ( dns_resolver) HandleSrvRecordQuery - Can't find SRV domain name in ip
17:17:17 ( lgr_psbrdif) !! [ERROR] DNSGetServiceInfo- problem with service name
17:17:17 ( dns_resolver) DoSRVQuery- SrvQueryString:_sips._tcp.6666666666666666 is
17:17:17 ( dns_resolver) DNSResolver::HandleTimerExpOnWaitSrvRecord: SrvQuerySta
17:17:17 ( lgr_psbrdif) !! [ERROR] DNSGetServiceInfo- problem with service name
17:17:17 ( dns_resolver) HandleARecordQuery - Host:6666666666666666 is not in cach
17:17:17 ( dns_resolver) DNSResolver::HandleTimerExpiredOnWaitForARecord: host:6

```

The displayed logged messages are color-coded as follows:

- **Green:** Opening messages at start of message log
- **Black:** Notice messages
- **Blue:** Warning (error) messages

To stop and clear the Message Log, close the Message Log page by accessing any another page in the Web interface.



Note:

- 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 displayed on the 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.

50.3 Configuring Debug Recording

This section describes how to configure debug recording and how to collect debug recording packets.



Note:

- Debug recording is collected only on the device's OAMP interface.
- For a detailed description of the debug recording parameters, see "Syslog, CDR and Debug Parameters" on page 758.

50.3.1 Configuring the Debug Recording Server Address

The procedure below describes how to configure the address of the debug recording server to where the device sends the captured traffic. Once you configure an address, the device generates debug recording packets for all calls. However, you can configure the device to generate debug recording packets for specific calls, using Logging Filter rules in the Logging Filters table (see "Configuring Log Filter Rules" on page 693).

➤ **To configure the debug recording server's address:**

1. Open the Logging Settings page (**Troubleshoot** tab > **Troubleshoot** menu > **Logging** folder > **Logging Settings**).

Figure 50-7: Configuring Debug Recording Server

DEBUG RECORDING	
Debug Recording Destination IP	<input type="text" value="0.0.0.0"/>
Debug Recording Destination Port	<input type="text" value="925"/>

2. In the 'Debug Recording Destination IP' field, configure the IP address of the debug capturing server.
3. In the 'Debug Recording Destination Port' field, configure the port of the debug capturing server.
4. Click **Apply**.

50.3.2 Collecting Debug Recording Messages

To collect debug recording packets, use the open source packet capturing program, Wireshark. AudioCodes proprietary plug-in files for Wireshark are required.



Note:

- The default debug recording port is 925. You can change the port in Wireshark (**Edit** menu > **Preferences** > **Protocols** > **AC DR**).
- The plug-in files are per major software release of Wireshark. For more information, contact your AudioCodes sales representative.
- The plug-in files are applicable only to Wireshark 32-bit for Windows.

➤ **To install Wireshark and the plug-ins for debug recording:**

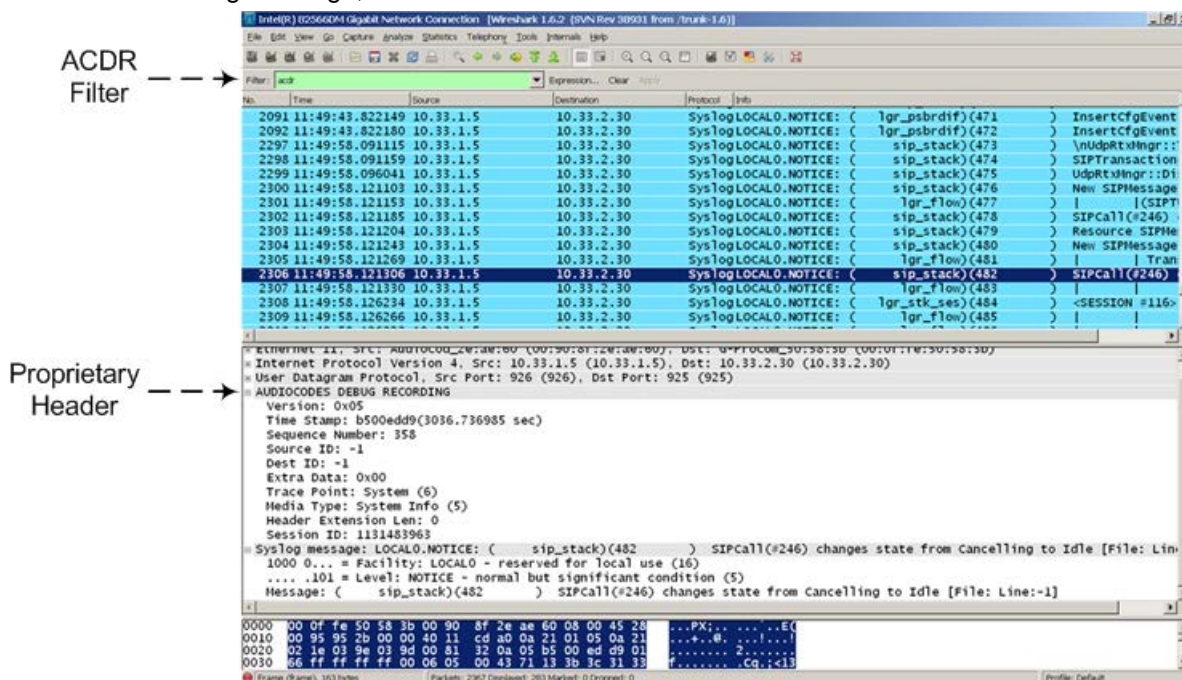
1. Install Wireshark on your computer. The Wireshark program can be downloaded from <http://www.wireshark.org>.
2. Download the proprietary plug-in files from www.audiocodes.com/downloads.
3. Copy the plug-in files to the directory in which you installed Wireshark, as follows:

Copy this file	To this folder on your PC
...\dtds\cdr.dtd	Wireshark\dtds\
...\plugins\<Wireshark ver.>*.dll	Wireshark\plugins\<Wireshark ver.>
...\tpncp\tpncp.dat	Wireshark\tpncp

4. Start Wireshark.

- 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:



50.3.3 Debug Capturing on Physical VoIP Interfaces

You can capture traffic on the device's physical (Ethernet LAN) VoIP interfaces (Layer-2 VLAN tagged packets). The captured traffic can be saved in a PCAP-format file (suitable for Wireshark) to a TFTP (default) or an FTP server. The generated PCAP file is in the Extensible Record Format (ERF). The maximum file size of debug captures that can be saved to the device is 100 MB.

To capture traffic on physical VoIP interfaces, use the following CLI commands:

- Starts physical VoIP debug capture:

```
# debug capture voip physical eth-lan
# debug capture voip physical start
```

- Captures packets continuously in a cyclical buffer (packets always captured until stop command):

```
# debug capture VoIP physical cyclic buffer
```

- Retrieves latest capture (PCAP file) saved on a specified server:

```
# debug capture VoIP physical get_last_capture <TFTP/FTP
server IP address>
```

The file is saved to the device's memory (not flash) and erased after a device reset.

- Marks the captured file (useful for troubleshooting process):

```
# debug capture VoIP physical insert-pad
```

Before running this command, the debug capture must be started.

- Displays debug status and configured rules:

```
# debug capture VoIP physical show
```

- Specifies the destination (FTP, TFTP, or USB) where you want the PCAP file sent:
debug capture VoIP physical target <ftp|tftp|usb>
- Stops the debug capture, creates a file named debug-capture-voip-<timestamp>.pcap, and sends it to the TFTP or FTP server:

```
# debug capture voip physical stop <TFTP/FTP server IP address>
```

If no IP address is defined, the capture is saved on the device for later retrieval.

51 Creating Core Dump and Debug Files upon Device Crash

For debugging, you can configure the device to create a core dump file and/or debug file. The files may assist you in identifying the cause of the crash. The core dump can either be included in or excluded from the debug file, or alternatively, sent separately to a TFTP server. You can then provide the files to AudioCodes support team for troubleshooting.

- **Core Dump File:** You can enable the device to send a core dump file to a remote destination upon a device crash. The core dump is a copy of the memory image at the time of the crash. It provides a powerful tool for determining the root cause of the crash. When enabled, the core dump file is sent to a user-defined TFTP server (IP address). If no address is configured, the core dump file is saved to the device's flash memory (if it has sufficient memory). Each time the device crashes, the new core dump file replaces the previous core dump file, if exists.

The core dump file is saved as a binary file with the following file name: "**core_<device name>_ver_<firmware version>_mac_<MAC address>_<date>_<time>**". For example, *core_acMediant_ver_700-8-4_mac_00908F099096_1-02-2015_3-29-29*.

- **Debug File:** You can manually retrieve the debug file from the device and save it to a folder on your local PC. The debug file contains the following information:
 - Exception information, indicating the specific point in the code where the crash occurred and a list of up to 50 of the most recent SNMP alarms that were raised by the device before it crashed.
 - Latest log messages that were recorded prior to the crash.
 - Core dump. The core dump is included **only** if core dump generation is enabled, no IP address has been configured, and the device has sufficient memory on its flash memory.
 - May include additional application-proprietary debug information.

The debug file is saved as a zipped file with the following file name: "**debug_<device name>_ver_<firmware version>_mac_<MAC address>_<date>_<time>**". For example, *debug_acMediant_ver_700-8-4_mac_00908F099096_1-03-2015_3-29-29*.

The following procedure describes how to configure core dump file creation through the Web interface.

➤ **To enable core dump file generation:**

1. Set up a TFTP server to where you want to send the core dump file.
2. Open the Debug Files page (**Troubleshoot** menu > **Troubleshoot** tab > **Debug** folder > **Debug Files**).

Figure 51-1: Debug Files Page

CORE DUMP SETTINGS

Enable Core Dump

Core Dump Destination IP

3. From the 'Enable Core Dump' drop-down list, select **Enable**.
4. (Optional) In the 'Core Dump Destination IP' field, enter an IP address of the remote server to where you want the file to be sent.
5. Click **Apply**.

You can also delete the core dump file through CLI, as described in the following procedure:

➤ **To delete the core dump file:**

- Navigate to the root CLI directory (enable mode), and then enter the following command:

```
# clear debug-file
```

The following procedure describes how to retrieve the debug file from the device through the Web interface.

➤ **To save the debug file:**

- In the Debug Files page, click the **Save Debug File** button.

52 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, 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, tone signals (e.g., DTMF), termination reasons, as well as voice quality statistics and thresholds (e.g., MOS).

52.1 Configuring Test Call Endpoints

The Test Call Rules table lets you test SIP signaling (setup and registration) and media (DTMF signals) of calls between a simulated phone on the device and a remote IP 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 endpoint can be defined as an IP Group or IP address. 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.



Note: By default, you can configure up to five test calls. However, this number can be increased by installing the relevant License Key. For more information, contact your AudioCodes sales representative.

The following procedure describes how to configure test calls through the Web interface. You can also configure it through ini file (Test_Call) or CLI (configure troubleshoot > test-call test-call-table).

➤ **To configure a test call:**

1. Open the Test Call Rules table (**Troubleshooting** tab > **Troubleshooting** menu > **Test Call** folder > **Test Call Rules**).

- Click **New**; the following dialog box appears:

Figure 52-1: Test Call Rules Table - Add Dialog Box

- Configure a test call according to the parameters described in the table below.
- Click **Apply**, and then save your settings to flash memory.

Table 52-1: Test Call Rules Table Parameter Descriptions

Parameter	Description
Common	
Index	Defines an index number for the new table row. Note: Each row must be configured with a unique index.
Endpoint URI endpoint-uri [Test_Call_EndpointURI]	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. The valid value is a string of up to 150 characters. By default, the parameter is not configured. Note: The parameter is mandatory.
Called URI called-uri [Test_Call_CalledURI]	Defines the destination (called) URI (user@host). The valid value is a string of up to 150 characters. By default, the parameter is not configured.
Route By route-by [Test_Call_RouteBy]	Defines the type of routing method. This applies to incoming and outgoing calls. <ul style="list-style-type: none"> [1] IP Group = (Default) Calls are matched by (or routed to) an IP Group. To specify the IP Group, see the 'IP Group' parameter in the table.

Parameter	Description
	<ul style="list-style-type: none"> ▪ [2] Dest Address = Calls are matched by (or routed to) a destination IP address. To configure the address, see the 'Destination Address' parameter in the table. <p>Note:</p> <ul style="list-style-type: none"> ▪ If configured to Dest Address, you must assign a SIP Interface (see the 'SIP Interface' parameter in the table). ▪ For REGISTER messages: <ul style="list-style-type: none"> ✓ If configured to IP Group, only Server-type IP Groups can be used.
IP Group ip-group-id [Test_Call_IPGroupName]	Assigns an IP Group. This is the IP Group that the test call is sent to or received from. By default, no value is defined. To configure IP Groups, see "Configuring IP Groups" on page 329. Note: <ul style="list-style-type: none"> ▪ The parameter is applicable only if you configure the 'Route By' parameter to IP Group. ▪ The IP Group is used for incoming and outgoing calls.
Destination Address dst-address [Test_Call_DestAddress]	Defines the destination host. The valid value is an IP address[:port] or DNS name[:port]. Note: The parameter is applicable only if the 'Route By' parameter is configured to Dest Address [2].
SIP Interface sip-interface-name [Test_Call_SIPInterfaceName]	Assigns a SIP Interface. This is the SIP Interface to which the test call is sent and received from. By default, no value is defined. To configure SIP Interfaces, see Configuring SIP Interfaces on page 321. Note: The parameter is applicable only if the 'Route By' parameter is configured to Dest Address .
Application Type application-type [Test_Call_ApplicationType]	Defines the application type for the endpoint. This associates the IP Group and SRD to a specific SIP interface. <ul style="list-style-type: none"> ▪ [2] SBC = SBC application Note: The parameter must always be set to SBC [2].
Destination Transport Type dst-transport [Test_Call_DestTransportType]	Defines the transport type for outgoing calls. <ul style="list-style-type: none"> ▪ [-1] = Not configured (default) ▪ [0] UDP ▪ [1] TCP ▪ [2] TLS Note: The parameter is applicable only if the 'Route By' parameter is set to Dest Address .
QoE Profile qoe-profile [Test_Call_QOEProfile]	Assigns a QoE Profile to the test call. By default, no value is defined. To configure QoE Profiles, see "Configuring Quality of Experience Profiles" on page 291.
Bandwidth Profile bandwidth-profile	Assigns a Bandwidth Profile to the test call. By default, no value is defined. To configure Bandwidth Profiles, see "Configuring Bandwidth

Parameter	Description
[Test_Call_BWProfile]	Profiles" on page 296.
Authentication	
Note: These parameters are applicable only if the 'Call Party' parameter (see below) is configured to Caller .	
Auto Register 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' parameter settings (see above). <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable
Username user-name [Test_Call_UserName]	Defines the authentication username. By default, no username is defined.
Password password [Test_Call_Password]	Defines the authentication password. By default, no password is defined.
Test Setting	
Call Party call-party [Test_Call_CallParty]	Defines whether the test endpoint is the initiator (caller) or receiving side (called) of the test call. <ul style="list-style-type: none"> ▪ [0] Caller (default) ▪ [1] Called
Maximum Channels for Session max-channels [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 configure the 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 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. Note: The parameter is applicable only if you configure 'Call Party' to Caller .
Calls per Second calls-per-second [Test_Call_CallsPerSecond]	Defines the number of calls per second. Note: The parameter is applicable only if you configure 'Call Party' to Caller .
Test Mode test-mode [Test_Call_TestMode]	Defines the test session mode. <ul style="list-style-type: none"> ▪ [0] Once = (Default) The test runs until the lowest value between the following is reached: <ul style="list-style-type: none"> ✓ Maximum channels is reached for the test session, configured by 'Maximum Channels for Session'. ✓ Call duration ('Call Duration') multiplied by calls per second ('Calls per Second'). ✓ Test duration expires, configured by 'Test Duration'. ▪ [1] Continuous = The test runs until the configured test duration is reached. If it reaches the maximum channels configured for

Parameter	Description
	<p>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.</p> <p>Note: The parameter is applicable only if you configure 'Call Party' to Caller.</p>
Test Duration test-duration [Test_Call_TestDuration]	<p>Defines the test duration (in minutes). The valid value is 0 to 100000. The default is 0 (i.e., unlimited).</p> <p>Note: The parameter is applicable only if you configure 'Call Party' to Caller.</p>
Play play [Test_Call_Play]	<p>Enables and defines the playing of a tone to the answered side of the call.</p> <ul style="list-style-type: none"> ▪ [0] Disable ▪ [1] DTMF = (Default) Plays a user-defined DTMF string, configured in "Configuring DTMF Tones for Test Calls" on page 720. ▪ [2] PRT = Plays a non-DTMF tone from the PRT file (Dial Tone 2). For this option, you must load a PRT file to the device (see "Prerecorded Tones File" on page 590). <p>Note:</p> <ul style="list-style-type: none"> ▪ To configure the DTMF signaling type (e.g., out-of-band or in-band) use the 'DTMF Transport Type' parameter (see Configuring DTMF Transport Types). ▪ The parameter is applicable only if you configure 'Call Party' to Caller.
Schedule Interval schedule-interval [Test_Call_ScheduleInterval]	<p>Defines the interval (in minutes) between automatic outgoing test calls. The valid value range is 0 to 100000. The default is 0 (i.e., scheduling is disabled).</p> <p>Note: The parameter is applicable only if you configure 'Call Party' to Caller.</p>

52.2 Starting and Stopping Test Calls

The following procedure describes how to start, stop, and restart test calls.

➤ **To start, stop, and restart a test call:**

1. In the Test Call Rules table, select the required test call entry.
2. From the **Action** drop-down list, choose the required command:
 - **Dial:** Starts the test call (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.

52.3 Viewing Test Call Status

You can view the status of test call rules in the 'Test Status' field of the Test Call Rules table. The status can be one of the following:

Table 52-2: Test Call Status Description

Status	Description
"Idle"	Test call is not active.
"Scheduled"	Test call is planned to run (according to the 'Schedule Interval' parameter).
"Running"	Test call has been started (i.e., by clicking Dial from the 'Action' drop-down list).
"Receiving":	Test call has been automatically activated by calls received from the remote endpoint for the test call endpoint (when all these calls end, the status returns to "Idle").
"Terminating"	Test call is in the process of terminating currently established calls (when Drop Call is clicked from the 'Action' drop-down list to stop the test).
"Done"	Test call has successfully completed (or was prematurely stopped by clicking the Drop Call from the 'Action' drop-down list).

52.4 Viewing Test Call Statistics

You can view statistical information on the test call.



Note:

- On the receiving side, when the first call is accepted in "Idle" state, statistics are reset.
- The device also generates CDRs for test calls if you have enabled CDR generation (see "Configuring CDR Reporting" on page 682). To view CDRs of test calls, see Viewing CDR Test Calls on page 659.

➤ **To view statistics of a test call:**

1. In the Test Call Rules table, select the required test call row.

2. Scroll down the page to the area below the table. Statistics of the selected test call are displayed under the **Statistics** group, as shown in the example below:

Figure 52-2: Viewing Test Call Statistics

STATISTICS	
Active Calls	0
Call Attempts	1
Total Established Calls	1
Total Failed Attempts	0
Remote Disconnections Count	1
Average CPS	1.00
Elapsed Time [HH:MM:SS]	00:00:20
Test Status	Done
Detailed Status	Done - Established Calls: 1, ASR: 100%
MOS Status	Local:N/A, Remote:N/A
Delay Status	Local:6 msec (Green), Remote:N/A
Jitter Status	Local:75 msec (Red), Remote:0 msec (Green)
Packet Loss Status	Local:0% (Green), Remote:0% (Green)
Bandwidth Status	Rx:0 KBytes/s (Green), Tx:0 KBytes/s (Green)

The statistics fields are described in the following table:

Table 52-3: Test Call Statistics Description

Statistics Field	Description
Active Calls	Number of currently established test calls.
Call Attempts	Number of calls that were attempted.
Total Established Calls	Total number of calls that were successfully established.
Total Failed Attempts	Total number of call attempts that failed.
Remote Disconnections Count	Number of calls that were disconnected by the remote side.
Average CPS	Average calls per second.
Elapsed Time	Duration of the test call since it was started (or restarted).
Test Status	Status (brief description) as displayed in the 'Test Status' field (see "Viewing Test Call Status" on page 718).
Detailed Status	<p>Displays a detailed description of the test call status:</p> <ul style="list-style-type: none"> ▪ "Idle": Test call is currently not active. ▪ "Scheduled - Established Calls: <number of established calls>, ASR: <ASR>%": Test call is planned to run (according to 'Schedule Interval' parameter settings) and also shows the following summary of completed test calls: <ul style="list-style-type: none"> ✓ 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: <ASR>%)": Test call has been started (i.e., the Dial command was clicked) and shows the following:

Statistics Field	Description
	<ul style="list-style-type: none"> ✓ Number of currently active test calls. ✓ Number of successfully answered calls out of the total number of calls attempted (Answer Success Ratio or ASR). ▪ "Receiving (<number of active calls>)": 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: <number of established calls>, ASR: <ASR>%": Test call has been successfully completed (or was prematurely stopped by clicking the Drop Call command) and shows the following: <ul style="list-style-type: none"> ✓ Total number of test calls that were established. ✓ Number of successfully answered calls out of the total number of calls attempted (ASR).
MOS Status	MOS count and color threshold status of local and remote sides according to the assigned QoE Profile.
Delay Status	Packet delay count and color-threshold status of local and remote sides according to the assigned QoE Profile.
Jitter Status	Jitter count and color-threshold status of local and remote sides according to the assigned QoE Profile.
Packet Loss Status	Packet loss count and color-threshold status of local and remote sides according to the assigned QoE Profile.
Bandwidth Status	Tx/Rx bandwidth and color-threshold status according to the assigned Bandwidth Profile.

52.5 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 test call in the Test Call Rules table by configuring the 'Play' parameter to **DTMF** (see "Configuring Test Call Endpoints" on page 713). If enabled, the default DTMF signal that is played is "3212333". You can change this as described below.



Note:

- You can configure the DTMF signaling type (e.g., out-of-band or in-band) using the 'DTMF Transport Type' parameter. For more information, see Configuring DTMF Transport Types.
- To generate DTMF tones, the device's DSP resources are required.
- Instead of playing DTMF tones, the device can play a non-DTMF tone from a PRT file (Dial Tone #2). To enable this, you must configure 'Play' to **PRT** in the Test Call Rules table and load a PRT file to the device (see "Prerecorded Tones File" on page 590).

➤ **To configure played DTMF signal to answered test call:**

1. Open the Test Call Settings page (**Troubleshooting** tab > **Troubleshooting** menu > **Test Call** folder > **Test Call Settings**).
2. In the 'Test Call DTMF String' field, enter the DTMF string (up to 15 digits):

Figure 52-3: Configuring Played DTMF Tone for Test Calls

Test Call DTMF String

3. Click **Apply**.

52.6 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.



Note:

- The SBC Test Call feature is initiated only upon receipt of incoming calls and with the configured prefix.
- This call test is done on all SIP interfaces.

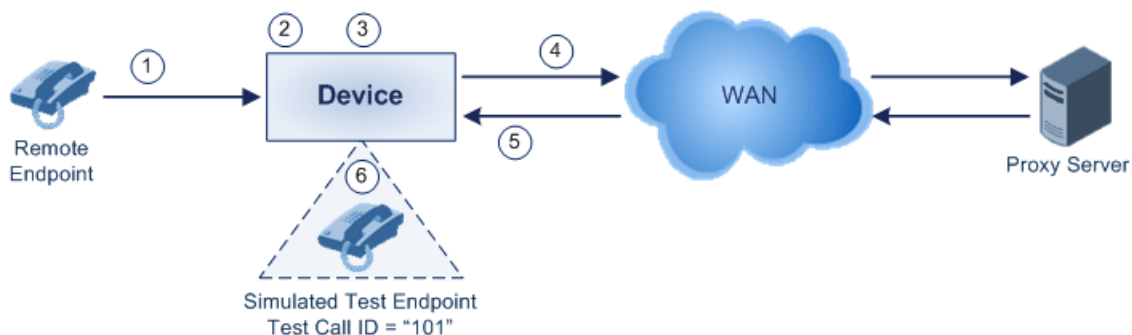
As this test call type involves an SBC call, you need to configure regular SBC rules such as classification and IP-to-IP routing. Therefore, this test call also allows you to verify correct SBC configuration.

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 52-4: 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 (for a full description, see "SIP Test Call Parameters" on page 757):
 - a. Open the Test Call Settings page (**Troubleshooting** tab > **Troubleshooting** menu > **Test Call** folder > **Test Call Settings**).

Figure 52-5: Configuring SBC Test Call with Proxy

GENERAL	
Test Call ID	<input type="text"/>
SBC Test ID	<input type="text"/>

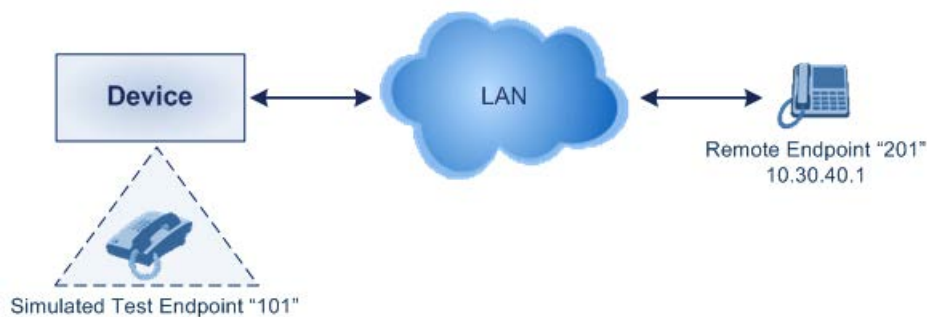
- b. In the 'Test Call ID' field, enter a prefix number for the simulated test endpoint on the device.
 - c. In the 'SBC Test ID' field, enter a called prefix number for identifying the call as an SBC test call.
 - d. Click **Apply**.
2. Configure regular SBC call processing rules for called number prefix "101", such as classification and IP-to-IP routing through a proxy server.

52.7 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.

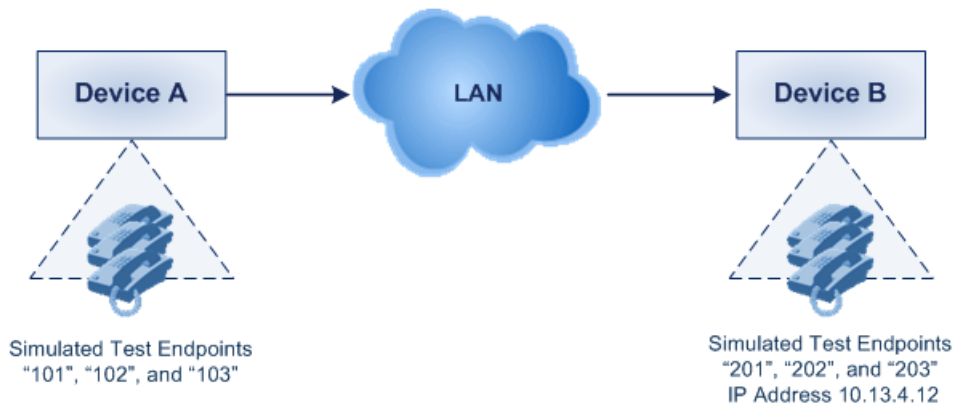
Figure 52-6: Single Test Call Example



- Test Call Rules table configuration:
 - ◆ Endpoint URI: "101"
 - ◆ Called URI: "201"

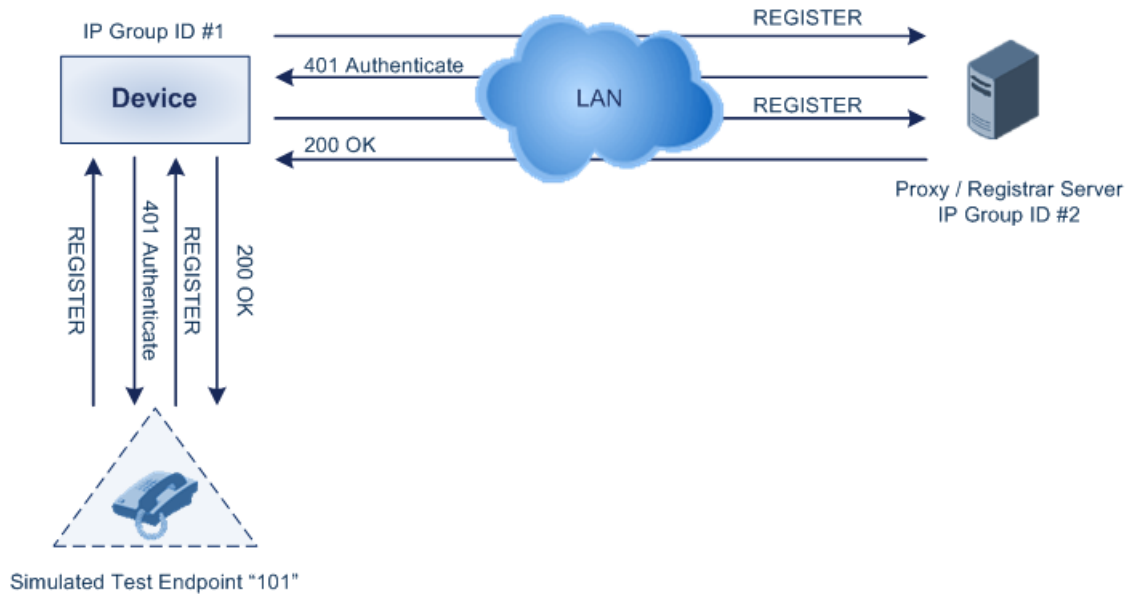
- ◆ Route By: **Dest Address**
 - ◆ Destination Address: "10.30.40.01"
 - ◆ SIP Interface: SIPInterface_0
 - ◆ Call Party: **Caller**
 - ◆ Test Mode: **Once**
- **Batch Test Call Scenario:** This example describes the configuration of a batch test call setup for scheduled and continuous call testing 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 52-7: Batch Test Call Example



- Test Call Rules table configuration at Device A:
 - ◆ Endpoint URI: "101"
 - ◆ Called URI: "201"
 - ◆ Route By: **Dest Address**
 - ◆ Destination Address: "10.13.4.12"
 - ◆ SIP Interface: SIPInterface_0
 - ◆ Call Party: **Caller**
 - ◆ Maximum Channels for Session: "3" (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 Rules table configuration at Device B:
 - ◆ Endpoint URI: "201"
 - ◆ Maximum Channels for Session: "3" (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 52-8: 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 Rules 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)
 - ◆ SIP Interface: SIPInterface_0
 - ◆ Auto Register: **Enable**
 - ◆ User Name: "testuser"
 - ◆ Password: "12345"
 - ◆ Call Party: **Caller**

53 Pinging a Remote Host or IP Address

You can verify the network connectivity with a remote host or IP address by pinging the network entity.

- IPv4: The ping to an IPv4 address can be done from any of the device's VoIP interfaces that is configured with an IPv4 address. The ping is done using the following CLI command:

```
# ping <IPv4 ip address or host name> source [voip] interface
```

For a complete description of the ping command, refer to the *CLI Reference Guide*.

This page is intentionally left blank.

Part XI

Appendix

54 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.



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.

Table 54-1: Dialing Plan Notations for Prefixes and Suffixes

Notation	Description
x (letter "x")	Wildcard that denotes any single digit or character.
# (pound symbol)	<ul style="list-style-type: none"> When used at the end of a prefix, it denotes the end of a number. For example, 54324# represents a 5-digit number that starts with the digits 54324. When used anywhere else in the number (not at the end), it is part of the number (pound key). For example, 3#45 represents the prefix number 3#45. To denote the pound key when it appears at the end of the number, the pound key must be enclosed in square brackets. For example, 134[#] represents any number that starts with 134#.
* (asterisk symbol)	<ul style="list-style-type: none"> When used on its own, it denotes any number or string. When used as part of a number, it denotes the asterisk key. For example, *345 represents a number that starts with *345.
\$ (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"> Source and Destination Phone Prefix Source and Destination Username Source and Destination Calling Name Prefix
<p>Range of Digits</p> <p>Note:</p> <ul style="list-style-type: none"> Dial plans denoting a prefix that is a range must be enclosed in square brackets, e.g., [4-8] or 23xx[456]. Dial plans denoting a prefix that is not a range is not enclosed, e.g., 12345#. Dial plans denoting a suffix must be enclosed in parenthesis, e.g., (4) and (4-8). Dial plans denoting a suffix that include multiple ranges, the range must be enclosed in square brackets, e.g., (23xx[4,5,6]). 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: [4-8](23[4,5,6]). 	
[n-m] or (n-m)	<p>Represents a range of numbers.</p> <p>Examples:</p> <ul style="list-style-type: none"> To depict prefix numbers from 5551200 to 5551300:

Notation	Description						
	<ul style="list-style-type: none"> ✓ [5551200-5551300]# ▪ To depict prefix numbers from 123100 to 123200: ✓ 123[100-200]# ▪ To depict prefix and suffix numbers together: <ul style="list-style-type: none"> ✓ 03(100): for any number that starts with 03 and ends with 100. ✓ [100-199](100,101,105): for a number that starts with 100 to 199 and ends with 100, 101 or 105. ✓ 03(abc): for any number that starts with 03 and ends with abc. ✓ 03(5xx): for any number that starts with 03 and ends with 5xx. ✓ 03(400,401,405): for any number that starts with 03 and ends with 400 or 401 or 405. <p>Note:</p> <ul style="list-style-type: none"> ▪ The value <i>n</i> must be less than the value <i>m</i>. ▪ Only numerical ranges are supported (not alphabetical letters). ▪ For suffix ranges, the starting (<i>n</i>) and ending (<i>m</i>) numbers in the range must include the same number of digits. For example, (23-34) is correct, but (3-12) is not. 						
[n,m,...] or (n,m,...)	<p>Represents multiple numbers. The value can include digits or characters. Examples:</p> <ul style="list-style-type: none"> ▪ To depict a one-digit number starting with 2, 3, 4, 5, or 6: [2,3,4,5,6] ▪ To depict a one-digit number ending with 7, 8, or 9: (7,8,9) ▪ Prefix with Suffix: [2,3,4,5,6](7,8,9) - prefix is denoted in square brackets; suffix in parenthesis <p>For prefix only, the notations <i>d[n,m]e</i> and <i>d[n-m]e</i> can also be used:</p> <ul style="list-style-type: none"> ▪ To depict a five-digit number that starts with 11, 22, or 33: [11,22,33]xxx# ▪ To depict a six-digit number that starts with 111 or 222: [111,222]xxx# 						
[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"> ▪ Prefix: [123-130,455,766,780-790] ▪ Suffix: (123-130,455,766,780-790) <p>Note: 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>						
Special ASCII Characters	<p>The device does not support the use of ASCII characters in manipulation rules and therefore, for LDAP-based queries, the device can use the hexadecimal (HEX) format of the ASCII characters for phone numbers instead. The HEX value must be preceded by a backslash "\". For example, you can configure a manipulation rule that changes the received number +49 (7303) 165-xxxxx to +49 \287303\29 165-xxxxx, where \28 is the ASCII HEX value for "(" and \29 is the ASCII HEX value for ")". The manipulation rule in this example would denote the parenthesis in the destination number prefix using "x" wildcards (e.g., xx165xxxxx#); the prefix to add to the number would include the HEX values (e.g., +49 \287303\29 165-).</p> <p>Below is a list of common ASCII characters and their corresponding HEX values:</p> <table border="0" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="text-align: left;">ASCII Character</th> <th style="text-align: left;">HEX Value</th> </tr> </thead> <tbody> <tr> <td style="padding-left: 20px;">*</td> <td style="padding-left: 20px;">\2a</td> </tr> <tr> <td style="padding-left: 20px;">(</td> <td style="padding-left: 20px;">\28</td> </tr> </tbody> </table>	ASCII Character	HEX Value	*	\2a	(\28
ASCII Character	HEX Value						
*	\2a						
(\28						

Notation	Description
)
	\
	/

This page is intentionally left blank.

55 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.

55.1 Management Parameters

This section describes the device's management-related parameters.

55.1.1 General Parameters

The general management parameters are described in the table below.

Table 55-1: General Management Parameters

Parameter	Description
[WebLoginBlockAutoComplete]	<p>Disables autocompletion when entering the management login username in the 'Username' field of the device's Web interface. Disabling autocompletion may be useful for security purposes by hiding previously entered usernames and thereby, preventing unauthorized access to the device's management interface.</p> <ul style="list-style-type: none"> [0] Disable = (Default) Autocompletion is enabled and the 'Username' field automatically offers previously logged in usernames. [1] Enable = Autocompletion is disabled.
[EnforcePasswordComplexity]	<p>Enables the enforcement of management login-password complexity requirements to ensure strong passwords.</p> <ul style="list-style-type: none"> [0] Disable (default) [1] Enable <p>For more information on password complexity requirements, see the 'Password' parameter in Configuring Management User Accounts on page 60.</p>
Access List Table <pre>configure network > access-list</pre> [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 the parameter, see "Configuring Web and Telnet Access List" on page 69.</p>
Product Key	Defines the device's Product Key.

Parameter	Description
configure system > product-key [ProductKey]	The valid value is a string of up to 40 characters.

55.1.2 Web Parameters

The Web parameters are described in the table below.

Table 55-2: Web Parameters

Parameter	Description
Enable web access from all interfaces web-access-from-all-interfaces [EnableWebAccessFromAllInterfaces]	<p>Enables Web access from any of the device's IP network interfaces. The feature applies to HTTP and HTTPS protocols.</p> <ul style="list-style-type: none"> ▪ [0] = (Default) Disable – Web access is only through the OAMP interface. ▪ [1] = Enable - Web access is through any network interface.
Password Change Interval [WebUserPassChangeInterval]	<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>Note: The parameter is applicable only when using the Local Users table, where the default value of the 'Password Age' parameter in the Local Users table inherits the parameter's value.</p>
User Inactivity Timer [UserInactivityTimer]	<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 Security Administrator or Master user.</p> <p>The valid value is 0 to 10000, where 0 means inactive. The default is 90.</p> <p>Note: The parameter is applicable only when using the Local Users table.</p>
Session Timeout [WebSessionTimeout]	<p>Defines the duration (in minutes) of inactivity of a logged-in user in the Web interface, after which the user is automatically logged off the Web session. In other words, the session expires when the user has not performed any operations (activities) in the Web interface for the configured duration.</p> <p>The valid value is 0-100000, where 0 means no timeout. The default is 15.</p> <p>Note: You can also configure the functionality per user in the Local Users table (see "Configuring Management User Accounts" on page 60), which overrides this global setting.</p>

Parameter	Description
Deny Access On Fail Count [DenyAccessOnFailCount]	<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>
Deny Authentication Timer [DenyAuthenticationTimer]	<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>
Display Last Login Information [DisplayLoginInformation]	<p>Enables display of user's login information on each successful login attempt.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable
[EnableMgmtTwoFactorAuthentication]	<p>Enables Web login authentication using a third-party, smart card.</p> <ul style="list-style-type: none"> ▪ [0] = Disable (default) ▪ [1] = Enable <p>When enabled, the device retrieves the Web user's login username from the smart card, which is automatically displayed (read-only) in 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>
http-port [HTTPport]	<p>Defines the LAN HTTP port for Web management. To enable Web management from the LAN, configure the desired port.</p> <p>The default is 80.</p> <p>Note: For the 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"> ▪ [0] = (Default) Enables modifications of parameters. ▪ [1] = Web interface is read-only. <p>When in read-only mode, parameters can't be modified and the following pages can't be accessed: Web User Accounts, TLS Contexts, Time and Date, Maintenance Actions, Load Auxiliary Files, Software Upgrade Wizard, and Configuration File.</p> <p>Note: For the parameter to take effect, a device reset is required.</p>

Parameter	Description
[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"> ▪ [0] = (Default) Password and username retain their values. ▪ [1] = Password and username are reset. <p>Note:</p> <ul style="list-style-type: none"> ▪ For the parameter to take effect, a device reset is required. ▪ 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: <ul style="list-style-type: none"> ✓ SNMP: <ol style="list-style-type: none"> 1) Set acSysGenericINILine to WEBPasswordControlViaSNMP = 1, and reset the device with a flash burn (set acSysActionSetResetControl to 1 and acSysActionSetReset to 1). 2) Change the username and password in the acSysWEBAccessEntry table. Use the following format: <ul style="list-style-type: none"> Username acSysWEBAccessUserName: old/pass/new Password acSysWEBAccessUserCode: username/old/new
[WelcomeMessage]	<p>Enables and defines a Welcome message that appears on the Web Login page for logging in to the Web interface. The format of the ini file table parameter is:</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>Note:</p> <ul style="list-style-type: none"> ▪ Each index row represents a line of text in the Welcome message box. Up to 20 lines (or rows) of text can be defined. ▪ The configured text message must be enclosed in double quotation marks (i.e., "..."). ▪ If the parameter is not configured, no Welcome message is displayed.

55.1.3 Telnet Parameters

The Telnet parameters are described in the table below.

Table 55-3: Telnet Parameters

Parameter	Description
Embedded Telnet Server configure system > cli- settings > telnet [TelnetServerEnable]	Enables the device's embedded Telnet server. Telnet is disabled by default for security. <ul style="list-style-type: none"> [0] Disable [1] Enable Unsecured (default) [2] Enable Secured Note: Only the primary Web User Account (which has Security Administration access level) can access the device using Telnet (see "Configuring Management User Accounts" on page 60).
Telnet Server TCP Port configure system > cli- settings > telnet-port [TelnetServerPort]	Defines the port number for the embedded Telnet server. The valid range is all valid port numbers. The default port is 23.
Telnet Server Idle Timeout configure system > cli- settings > idle-timeout [TelnetServerIdleDisconnect]	Defines the timeout (in minutes) for disconnection of an idle Telnet session. When set to zero, idle sessions are not disconnected. The valid range is any value. The default is 0. Note: For the parameter to take effect, a device reset is required.
Maximum Telnet Sessions configure system > cli- settings > telnet-max- sessions [TelnetMaxSessions]	Defines the maximum number of permitted, concurrent Telnet/SSH sessions. The valid range is 1 to 5 sessions. The default is 2. Note: Before changing the value, make sure that not more than this number of sessions are currently active; otherwise, the new setting will not take effect.
[CLIPrivPass]	Defines the password to access the Enable configuration mode in the CLI. The valid value is a string of up to 50 characters. The default is "Admin". Note: The password is case-sensitive.

55.1.4 ini File Parameters

The parameters relating to ini-file management are described in the table below.

Table 55-4: ini File Parameters

Parameter	Description
[INIPasswordsDisplayType]	Defines how passwords are displayed in the ini file. <ul style="list-style-type: none"> [0] = (default) Disable. Passwords are obscured ("encoded"). The passwords are displayed in the following syntax: \$1\$<obscured password> (e.g., \$1\$S3p+fno=). [1] = Enable. All passwords are hidden and replaced by an asterisk (*).

55.1.5 SNMP Parameters

The SNMP parameters are described in the table below.

Table 55-5: SNMP Parameters

Parameter	Description
Disable SNMP configure system > snmp settings > disable [DisableSNMP]	Enables SNMP. <ul style="list-style-type: none"> ▪ [0] No (default) ▪ [1] Yes = SNMP is disabled and no traps are sent.
configure system > snmp settings > port [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. Note: For the parameter to take effect, a device reset is required.
[ChassisPhysicalAlias]	Defines the 'alias' name object for the physical entity as specified by a network manager, and provides a non-volatile 'handle' for the physical entity. The valid range is a string of up to 255 characters.
[ChassisPhysicalAssetID]	Defines the user-assigned asset tracking identifier object for the device's chassis as specified by an EMS, and provides non-volatile storage of this information. The valid range is a string of up to 255 characters.
[ifAlias]	Defines the textual name of the interface. The value is equal to the ifAlias SNMP MIB object. The valid range is a string of up to 64 characters.
configure system > snmp trap > auto-send-keep-alive [SendKeepAliveTrap]	Enables the device to send NAT keep-alive traps to the port of the SNMP network management station (e.g., AudioCodes EMS). This is used for NAT traversal, and allows SNMP communication with AudioCodes EMS management platform, located in the WAN, when the device is located behind NAT. It is needed to keep the NAT pinhole open for the SNMP messages sent from EMS to the device. The device sends the trap periodically - every 9/10 of the time configured by the NATBindingDefaultTimeout parameter. The trap that is sent is acKeepAlive. For more information on the SNMP trap, refer to the <i>SNMP Reference Guide</i> . <ul style="list-style-type: none"> ▪ [0] = (Default) Disable ▪ [1] = Enable To configure the port number, use the KeepAliveTrapPort parameter. Note: For the parameter to take effect, a device reset is required.
[KeepAliveTrapPort]	Defines the port of the SNMP network management station to which the device sends keep-alive traps. The valid range is 0 - 65534. The default is port 162. To enable NAT keep-alive traps, use the SendKeepAliveTrap parameter.

Parameter	Description
[PM_EnableThresholdAlarms]	Enables the sending of the SNMP trap event, acPerformanceMonitoringThresholdCrossing which is sent every time the threshold (high and low) of a Performance Monitored object (e.g., acPMMediaRealmAttributesMediaRealmBytesTxHighThreshold) is crossed. <ul style="list-style-type: none"> [0] = (Default) Disable [1] = Enable
configure system > snmp settings > sys-oid [SNMPSysOid]	Defines the base product system OID. The default is eSNMP_AC_PRODUCT_BASE_OID_D. Note: For the 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 the parameter. Note: For the 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. The 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 500. Note: For the parameter to take effect, a device reset is required.
configure system > snmp settings > engine-id [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 (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 Note: <ul style="list-style-type: none"> For the parameter to take effect, a device reset is required. Before setting the parameter, all SNMPv3 users must be deleted; otherwise, the parameter setting is ignored. 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.
SNMP Trap Destination Parameters (configure system > snmp trap destination)	
Note: Up to five SNMP trap managers can be defined.	
SNMP Manager [SNMPManagerIsUsed_x]	Determines the validity of the parameters (IP address and port number) of the corresponding SNMP Manager used to receive SNMP traps.

Parameter	Description
	<ul style="list-style-type: none"> ▪ [0] (Check box cleared) = Disabled (default) ▪ [1] (Check box selected) = Enabled
IP Address ip-address [SNMPManagerTableIP_x]	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.
Trap Port port [SNMPManagerTrapPort_x]	Defines the port number of the remote SNMP Manager. The device sends SNMP traps to this port. The valid SNMP trap port range is 100 to 4000. The default port is 162.
Trap Enable send-trap [SNMPManagerTrapSendingEnable_x]	Enables the sending of traps to the corresponding SNMP manager. <ul style="list-style-type: none"> ▪ [0] Disable = Sending is disabled. ▪ [1] Enable = (Default) Sending is enabled.
Trap User trap-user [SNMPManagerTrapUser_x]	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). The valid value is a string.
Trap Manager Host Name manager-host-name [SNMPTrapManagerHostName]	Defines an FQDN of the remote host used as an SNMP manager to receive traps sent by the device. The device sends the traps to the DNS-resolved IP address. The valid range is a string of up to 99 characters. For more information, see "Configuring an SNMP Trap Destination with FQDN" on page 87.
Activity Trap configure troubleshoot > activity-trap [EnableActivityTrap]	Enables the device to send an SNMP trap to notify of Web user activities in the Web interface. The activities to report are configured by the ActivityListToLog parameter. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable
SNMP Community String Parameters	
Read Only Community Strings configure system > snmp settings > ro-community-string [SNMPReadOnlyCommunityString_x]	Defines a read-only SNMP community string. Up to five read-only community strings can be configured. The valid value is a string of up to 19 characters that can include only the following: <ul style="list-style-type: none"> ▪ Upper- and lower-case letters (a to z, and A to Z) ▪ Numbers (0 to 9) ▪ Hyphen (-) ▪ Underline (_) For example, "Public-comm_string1". The default is "public".
Read/Write Community Strings configure system > snmp settings > rw-community-string [SNMPReadWriteCommunityString_x]	Defines a read-write SNMP community string. Up to five read-write community strings can be configured. The valid value is a string of up to 19 characters that can include only the following: <ul style="list-style-type: none"> ▪ Upper- and lower-case letters (a to z, and A to Z)

Parameter	Description
	<ul style="list-style-type: none"> ▪ Numbers (0 to 9) ▪ Hyphen (-) ▪ Underline (_) For example, "Private-comm_string1". The default is "private".
Trap Community String configure system > snmp trap > community-string [SNMPTrapCommunityString]	Defines the community string for SNMP traps. The valid value is a string of up to 19 characters that can include only the following: <ul style="list-style-type: none"> ▪ Upper- and lower-case letters (a to z, and A to Z) ▪ Numbers (0 to 9) ▪ Hyphen (-) ▪ Underline (_) For example, "Trap-comm_string1". The default is "trapuser".
SNMP Trusted Managers Table	
SNMP Trusted Managers configure system > snmp settings > trusted-managers [SNMPTrustedMgr_x]	The table defines up to five IP addresses of remote trusted SNMP managers from which the SNMP agent accepts and processes SNMP Get and Set requests. For a description of the table, see "Configuring SNMP Trusted Managers" on page 87.
SNMP V3 Users Table	
SNMP V3 Users configure system > snmp v3-users [SNMPUsers]	The table defines SNMP v3 users. The format of the ini file table parameter is: [SNMPUsers] FORMAT SNMPUsers_Index = SNMPUsers_Username, SNMPUsers_AuthProtocol, SNMPUsers_PrivProtocol, SNMPUsers_AuthKey, SNMPUsers_PrivKey, SNMPUsers_Group; [SNMPUsers] 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. For a description of the table, see "Configuring SNMP V3 Users" on page 88.

55.1.6 Serial Parameters

The serial interface parameters are described in the table below.

Table 55-6: Serial Parameters

Parameter	Description
[DisableRS232]	Enables the device's RS-232 (serial) port. <ul style="list-style-type: none"> ▪ [0] = Enabled ▪ [1] = (Default) Disabled The RS-232 serial port can be used to change the networking parameters and view error/notification messages. To establish serial communication with the device, see "Establishing a CLI Session" on page 79. Note: For the parameter to take effect, a device reset is required.
[SerialBaudRate]	Defines the serial communication baud rate. <p>The valid values include the following: 1200, 2400, 9600, 14400, 19200, 38400, 57600, or 115200 (default).</p> Note: For the parameter to take effect, a device reset is required.
[SerialData]	Defines the serial communication data bit. <ul style="list-style-type: none"> ▪ [7] = 7-bit ▪ [8] = (Default) 8-bit Note: For the parameter to take effect, a device reset is required.
[SerialParity]	Defines the serial communication polarity. <ul style="list-style-type: none"> ▪ [0] = (Default) None ▪ [1] = Odd ▪ [2] = Even Note: For the parameter to take effect, a device reset is required.
[SerialStop]	Defines the serial communication stop bit. <ul style="list-style-type: none"> ▪ [1] = (Default) 1-bit (default) ▪ [2] = 2-bit Note: For the parameter to take effect, a device reset is required.
[SerialFlowControl]	Defines the serial communication flow control. <ul style="list-style-type: none"> ▪ [0] = (Default) None ▪ [1] = Hardware Note: For the parameter to take effect, a device reset is required.

55.1.7 Auxiliary and Configuration File Name Parameters

The table below lists the *ini* file parameters associated with the Auxiliary files. For more information on Auxiliary files, see "Loading Auxiliary Files" on page 585.

Table 55-7: Auxiliary and Configuration File Parameters

Parameter	Description
General Parameters	
[SetDefaultOnIniFileProcess]	Determines if all the device's parameters are set to their defaults before processing the updated <i>ini</i> file. <ul style="list-style-type: none"> ▪ [0] = Disable - parameters not included in the downloaded ini file are not returned to default settings (i.e., retain their current settings).

Parameter	Description
	<ul style="list-style-type: none"> [1] = Enable (default). <p>Note: The 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>
[SaveConfiguration]	<p>Determines if the device's configuration (parameters and files) is saved to flash (non-volatile memory).</p> <ul style="list-style-type: none"> [0] = Configuration isn't saved to flash memory. [1] = (Default) Configuration is saved to flash memory.
Auxiliary and Configuration File Name Parameters	
Call Progress Tones File [CallProgressTonesFilename]	<p>Defines the name of the file containing the Call Progress Tones definitions.</p> <p>For the ini file, the name must be enclosed by single apostrophes, for example, 'cpt_us.dat'.</p> <p>For more information on how to create and load this file, refer to <i>DConvert Utility User's Guide</i>.</p> <p>Note: For the parameter to take effect, a device reset is required.</p>
Prerecorded Tones File [PrerecordedTonesFileName]	<p>Defines the name of the file containing the Prerecorded Tones.</p> <p>Note: For the parameter to take effect, a device reset is required.</p>
Dial Plan File [DialPlanFileName]	<p>Defines the name of the Dial Plan file. This file should be created using AudioCodes DConvert utility (refer to <i>DConvert Utility User's Guide</i>).</p> <p>For the ini file, the name must be enclosed by single apostrophes, for example, 'dial_plan.dat'.</p>
[UserInfoFileName]	<p>Defines the name of the file containing the User Information data.</p> <p>For the ini file, the name must be enclosed by single apostrophes, for example, 'userinfo_us.dat'.</p>

55.1.8 Automatic Update Parameters

The automatic update of software and configuration files parameters are described in the table below.

Table 55-8: Automatic Update of Software and Configuration Files Parameters

Parameter	Description
General Automatic Update Parameters	
CLI path: configure system > automatic-update	
update-firmware [AutoUpdateCmpFile]	<p>Enables the Automatic Update mechanism for the cmp file.</p> <ul style="list-style-type: none"> [0] = (Default) The Automatic Update mechanism doesn't apply to the cmp file. [1] = The Automatic Update mechanism includes the cmp file. <p>Note: For the parameter to take effect, a device reset is required.</p>
update-frequency [AutoUpdateFrequency]	<p>Defines the interval (in minutes) that the device waits between consecutive automatic updates.</p> <p>The default is 0 (i.e., the update at fixed intervals mechanism is disabled).</p>

Parameter	Description
predefined-time [AutoUpdatePredefinedTime]	<p>Note: For the parameter to take effect, a device reset is required.</p> <p>Defines schedules (time of day) for performing automatic updates. The format syntax of the parameter is 'hh:mm', where <i>hh</i> denotes the hour and <i>mm</i> the minutes. The value must be enclosed in single apostrophes. For example, '20:18'.</p> <p>Note:</p> <ul style="list-style-type: none"> For the parameter to take effect, a device reset is required. The actual update time is randomized by five minutes to reduce the load on the Web servers.
http-user-agent [AupdHttpUserAgent]	<p>Defines the information sent in the HTTP User-Agent header in the HTTP Get requests sent by the device to the provisioning server for the Automatic Update mechanism.</p> <p>The valid value is a string of up to 511 characters. The information can include any user-defined string or the following string variable tags (case-sensitive):</p> <ul style="list-style-type: none"> <NAME>: product name, according to the installed License Key <MAC>: device's MAC address <VER>: software version currently installed on the device, e.g., "7.00.200.001" <CONF>: configuration version, as configured by the ini file parameter, INIFileVersion or CLI command, configuration-version <p>The device automatically populates these tag variables with actual values in the sent header. By default, the device sends the following in the User-Agent header:</p> <pre>User-Agent: Mozilla/4.0 (compatible; AudioCodes; <NAME>;<VER>;<MAC>;<CONF>)</pre> <p>For example, if you set AupdHttpUserAgent = MyWorld-<NAME>;<VER>(<MAC>), the device sends the following User-Agent header:</p> <pre>User-Agent: MyWorld- Mediant;7.00.200.001(00908F1DD0D3)</pre> <p>Note:</p> <ul style="list-style-type: none"> The variable tags are case-sensitive. If you configure the parameter with the <CONF> variable tag, you must reset the device with a save-to-flash for your settings to take effect. The tags can be defined in any order. The tags must be defined adjacent to one another (i.e., no spaces).
auto-firmware [AutoCmpFileUrl]	<p>Defines the filename and path (URL) to the provisioning server from where the software file (.cmp) can be downloaded, based on timestamp for the Automatic Updated mechanism.</p> <p>The valid value is an IP address in dotted-decimal notation or an FQDN.</p>
aupd-verify-cert [AUPDVerifyCertificates]	<p>Determines whether the Automatic Update mechanism verifies the TLS certificate received from the provisioning server when the connection is HTTPS.</p> <ul style="list-style-type: none"> [0] = Disable (default) [1] = Enables TLS certificate verification when the connection with the provisioning server is based on HTTPS. The device verifies the

Parameter	Description
	<p>authentication of the certificate received from the provisioning server. The device authenticates the certificate against its trusted root certificate store (see "Configuring SSL/TLS Certificates" on page 99) and if ok, allows communication with the provisioning server. If authentication fails, the device denies communication (i.e., handshake fails).</p>
[AUPDDigestUsername]	<p>Defines the username for digest (MD5 cryptographic hashing) access authentication with the HTTP server used for the Automatic Update feature.</p> <p>The valid value is a string of up to 50 characters. By default, no value is defined.</p>
[AUPDDigestPassword]	<p>Defines the password for digest (MD5 cryptographic hashing) access authentication with the HTTP server used for the Automatic Update feature.</p> <p>The valid value is a string of up to 50 characters. By default, no value is defined.</p>
<p>crc-check regular [AUPDCheckIfIniChanged]</p>	<p>Enables the device to perform cyclic redundancy checks (CRC) on downloaded configuration files during the Automatic Update process. The CRC checks whether the content (raw data) of the downloaded file is different to the content of the previously downloaded file from the previous Automatic Update process. The device compares the CRC check value (code) result with the check value of the previously downloaded file. If the check values are identical, it indicates that the file has no new configuration settings, and the device discards the file. If the check values are different, the device installs the downloaded file and applies the new configuration settings.</p> <ul style="list-style-type: none"> ▪ [0] = (Default) Disable - the device does not perform CRC and installs the downloaded file regardless. ▪ [1] = Enable CRC for the entire file, including line order (i.e., same text must be on the same lines). If there are differences between the files, the device installs the downloaded file. If there are no differences, the device discards the newly downloaded file. ▪ [2] = Enable CRC for individual lines only. Same as option [1], except that the CRC ignores the order of lines (i.e., same text can be on different lines).
<p>tftp-block-size [AUPDTftpBlockSize]</p>	<p>Defines the size of the TFTP data blocks (packets) when downloading a file from a TFTP server for the Automatic Update mechanism. This is in accordance to RFC 2348. TFTP block size is the physical packet size (in bytes) that a network can transmit. When configured to a value higher than the default (512 bytes), but lower than the client network's Maximum Transmission Unit (MTU), the file download speed can be significantly increased.</p> <p>The valid value is 512 to 8192. The default is 512.</p> <p>Note:</p> <ul style="list-style-type: none"> ▪ A higher value does not necessarily mean better performance. ▪ The block size should be small enough to avoid IP fragmentation in the client network (i.e., below MTU). ▪ This feature is applicable only to TFTP servers that support this option.
[ResetNow]	<p>Invokes an immediate device reset. This option can be used to</p>

Parameter	Description
	activate offline (i.e., not on-the-fly) parameters that are loaded using the parameter IniFileUrl. <ul style="list-style-type: none"> ▪ [0] = (Default) The immediate restart mechanism is disabled. ▪ [1] = The device immediately resets after an <i>ini</i> file with the parameter set to 1 is loaded. <p>Note: If you use the parameter in an ini file for periodic automatic provisioning with non-HTTP (e.g., TFTP) and without CRC, the device resets upon every file download.</p>
<p>Software/Configuration File URL Path for Automatic Update Parameters CLI path: configure system > automatic-update</p>	
firmware [CmpFileURL]	Defines the name of the <i>cmp</i> file and the URL address (IP address or FQDN) of the server on which the file is located. For example: http://192.168.0.1/filename <p>Note:</p> <ul style="list-style-type: none"> ▪ For the parameter to take effect, a device reset is required. ▪ When the parameter is configured, the device always loads the <i>cmp</i> file after it is reset. ▪ 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. ▪ The maximum length of the URL address is 255 characters.
voice-configuration [IniFileURL]	Defines the name of the <i>ini</i> file and the URL address (IP address or FQDN) of the server on which the file is located. For example: http://192.168.0.1/filename http://192.8.77.13/config_<MAC>.ini https://<username>:<password>@<IP address>/<file name> <p>Note:</p> <ul style="list-style-type: none"> ▪ For the parameter to take effect, a device reset is required. ▪ 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. ▪ The case-sensitive string, "<MAC>" can be used in the file name for instructing the device to replace it with the device's MAC address. For more information, see "MAC Address Placeholder in Configuration File Name" on page 619. This option allows the loading of specific configurations for specific devices. ▪ The maximum length of the URL address is 99 characters.
cli-script <URL> [AUPDCliScriptURL]	Defines the URL of the server where the CLI Script file containing the device's configuration is located. This file is used for automatic provisioning. <p>Note: The case-sensitive string, "<MAC>" can be used in the file name for instructing the device to replace it with the device's MAC address. For more information, see MAC Address Placeholder in Configuration File Name on page 619.</p>
prerecorded-tones [PrtFileURL]	Defines the name of the Prerecorded Tones (PRT) file and the URL address (IP address or FQDN) of the server on which the file is located. For example: http://server_name/file, https://server_name/file <p>Note: The maximum length of the URL address is 99 characters.</p>

Parameter	Description
call-progress-tones [CptFileURL]	Defines the name of the CPT file and the URL address (IP address or FQDN) of the server on which the file is located. For example: http://server_name/file, https://server_name/file Note: The maximum length of the URL address is 99 characters.
tls-root-cert [TLSPRootFileUrl]	Defines the name of the TLS trusted root certificate file and the URL address of the server on which the file is located. Note: For the parameter to take effect, a device reset is required.
tls-cert [TLSCertFileUrl]	Defines the name of the TLS certificate file and the URL address of the server on which the file is located. Note: For the parameter to take effect, a device reset is required.
tls-private-key [TLSPkeyFileUrl]	Defines the URL address of the server on which the TLS private key file is located.
[UserInfoFileURL]	Defines the name of the User Information file and the URL address (IP address or FQDN) of the server on which the file is located. For example: http://server_name/file, https://server_name/file Note: The maximum length of the URL address is 99 characters.
feature-key [FeatureKeyURL]	Defines the name of the License Key file and the URL address of the server on which the file is located.
template-url [TemplateUrl]	Defines the URL address in the File Template for automatic updates, of the provisioning server on which the files to download are located. For more information, see "File Template for Automatic Provisioning" on page 620.
template-files-list [AupdFilesList]	Defines the list of file types in the File Template for automatic updates, to download from the provisioning server. For more information, see "File Template for Automatic Provisioning" on page 620.

55.2 Networking Parameters

This subsection describes the device's networking parameters.

55.2.1 Ethernet Parameters

The Ethernet parameters are described in the table below.

Table 55-9: Ethernet Parameters

Parameter	Description
Physical Ports Table	
Physical Ports configure network > physical-port [PhysicalPortsTable]	The table configures the physical Ethernet ports. The format of the ini file table parameter is as follows: [PhysicalPortsTable] FORMAT PhysicalPortsTable_Index = PhysicalPortsTable_Port,

Parameter	Description
	PhysicalPortsTable_Mode, PhysicalPortsTable_SpeedDuplex, PhysicalPortsTable_PortDescription, PhysicalPortsTable_GroupMember, PhysicalPortsTable_GroupStatus; [\PhysicalPortsTable] For a detailed description of the table, see Configuring Physical Ethernet Ports on page 124.
Ethernet Groups Table	
Ethernet Groups configure network > ether-group [EtherGroupTable]	Defines the transmit (Tx) and receive (Rx) settings for the Ethernet port groups. The format of the ini file table parameter is: [EtherGroupTable] FORMAT EtherGroupTable_Index = EtherGroupTable_Group, EtherGroupTable_Mode, EtherGroupTable_Member1, EtherGroupTable_Member2; [\EtherGroupTable] For a detailed description of the table, see Configuring Ethernet Port Groups on page 126. Note: For the parameter to take effect, a device reset is required.
Ethernet Devices table	
Ethernet Devices table configure network > network-dev [DeviceTable]	Defines Ethernet Devices (VLANs). The format of the ini file table parameter is as follows: [DeviceTable] FORMAT DeviceTable_Index = DeviceTable_VlanID, DeviceTable_UnderlyingInterface, DeviceTable_DeviceName, DeviceTable_Tagging; [\DeviceTable] For a detailed description of the table, see Configuring Underlying Ethernet Devices on page 128.

55.2.2 Multiple VoIP Network Interfaces and VLAN Parameters

The IP network interfaces and VLAN parameters are described in the table below.

Table 55-10: IP Network Interfaces and VLAN Parameters

Parameter	Description
IP Interfaces Table	

Parameter	Description
IP Interfaces configure network > interface network-if [InterfaceTable]	The table configures IP network interfaces. The format of the ini file table parameter is as follows: [InterfaceTable] FORMAT InterfaceTable_Index = InterfaceTable_ApplicationTypes, InterfaceTable_InterfaceMode, InterfaceTable_IPAddress, InterfaceTable_PrefixLength, InterfaceTable_Gateway, InterfaceTable_VlanID, InterfaceTable_InterfaceName, InterfaceTable_PrimaryDNSServerIPAddress, InterfaceTable_SecondaryDNSServerIPAddress, InterfaceTable_UnderlyingDevice; [\InterfaceTable] For a detailed description of the table, see "Configuring IP Network Interfaces" on page 130.
VLAN Parameters	
[EnableNTPasOAM]	Defines the application type for Network Time Protocol (NTP) services. <ul style="list-style-type: none"> ▪ [1] = OAMP (default) ▪ [0] = Control Note: For the parameter to take effect, a device reset is required.

55.2.3 Routing Parameters

The IP network routing parameters are described in the table below.

Table 55-11: IP Network Routing Parameters

Parameter	Description
Send ICMP Unreachable Messages configure network > network-settings > icmp- disable-unreachable [DisableICMPUnreachable]	Enables sending of ICMP Unreachable messages. <ul style="list-style-type: none"> ▪ [0] Enable = (Default) Device sends these messages. ▪ [1] Disable = Device does not send these messages.
Send and Receive ICMP Redirect Messages configure network > network-settings > icmp- disable-redirect [DisableICMPRedirects]	Enables sending and receiving of ICMP Redirect messages. <ul style="list-style-type: none"> ▪ [0] Enable = (Default) Device sends and accepts these messages. ▪ [1] Disable = Device rejects these messages and also does not send them.
Static Routes Table	
Static Routes configure network > static [StaticRouteTable]	Defines up to 30 static IP routes for the device. The format of the ini file table parameter is as follows: [StaticRouteTable] FORMAT StaticRouteTable_Index = StaticRouteTable_DeviceName, StaticRouteTable_Destination, StaticRouteTable_PrefixLength, StaticRouteTable_Gateway, StaticRouteTable_Description; [\StaticRouteTable]

Parameter	Description
	For a description of the parameter, see "Configuring Static IP Routes" on page 138.

55.2.4 Quality of Service Parameters

The Quality of Service (QoS) parameters are described in the table below.

Table 55-12: QoS Parameters

Parameter	Description
Layer-2 Class Of Service (CoS) Parameters (VLAN Tag Priority Field)	
DiffServ Table configure network > qos vlan-mapping [DiffServToVlanPriority]	<p>The table 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.</p> <p>The format of this ini file is as follows:</p> <pre>[DiffServToVlanPriority] FORMAT DiffServToVlanPriority_Index = DiffServToVlanPriority_DiffServ, DiffServToVlanPriority_VlanPriority; [\DiffServToVlanPriority]</pre> <p>For example: DiffServToVlanPriority 0 = 46, 6; DiffServToVlanPriority 1 = 40, 6; DiffServToVlanPriority 2 = 26, 4; DiffServToVlanPriority 3 = 10, 2;</p> <p>For a description of the table, see Configuring Quality of Service on page 148.</p> <p>Note: For the parameter to take effect, a device reset is required.</p>
Layer-3 Class of Service (TOS/DiffServ) Parameters CLI path: configure network > qos application-mapping	
Media Premium QoS media-qos [PremiumServiceClassMediaDiffServ]	<p>Global parameter defining the DiffServ value for Premium Media CoS content.</p> <p>You can also configure this functionality per specific calls, using IP Profiles (IpProfile_IPDiffServ). For a detailed description of the parameter and To configure the functionality, see "Configuring IP Profiles" on page 388.</p> <p>Note: If the functionality is configured for a specific profile, the settings of this global parameter is ignored for calls associated with the profile.</p>
Control Premium QoS control-qos [PremiumServiceClassControlDiffServ]	<p>Global parameter defining the DiffServ value for Premium Control CoS content (Call Control applications).</p> <p>You can also configure the functionality per specific calls, using IP Profiles (IpProfile_SigIPDiffServ). For a detailed description of the parameter and To configure the functionality in the IP Profiles table, see "Configuring IP Profiles" on page 388 .</p> <p>Note: If the functionality is configured for a specific profile,</p>

Parameter	Description
	the settings of this global parameter is ignored for calls associated with the profile.
Gold QoS 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.
Bronze QoS 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.

55.2.5 NAT Parameters

The Network Address Translation (NAT) parameters are described in the table below.

Table 55-13: NAT Parameters

Parameter	Description
NAT Parameters	
NAT Traversal configure voip > media settings > disable-NAT- traversal [NATMode]	<p>Enables the NAT traversal feature for media when the device communicates with UAs located behind NAT.</p> <ul style="list-style-type: none"> ▪ [0] Enable NAT Option = NAT traversal is performed only if the UA is located behind NAT: <ul style="list-style-type: none"> ✓ UA behind NAT: The device sends the media packets to the IP address:port obtained from the source address of the first media packet received from the UA. ✓ UA not behind NAT: The device sends the packets to the IP address:port specified in the SDP 'c=' line (Connection) of the first received SIP message. <p>Note: If the SIP session is established (ACK) and the device (not the UA) sends the first packet, it sends it to the address obtained from the SIP message and only after the device receives the first packet from the UA does it determine whether the UA is behind NAT.</p> <ul style="list-style-type: none"> ▪ [1] Disable NAT = (Default) The device considers the UA as not located behind NAT and sends media packets to the UA using the IP address:port specified in the SDP 'c=' line (Connection) of the first received SIP message. ▪ [2] Force NAT = The device always considers the UA as behind NAT and sends the media packets to the IP address:port obtained from the source address of the first media packet received from the UA. The device only sends packets to the UA after it receives the first packet from the UA (to obtain the IP address). ▪ [3] NAT By Signaling = The device identifies whether or not the UA is located behind NAT based on the SIP signaling. The device assumes that if signaling is behind NAT that the media is also behind NAT, and vice versa. If located behind NAT, the device sends media as described in option [2] Force NAT; if not behind NAT, the device sends media as described in option [1] Disable NAT. This option is applicable only to SBC calls. If the parameter is configured to this option, Gateway calls use option [0] Enable NAT

Parameter	Description
	Option, by default. For more information on NAT traversal, see 'First Incoming Packet Mechanism' on page 145.
[NATBindingDefaultTimeout]	The device sends SNMP keep-alive traps periodically - every 9/10 of the time configured by the parameter (in seconds). Therefore, the parameter is applicable only if the SendKeepAliveTrap parameter is set to 1. The parameter is used to allow SNMP communication with AudioCodes EMS management platform, located in the WAN, when the device is located behind NAT. It is needed to keep the NAT pinhole open for the SNMP messages sent from EMS to the device. The valid range is 0 to 2,592,000. The default is 30. Note: For the parameter to take effect, a device reset is required.
SIP NAT Detection configure voip > sip- definition advanced-settings > sip-nat-detect [SIPNatDetection]	Enables the device to detect whether the incoming INVITE message is sent from an endpoint located behind NAT. <ul style="list-style-type: none"> ▪ [0] Disable = Disables the device's NAT Detection mechanism. Incoming SIP messages are processed as received from endpoints that are not located behind NAT and sent according to the SIP standard. ▪ [1] Enable (default) = Enables the device's NAT Detection mechanism.

55.2.6 DNS Parameters

The Domain name System (DNS) parameters are described in the table below.

Table 55-14: DNS Parameters

Parameter	Description
Internal DNS Table	
Internal DNS Table configure network > dns dns-to-ip [DNS2IP]	The table defines the internal DNS table for resolving host names into IP addresses. The format of the ini file table parameter is: [Dns2Ip] FORMAT Dns2Ip_Index = Dns2Ip_DomainName, Dns2Ip_FirstIpAddress, Dns2Ip_SecondIpAddress, Dns2Ip_ThirdIpAddress; [\Dns2Ip] For example: Dns2Ip 0 = DnsName, 1.1.1.1, 2.2.2.2, 3.3.3.3, ; For a detailed description of the table, see "Configuring the Internal DNS Table" on page 152.
Internal SRV Table	
Internal SRV Table configure network > dns srv2ip [SRV2IP]	The table 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 the ini file table parameter is:

Parameter	Description
	<p>[SRV2IP] FORMAT SRV2IP_Index = SRV2IP_InternalDomain, SRV2IP_TransportType, SRV2IP_Dns1, SRV2IP_Priority1, SRV2IP_Weight1, SRV2IP_Port1, SRV2IP_Dns2, SRV2IP_Priority2, SRV2IP_Weight2, SRV2IP_Port2, SRV2IP_Dns3, SRV2IP_Priority3, SRV2IP_Weight3, SRV2IP_Port3; [\SRV2IP]</p> <p>For example: SRV2IP 0 = SrvDomain,0,Dnsname1,1,1,500,Dnsname2,2,2,501,\$\$,0,0,0;</p> <p>For a detailed description of the table, see "Configuring the Internal SRV Table" on page 153.</p>

55.2.7 DHCP Parameters

The Dynamic Host Control Protocol (DHCP) parameters are described in the table below.

Table 55-15: DHCP Parameters

Parameter	Description
Enable DHCP [DHCPEnable]	<p>Enables DHCP client functionality.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable <p>Note:</p> <ul style="list-style-type: none"> ▪ For the parameter to take effect, a device reset is required. ▪ For a detailed description of DHCP, see "DHCP-based Provisioning" on page 615. ▪ The parameter is a "hidden" parameter. Once defined and saved to flash memory, its value doesn't revert to default even if the parameter doesn't appear in the <i>ini</i> file.
[DHCP120OptionMode]	<p>Enables the acceptance of DHCP Option 120 in DHCP responses sent by a DHCP server.</p> <ul style="list-style-type: none"> ▪ [0] = DHCP Option 120 is not supported and ignored if received in the DHCP response. ▪ [1] = (Default) DHCP Option 120 is supported and if received, the device adds the SIP server information to the Proxy Set.
[DHCPspeedFactor]	<p>Defines the device's DHCP renewal speed for a leased IP address from a DHCP server.</p> <ul style="list-style-type: none"> ▪ [0] = Disable ▪ [1] = (Default) Normal ▪ [2] to [10] = Fast <p>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.</p> <p>Note: For the parameter to take effect, a device reset is required.</p>
DHCP Servers Table	

Parameter	Description
DHCP Servers Table configure network > dhcp server <index> [DhcpServer]	Defines the device's embedded DHCP server. The format of the ini file table parameter is as follows: [DhcpServer] FORMAT DhcpServer_Index = DhcpServer_InterfaceName, DhcpServer_StartIPAddress, DhcpServer_EndIPAddress, DhcpServer_SubnetMask, DhcpServer_LeaseTime, DhcpServer_DNSServer1, DhcpServer_DNSServer2, DhcpServer_NetbiosNameServer, DhcpServer_NetbiosNodeType, DhcpServer_NTPServer1, DhcpServer_NTPServer2, DhcpServer_TimeOffset, DhcpServer_TftpServer, DhcpServer_BootFileName, DhcpServer_ExpandBootfileName, DhcpServer_OverrideRouter, DhcpServer_SipServer, DhcpServer_SipServerType; [\DhcpServer] For a detailed description of the table, see Configuring the Device's DHCP Server.
DHCP Vendor Class Table	
DHCP Vendor Class table configure network > dhcp- server vendor-class [DhcpVendorClass]	Defines Vendor Class Identifier (VCI) names (DHCP Option 60) for the device's DHCP server. Only if the DHCPDiscover request message, received from the DHCP client, contains this value does the device provide DHCP services. The format of the ini file table parameter is as follows: [DhcpVendorClass] FORMAT DhcpVendorClass_Index = DhcpVendorClass_DhcpServerIndex, DhcpVendorClass_VendorClassId; [\DhcpVendorClass] For a detailed description of the table, see Configuring the Vendor Class Identifier on page 206.
DHCP Option Table	
DHCP Option table configure network > dhcp- server option [DhcpOption]	Defines additional DHCP Options that the device's DHCP server can use to service its DHCP clients. The format of the ini file table parameter is as follows: [DhcpOption] FORMAT DhcpOption_Index = DhcpOption_DhcpServerIndex, DhcpOption_Option, DhcpOption_Type, DhcpOption_Value, DhcpOption_ExpandValue; [\DhcpOption] For a detailed description of the table, see Configuring Additional DHCP Options on page 207.
DHCP Static IP Table	
DHCP Static IP table configure network > dhcp- server static-ip <index> [DhcpStaticIP]	Defines static "reserved" IP addresses that the device's DHCP server allocates to specific DHCP clients defined by MAC address. The format of the ini file table parameter is as follows: [DhcpStaticIP] FORMAT DhcpStaticIP_Index = DhcpStaticIP_DhcpServerIndex, DhcpStaticIP_IPAddress, DhcpStaticIP_MACAddress; [\DhcpStaticIP] For a detailed description of the table, see Configuring Static IP

Parameter	Description
	Addresses for DHCP Clients on page 209.

55.2.8 NTP and Daylight Saving Time Parameters

The Network Time Protocol (NTP) and daylight saving time parameters are described in the table below.

Table 55-16: NTP and Daylight Saving Time Parameters

Parameter	Description
NTP Parameters CLI path: configure system > ntp > Note: For more information on Network Time Protocol (NTP), see "Simple Network Time Protocol Support" on page 115.	
Primary NTP Server Address primary-server [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).
Secondary NTP Server Address secondary-server [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.
NTP Update Interval 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. Note: It is not recommend to set the parameter to beyond one month (i.e., 2592000 seconds).
NTP Authentication Key Identifier auth-key-id [NtpAuthKeyId]	Defines the NTP authentication key identifier for authenticating NTP messages. The identifier must match the value configured on the NTP server. The NTP server may have several keys configured for different clients; this number identifies which key is used. The valid value is 1 to 65535. The default is 0 (i.e., no authentication is done).
NTP Authentication Secret Key auth-key-md5 [ntpAuthMd5Key]	Defines the secret authentication key shared between the device (client) and the NTP server, for authenticating NTP messages. The valid value is a string of up to 32 characters. By default, no key is defined.
Regional Clock and Daylight Saving Time Parameters	
UTC Offset configure system > clock > utc-offset [NTPServerUTCOffset]	Defines the Universal Time Coordinate (UTC) offset (in seconds) from the local time. The valid range is -43200 to 43200. The default is 0. Note: The offset setting is applied only on the hour. For example, if you configure the parameter at 15:42, the device applies the setting only at 16:00.

Parameter	Description
Daylight Saving Time configure system > clock > summer-time > summer-time [DayLightSavingTimeEnable]	Enables daylight saving time (DST). <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable
Start Time / Day of Month Start configure system > clock > summer-time > start [DayLightSavingTimeStart]	Defines the date and time when DST begins. This value can be configured using any of the following formats: <ul style="list-style-type: none"> ▪ Day of year - <i>mm:dd:hh:mm</i>, where: <ul style="list-style-type: none"> ✓ <i>mm</i> denotes month ✓ <i>dd</i> denotes date of the month ✓ <i>hh</i> denotes hour ✓ <i>mm</i> denotes minutes For example, "05:01:08:00" denotes daylight saving starting from May 1 at 8 A.M. ▪ Day of month - <i>mm:day/wk:hh:mm</i>, where: <ul style="list-style-type: none"> ✓ <i>mm</i> denotes month (e.g., 04) ✓ <i>day</i> denotes day of week (e.g., FRI) ✓ <i>wk</i> denotes week of the month (e.g., 03) ✓ <i>hh</i> denotes hour (e.g., 23) ✓ <i>mm</i> denotes minutes (e.g., 10) 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.
End Time / Day of Month End configure system > clock > summer-time > end [DayLightSavingTimeEnd]	Defines the date and time when DST ends. For a description of the format of this value, see the DayLightSavingTimeStart parameter.
Offset configure system > clock > summer-time > offset [DayLightSavingTimeOffset]	Defines the DST offset (in minutes). The valid range is 0 to 120. The default is 60. Note: The offset setting is applied only on the hour. For example, if you configure the parameter at 15:42, the device applies the setting only at 16:00.

55.3 Debugging and Diagnostics Parameters

This subsection describes the device's debugging and diagnostic parameters.

55.3.1 General Parameters

The general debugging and diagnostic parameters are described in the table below.

Table 55-17: General Debugging and Diagnostic Parameters

Parameter	Description
[EnableDiagnostics]	Determines the method for verifying correct functioning of the different hardware components on the device. On completion of the

Parameter	Description
	<p>check and if the test fails, the device sends information on the test results of each hardware component to the Syslog server.</p> <ul style="list-style-type: none"> [0] = (Default) Rapid and Enhanced self-test mode. [1] = Detailed self-test mode (full test of DSPs, PCM, Switch, LAN, PHY and Flash). [2] = A quicker version of the Detailed self-test mode (full test of DSPs, PCM, Switch, LAN, PHY, but partial test of Flash). <p>Note: For the parameter to take effect, a device reset is required.</p>
Delay After Reset [sec] configure voip > sip-definition advanced-settings > delay- after-reset [GWAppDelayTime]	<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>Note: This feature helps overcome connection problems caused by some LAN routers or IP configuration parameters' modifications by a DHCP server.</p>
[EnableAutoRAITransmitBER]	<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"> [0] Disable (default) [1] Enable

55.3.2 SIP Test Call Parameters

The SIP Signaling Test Call parameters are described in the table below.

Table 55-18: SIP Test Call Parameters

Parameter	Description
Test Call DTMF String configure troubleshoot > test-call settings > testcall- dtmf-string [TestCallDtmfString]	<p>Defines the DTMF tone that is played for answered test calls (incoming and outgoing).</p> <p>The DTMF string can be up to 15 strings. The default is "3212333". If no string is defined (empty), DTMF is not played.</p>
Test Call ID configure troubleshoot > test-call settings > testcall- 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>Note: The parameter is only for testing incoming calls destined to this prefix number.</p>
SBC Test ID 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>The 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>

Parameter	Description
	<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>
Test Call Rules Table	
Test Call Rules configure troubleshoot >test-call test-call-table [Test_Call]	Defines Test Call rules. [Test_Call] FORMAT Test_Call_Index = Test_Call_EndpointURI, Test_Call_CalledURI, Test_Call_RouteBy, Test_Call_IPGroupName, Test_Call_DestAddress, Test_Call_DestTransportType, Test_Call_SIPInterfaceName, 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, Test_Call_QOEProfile, Test_Call_BWProfile; [\Test_Call] For a description of the table, see "Configuring Test Call Endpoints" on page 713.

55.3.3 Syslog, CDR and Debug Parameters

The Syslog, CDR and debug parameters are described in the table below.

Table 55-19: Syslog, CDR and Debug Parameters

Parameter	Description
Enable Syslog configure troubleshoot > syslog > syslog [EnableSyslog]	Determines whether the device sends logs and error messages (e.g., CDRs) generated by the device to a Syslog server. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable <p>Note:</p> <ul style="list-style-type: none"> ▪ If you enable Syslog, you must enter an IP address of the Syslog server (using the SyslogServerIP parameter). ▪ Syslog messages may increase the network traffic. ▪ To configure Syslog SIP message logging levels, use the GwDebugLevel parameter. ▪
Syslog Server IP configure troubleshoot > syslog > syslog-ip [SyslogServerIP]	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. The default IP address is 0.0.0.0.
Syslog Server Port configure troubleshoot > syslog > syslog-port	Defines the UDP port of the Syslog server. The valid range is 0 to 65,535. The default port is 514.

Parameter	Description
[SyslogServerPort]	
CDR Server IP Address configure troubleshoot > cdr > cdr-srvr-ip-adrr [CDRSyslogServerIP]	<p>Defines the destination IP address to where CDR logs are sent. The default value is a null string, which causes CDR messages to be sent with all Syslog messages to the Syslog server.</p> <p>Note:</p> <ul style="list-style-type: none"> The CDR messages are sent to UDP port 514 (default Syslog port). This mechanism is active only when Syslog is enabled (i.e., the parameter EnableSyslog is set to 1).
CDR Report Level configure troubleshoot > cdr > cdr-report-level [CDRReportLevel]	<p>Enables signaling-related CDRs to be sent to a Syslog server and defines the call stage at which they are sent.</p> <ul style="list-style-type: none"> [0] None = (Default) CDRs are not used. [1] End Call = CDR is sent to the Syslog server at the end of each call. [2] Start & End Call = CDR report is sent to Syslog at the start and end of each call. [3] Connect & End Call = CDR report is sent to Syslog at connection and at the end of each call. [4] Start & End & Connect Call = CDR report is sent to Syslog at the start, at connection, and at the end of each call. <p>Note:</p> <ul style="list-style-type: none"> For the SBC application, the parameter enables only signaling-related CDRs. To enable media-related CDRs for SBC calls, use the MediaCDRReportLevel parameter. The CDR Syslog message complies with RFC 3164 and is identified by: Facility = 17 (local1) and Severity = 6 (Informational). This mechanism is active only when Syslog is enabled (i.e., the parameter EnableSyslog is set to 1).
Media CDR Report Level configure troubleshoot > cdr > media-cdr-rprt-level [MediaCDRReportLevel]	<p>Enables media-related CDRs of SBC calls to be sent to a Syslog server and defines the call stage at which they are sent.</p> <ul style="list-style-type: none"> [0] None = (Default) No media-related CDR is sent. [1] End Media = Sends a CDR only at the end of the call. [2] Start & 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. [3] Update & 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. [4] Start & End & 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. <p>Note: To enable CDR generation as well as enable signaling-related CDRs, use the CDRReportLevel parameter.</p>
Local Storage Max File Size	Defines the size (in kilobytes) of each stored CDR file. Once the file

Parameter	Description
configure troubleshoot > cdr > local-storage-max-file-size [CDRLocalMaxFileSize]	size is reached, the device creates a new file for subsequent CDRs, and so on. The valid value is 100 to 1024. The default is 1024.
Local Storage Max Number of Files configure troubleshoot > cdr > local-storage-max-files [CDRLocalMaxNomOfFiles]	Defines the maximum number of stored CDR files. If the maximum number is reached, the device replaces (overwrites) the oldest created file with a subsequent new file, and so on. The valid value is 2 to 4096. The default is 5.
Local Storage File Creation Interval configure troubleshoot > cdr > local-storage-interval [CDRLocalInterval]	Defines how often (in minutes) the device creates a new CDR file. For example, if configured to 60, it creates a new file every hour. This occurs even if the maximum configured file size has not been reached (see the CDRLocalMaxFileSize parameter). However, if the maximum configured file size has been reached and the interval configured by the parameter has not been reached, a new CDR file is created. The valid value is 2 to 1440. The default is 60.
Debug Level configure troubleshoot > syslog > debug-level [GwDebugLevel]	Enables Syslog debug reporting and logging level. <ul style="list-style-type: none"> ▪ [0] No Debug = (Default) Debug is disabled and Syslog messages are not sent. ▪ [1] Basic = Sends debug logs of incoming and outgoing SIP messages. ▪ [5] Detailed = Sends debug logs of incoming and outgoing SIP message as well as many other logged processes.
configure system > cdr > non-call-cdr-rprt [EnableNonCallCdr]	Enables creation of CDR messages for non-call SIP dialogs (such as SUBSCRIBE, OPTIONS, and REGISTER). <ul style="list-style-type: none"> ▪ [0] = (Default) Disable ▪ [1] = Enable
Syslog Optimization configure troubleshoot > syslog > syslog-optimization [SyslogOptimization]	Enables the device to accumulate and bundle multiple debug messages into a single UDP packet and then send it to a Syslog server. The benefit of this feature is that it reduces the number of UDP Syslog packets, thereby improving (optimizing) CPU utilization. <ul style="list-style-type: none"> ▪ [0] Disable ▪ [1] Enable (default) Note: The size of the bundled message is configured by the MaxBundleSyslogLength parameter.
mx-syslog-igth [MaxBundleSyslogLength]	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. The valid value range is 0 to 1220 (where 0 indicates that no bundling occurs). The default is 1220. Note: The parameter is applicable only if the GwDebugLevel parameter is enabled.
Syslog CPU Protection configure troubleshoot > syslog > syslog-cpu-protection [SyslogCpuProtection]	Enables the protection of the device's CPU resources during debug reporting, ensuring voice traffic is unaffected. If CPU resources drop (i.e., high CPU usage) to a critical level (threshold), the device automatically lowers the debug level to free up CPU resources that were required for the previous debug-level functionality. When sufficient CPU resources become available again, the device increases the debug level. The threshold is configured by the 'Debug

Parameter	Description
	Level High Threshold' parameter (see below). <ul style="list-style-type: none"> ▪ [0] Disable ▪ [1] Enable (default)
Debug Level High Threshold configure voip > sip-definition settings > debug-level-high- threshold [DebugLevelHighThreshold]	Defines the threshold (in percentage) for automatically switching to a different debug level, depending on CPU usage. The parameter is applicable only if the 'Syslog CPU Protection' parameter is enabled. The valid value is 0 to 100. The default is 90. The debug level is changed upon the following scenarios: <ul style="list-style-type: none"> ▪ CPU usage equals threshold: Debug level is reduced one level. ▪ CPU usage is at least 5% greater than threshold: Debug level is reduced another level. ▪ CPU usage is 5 to 19% less than threshold: Debug level is increased by one level. ▪ CPU usage is at least 20% less than threshold: Debug level is increased by another level. For example, assume that the threshold is set to 70% and the Debug Level to Detailed (5). When CPU usage reaches 70%, the debug level is reduced to Basic (1). When CPU usage increases by 5% or more than the threshold (i.e., greater than 75%), the debug level is disabled - No Debug (0). When the CPU usage decreases to 5% less than the threshold (e.g., 65%), the debug level is increased to Basic (1). When the CPU usage decreases to 20% less than the threshold (e.g., 50%), the debug level changes to Detailed (5). Note: The device does not increase the debug level to a level that is higher than what you configured for the 'Debug Level' parameter.
Syslog Facility Number [SyslogFacility]	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. <ul style="list-style-type: none"> ▪ [16] = (Default) local use 0 (local0) ▪ [17] = local use 1 (local1) ▪ [18] = local use 2 (local2) ▪ [19] = local use 3 (local3) ▪ [20] = local use 4 (local4) ▪ [21] = local use 5 (local5) ▪ [22] = local use 6 (local6) ▪ [23] = local use 7 (local7)
CDR Syslog Sequence Number configure system > cdr > cdr- seq-num [CDRSyslogSeqNum]	Enables or disables the inclusion of the sequence number (S=) in CDR Syslog messages. <ul style="list-style-type: none"> ▪ [0] Disable ▪ [1] Enable (default)
Activity Types to Report via Activity Log Messages configure troubleshoot >	Defines the operations (activities) performed in the Web interface that are reported to a Syslog server. <ul style="list-style-type: none"> ▪ [pvc] Parameters Value Change = Changes made on-the-fly to

Parameter	Description
activity-log [ActivityListToLog]	<p>parameters and tables, and Configuration file load. Note that the ini file parameter, EnableParametersMonitoring can also be used to set this option.</p> <ul style="list-style-type: none"> ▪ [afl] Auxiliary Files Loading = Loading of Auxiliary files. ▪ [dr] Device Reset = Resetting of the device through the Maintenance Actions page. Note: For this option to take effect, a device reset is required. ▪ [fb] Flash Memory Burning = Saving configuration with burn to flash (in the Maintenance Actions page). ▪ [swu] Device Software Update = Software updates (i.e., loading of cmp file) through the Software Upgrade Wizard. ▪ [ard] Access to Restricted Domains = Access to restricted Web pages: <ul style="list-style-type: none"> ✓ (1) ini parameters (AdminPage) ✓ (2) General Security Settings ✓ (3) Configuration File ✓ (5) License Key ✓ (7) Access List ✓ (8) Web User Accounts ▪ [naa] Non-Authorized Access = Attempts to log in to the Web interface with a false or empty username or password. ▪ [spc] Sensitive Parameters Value Change = Changes made to "sensitive" parameters: <ul style="list-style-type: none"> ✓ (1) IP Address ✓ (2) Subnet Mask ✓ (3) Default Gateway IP Address ✓ (4) ActivityListToLog ▪ [ll] Login and Logout = Web login and logout attempts. ▪ [cli] = CLI commands entered by the user. ▪ [ae] Action Executed = Logs user actions that are not related to parameter changes. The actions can include, for example, file uploads, file delete, lock-unlock maintenance actions, LDAP clear cache, register-unregister, and start-stop trunk. In the Web, these actions are typically done by clicking a button (e.g., the LOCK button). <p>Note: For the <i>ini</i> file parameter, enclose values in single quotation marks, for example: ActivityListToLog = 'pvc', 'afl', 'dr', 'fb', 'swu', 'ard', 'naa', 'spc'.</p>
[EnableParametersMonitoring]	<p>Enables the monitoring, through Syslog messages, of parameters that are modified on-the-fly.</p> <ul style="list-style-type: none"> ▪ [0] = (Default) Disable ▪ [1] = Enable
Debug Recording Destination IP configure troubleshoot > logging settings > dbg-rec-dest-ip [DebugRecordingDestIP]	<p>Defines the IP address of the server for capturing debug recording.</p>
Debug Recording Destination Port configure troubleshoot >	<p>Defines the UDP port of the server for capturing debug recording. The default is 925.</p>

Parameter	Description
logging settings > dbg-rec-dest-port [DebugRecordingDestPort]	
Enable Core Dump [EnableCoreDump]	Enables the automatic generation of a Core Dump file upon a device crash. <ul style="list-style-type: none"> ▪ [0] Disable (disable) ▪ [1] Enable
Core Dump Destination IP [CoreDumpDestIP]	Defines the IP address of the remote server where you want the device to send the Core Dump file. By default, no IP address is defined.
Logging Filters Table	
Logging Filters Table configure troubleshoot > logging logging-filters [LoggingFilters]	The table defines log filtering rules for Syslog messages and debug recordings. The format of the ini file table parameter is: [LoggingFilters] FORMAT LoggingFilters_Index = LoggingFilters_FilterType, LoggingFilters_Value, LoggingFilters_LogDestination, LoggingFilters_CaptureType, LoggingFilters_Mode; [\LoggingFilters] For a detailed description of the table, see "Configuring Log Filter Rules" on page 693.
SBC CDR Format Table	
SBC CDR Format Table configure troubleshoot > cdr > cdr-format sbccdr-format [SBCCDRFormat]	The table defines CDR customization rules for SBC calls. The format of the ini file table parameter is: [SBCCDRFormat] FORMAT SBCCDRFormat_Index = SBCCDRFormat_CDRType, SBCCDRFormat_FieldType, SBCCDRFormat_Title, SBCCDRFormat_RadiusType, SBCCDRFormat_RadiusID; [\SBCCDRFormat] For a detailed description of the table, see Customizing CDRs for SBC Calls on page 678.

55.3.4 Resource Allocation Indication Parameters

The Resource Allocation Indication (RAI) parameters are described in the table below.

Table 55-20: RAI Parameters

Parameter	Description
[EnableRAI]	Enables Resource Available Indication (RAI) alarm generation if the device's busy endpoints exceed a user-defined threshold, configured by the RAIHighThreshold parameter. When enabled and the threshold is crossed, the device sends the SNMP trap, acBoardCallResourcesAlarm. <ul style="list-style-type: none"> ▪ [0] = (Default) Disable ▪ [1] = Enable

Parameter	Description
	Note: For the parameter to take effect, a device reset is required.
[RAIHighThreshold]	<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>Note: The percentage of busy endpoints is calculated by dividing the number of busy endpoints by the total number of "enabled" endpoints.</p>
[RAILowThreshold]	<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>
[RAILoopTime]	<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>

55.4 HA Parameters

The High Availability (HA) parameters are described in the table below.

Table 55-21: HA Parameters

Parameter	Description
HA Device Name configure network > high-availability > unit-id-name [HAUnitIdName]	<p>Defines a name for the active device, which is displayed on the Home page to indicate the active device. The valid value is a string of up to 128 characters. The default value is "Device 1".</p>
Redundant HA Device Name configure network > high-availability > redundant-unit-id-name	<p>Defines a name for the redundant device, which is displayed on the Home page to indicate the redundant device. The valid value is a string of up to 128 characters. The default value is "Device 2".</p>
HA Remote Address configure network > high-availability > remote-address [HARemoteAddress]	<p>Defines the Maintenance interface address of the redundant device in the HA system. By default, no value is defined.</p> <p>Note: For the parameter to take effect, a device reset is required.</p>
Preempt Mode configure network > high-availability > revertive-mode [HARevertiveEnabled]	<p>Enables HA switchover based on HA priority.</p> <ul style="list-style-type: none"> ▪ [0] Disable = (Default) A switchover over to the redundant device is done only if a failure occurs in the currently active device. ▪ [1] Enable = A switchover over to the redundant device is done if a failure occurs in the currently active device. However, a switchover to the device with the highest priority (configured by the HAPriority parameter) occurs whenever the device recovers from a failure. Therefore, whenever possible, the highest priority device is the active

Parameter	Description
	<p>one.</p> <p>For more information on the HA switchover mechanism, see Device Switchover upon Failure on page 557.</p> <p>Note: For the parameter to take effect, a device reset is required.</p>
Preempt Priority configure network > high-availability > priority [HAPriority]	<p>Defines the priority of the active device used in the HA Preempt mechanism.</p> <p>The valid value is 1 (lowest priority) to 10 (highest priority). The default is 5.</p> <p>Note:</p> <ul style="list-style-type: none"> For the parameter to take effect, a device reset is required. The parameter is applicable only if you configure the 'Preempt Mode' parameter to Enable. You must configure each device in the HA system with different parameter values (priorities).
Redundant Preempt Priority configure network > high-availability > redundant-priority	<p>Defines the priority of the redundant device used in the HA Preempt mechanism.</p> <p>The valid value is 1 (lowest priority) to 10 (highest priority). The default is 5.</p> <p>Note:</p> <ul style="list-style-type: none"> For the parameter to take effect, a device reset is required. The parameter is applicable only if you configure the 'Preempt Mode' parameter to Enable. You must configure each device in the HA system with different parameter values (priorities).
HA Network Reachability Parameters	
HA Network Reachability configure network > high-availability > net-mon-enable [HAPingEnabled]	<p>Enables the pinging of an active IP network destination in HA mode to test reachability from one of the device's IP network interfaces. If no reply is received from a ping and the previous ping was successful, a switchover occurs to the redundant device.</p> <ul style="list-style-type: none"> [0] Disable (default) [1] Enable
Destination Address configure network > high-availability > net-mon-destination [HAPingDestination]	<p>Defines the IP address of the destination that the device pings.</p> <p>The default is 0.0.0.0.</p>
Source Interface Name configure network > high-availability > net-mon-source-interface [HAPingSourceIfName]	<p>Defines the device's IP network interface from where the ping is sent.</p> <p>The valid value is the name of the IP interface as configured in the 'Interface Name' field of the IP Interfaces table. By default, no IP network is defined.</p>
Ping Timeout configure network > high-availability > net-mon-ping-timeout [HAPingTimeout]	<p>Defines the timeout (in seconds) for which the ping request waits for a reply.</p> <p>The valid value is 1 to 60. The default is 1.</p>

Parameter	Description
Ping Retries configure network > high-availability > net-mon-ping-retries [HAPingRetries]	Defines the number of ping requests that the device sends after no response is received from the destination, before the destination is declared unavailable. For example, if you specify 2, the destination is declared as down after three consecutive ping requests fail to evoke a response from the destination. The valid value is 0 to 100. The default 2.

55.5 Security Parameters

This subsection describes the device's security parameters.

55.5.1 General Security Parameters

The general security parameters are described in the table below.

Table 55-22: General Security Parameters

Parameter	Description
Firewall Table	
Firewall configure network > access-list [AccessList]	The table defines the device's access list (firewall), which defines network traffic filtering rules. The format of the ini file table parameter is: [AccessList] 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; [AccessList] 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; 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. For a detailed description of the table, see "Configuring Firewall Rules" on page 157.
Media Latching	
Inbound Media Latch Mode configure voip > media settings > inbound-media-latch-mode [InboundMediaLatchMode]	Enables the Media Latching feature. <ul style="list-style-type: none"> ▪ [0] Strict = Device latches onto the first original stream (IP address:port). It does not latch onto any other stream during the session. ▪ [1] Dynamic = (Default) Device latches onto the first stream. If it receives at least a minimum number of consecutive packets (configured by New<media type>StreamPackets) from a

Parameter	Description
	<p>different source(s) and the device has not received packets from the current stream for a user-defined period (TimeoutToRelatch<media type>Msec), it latches onto the next packet received from any other stream. If other packets of a different media type are received from the new stream, based on IP address and SSRC for RTCP/RTP and based on IP address only for T.38, the packet is accepted immediately. Note: If a packet from the original (first latched onto) IP address:port is received at any time, the device latches onto this stream.</p> <ul style="list-style-type: none"> ▪ [2] Dynamic-Strict = Device latches onto the first stream. If it receives at least a minimum number of consecutive packets (configured by New<media type>StreamPackets) all from the same source which is different to the first stream and the device has not received packets from the current stream for a user-defined period (TimeoutToRelatch<media type>Msec), it latches onto the next packet received from any other stream. If other packets of different media type are received from the new stream based on IP address and SSRC for RTCP and based on IP address only for T.38, the packet is accepted immediately. Note: If a packet from the original (first latched onto) IP address:port is received at any time, the device latches onto this stream. ▪ [3] Strict-On-First = Typically used for NAT, where the correct IP address:port is initially unknown. The device latches onto the stream received in the first packet. The device does not change this stream unless a packet is later received from the original source. <p>Note: If you configure the parameter to [0] Strict, the device cannot perform NAT traversal. In this setup, configure the NATMode parameter to [1] Disable NAT.</p>
New RTP Stream Packets [NewRtpStreamPackets]	<p>Defines the minimum number of continuous RTP packets received by the device's channel to allow latching onto the new incoming stream.</p> <p>The valid range is 0 to 20. The default is 3. If set to 0, the device is left exposed to attacks against multiple packet streams.</p>
New RTCP Stream Packets [NewRtcpStreamPackets]	<p>Defines the minimum number of continuous RTCP packets received by the device's channel to allow latching onto the new incoming stream.</p> <p>The valid range is 0 to 20. The default is 3. If set to 0, the device is left exposed to attacks against multiple packet streams.</p>
New SRTP Stream Packets [NewSRTPStreamPackets]	<p>Defines the minimum number of continuous SRTP packets received by the device's channel to allow latching onto the new incoming stream.</p> <p>The valid range is 0 to 20. The default is 3. If set to 0, the device is left exposed to attacks against multiple packet streams.</p>
New SRTCP Stream Packets [NewSRTCPStreamPackets]	<p>Defines the minimum number of continuous SRTCP packets received by the device's channel to allow latching onto the new incoming stream.</p> <p>The valid range is 0 to 20. The default is 3. If set to 0, the device is left exposed to attacks against multiple packet streams.</p>

Parameter	Description
Timeout To Relatch RTP [TimeoutToRelatchRTPMsec]	Defines a period (msec) during which if no packets are received from the current RTP session, the channel can re-latch onto another stream. The valid range is any value from 0. The default is 200.
Timeout To Relatch SRTP [TimeoutToRelatchSRTPMsec]	Defines a period (msec) during which if no packets are received from the current SRTP session, the channel can re-latch onto another stream. The valid range is any value from 0. The default is 200.
Timeout To Relatch Silence [TimeoutToRelatchSilenceMsec]	Defines a period (msec) during which if no packets are received from the current RTP/SRTP session and the channel is in silence mode, the channel can re-latch onto another stream. The valid range is any value from 0. The default is 200.
Timeout To Relatch RTCP [TimeoutToRelatchRTCPMsec]	Defines a period (msec) during which if no packets are received from the current RTCP session, the channel can re-latch onto another RTCP stream. The valid range is any value from 0. The default is 10,000.
Fax Relay Rx/Tx Timeout [FaxRelayTimeoutSec]	Defines a period (sec) during which if no T.38 packets are received or sent from the current T.38 fax relay session, the channel can re-latch onto another stream. The valid range is 0 to 255. The default is 10.

55.5.2 HTTPS Parameters

The Secure Hypertext Transport Protocol (HTTPS) parameters are described in the table below.

Table 55-23: HTTPS Parameters

Parameter	Description
Secured Web Connection (HTTPS) configure system > web > secured-connection [HTTPSONly]	Determines the protocol used to access the Web interface. <ul style="list-style-type: none"> ▪ [0] HTTP and HTTPS (default). ▪ [1] HTTPs Only = Unencrypted HTTP packets are blocked. Note: For the parameter to take effect, a device reset is required.
configure system > web > https-port [HTTPSPort]	Defines the local Secured HTTPS port of the device. The parameter allows secure remote device Web management from the LAN. To enable secure Web management from the LAN, configure the desired port. The valid range is 1 to 65535 (other restrictions may apply within this range). The default port is 443. Note: For the parameter to take effect, a device reset is required.
HTTPS Cipher String configure system > web > https-cipher-string [HTTPSCipherString]	Defines the Cipher string for HTTPS (in OpenSSL cipher list format). For the valid range values, refer to URL http://www.openssl.org/docs/apps/ciphers.html . 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.

Parameter	Description
	<p>Note:</p> <ul style="list-style-type: none"> For the parameter to take effect, a device reset is required. If the installed License Key includes the Strong Encryption feature, the default of the parameter is changed to 'RC4:EXP', enabling RC-128bit encryption. The value 'ALL' can be configured only if the installed License Key includes the Strong Encryption feature.
Require Client Certificates for HTTPS connection configure system > web > req-client-cert [HTTPSRequireClientCertificate]	<p>Enables the requirement of client certificates for HTTPS connection.</p> <ul style="list-style-type: none"> [0] Disable = (Default) Client certificates are not required. [1] 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. <p>Note:</p> <ul style="list-style-type: none"> For the parameter to take effect, a device reset is required. For a description on implementing client certificates, see "TLS for Remote Device Management" on page 112.

55.5.3 SRTP Parameters

The Secure Real-Time Transport Protocol (SRTP) parameters are described in the table below.

Table 55-24: SRTP Parameters

Parameter	Description
Media Security configure voip > media security > media-security-enable [EnableMediaSecurity]	<p>Enables Secure Real-Time Transport Protocol (SRTP).</p> <ul style="list-style-type: none"> [0] Disable (default) [1] Enable <p>Note: For the parameter to take effect, a device reset is required.</p>
Master Key Identifier (MKI) Size configure voip > media security > srtp-tx-packet-mki-size [SRTPTxPacketMKISize]	<p>Global parameter that defines the size (in bytes) of the Master Key Identifier (MKI) in SRTP Tx packets. You can also configure this functionality per specific calls, using IP Profiles (IpProfile_MKISize). For a detailed description of the parameter and for configuring this functionality in the IP Profiles table, see "Configuring IP Profiles" on page 388.</p> <p>Note: If this functionality is configured for a specific IP Profile, the settings of this global parameter is ignored for calls associated with the IP Profile.</p>
Symmetric MKI Negotiation configure voip > media security > symmetric-mki [EnableSymmetricMKI]	<p>Global parameter that enables symmetric MKI negotiation. You can also configure this functionality per specific calls, using IP Profiles (IpProfile_EnableSymmetricMKI). For a detailed description of the parameter and for configuring this functionality in the IP Profiles table, see "Configuring IP Profiles" on page 388.</p> <p>Note: If this functionality is configured for a specific IP Profile, the settings of this global parameter is ignored for calls associated with</p>

Parameter	Description
	the IP Profile.
Offered SRTP Cipher Suites configure voip > media security > offer-srtp-cipher [SRTPOfferedSuites]	Defines the offered crypto suites (cipher encryption algorithms) for SRTP. <ul style="list-style-type: none"> ▪ [0] All = (Default) All available crypto suites. ▪ [1] 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. ▪ [2] 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. <p>Note: The 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>
configure voip > sbc settings > sbc-dtls-mtu [SbcDtlsMtu]	Defines the maximum transmission unit (MTU) size for the DTLS handshake. The device does not attempt to send handshake packets that are larger than the configured value. Adjusting the MTU is useful when there are network constraints on the size of packets that can be sent. The valid value range is 228 to 1500. The default is 1500.
Disable Authentication On Transmitted RTP Packets configure voip > media security > RTP- authentication-disable-tx [RTPAuthenticationDisableTx]	Enables authentication on transmitted RTP packets in a secured RTP session. <ul style="list-style-type: none"> ▪ [0] Enable (default) ▪ [1] Disable
Disable Encryption On Transmitted RTP Packets configure voip > media security > RTP-encryption- disable-tx [RTPEncryptionDisableTx]	Enables encryption on transmitted RTP packets in a secured RTP session. <ul style="list-style-type: none"> ▪ [0] Enable (default) ▪ [1] Disable
Disable Encryption On Transmitted RTCP Packets configure voip > media security > RTCP-encryption- disable-tx [RTCPEncryptionDisableTx]	Enables encryption on transmitted RTCP packets in a secured RTP session. <ul style="list-style-type: none"> ▪ [0] Enable (default) ▪ [1] Disable
configure voip > sip-definition settings > srtp-state-behavior- mode [ResetSRTPStateUponRekey]	Global parameter that enables synchronization of the SRTP state between the device and a server when a new SRTP key is generated upon a SIP session expire. You can also configure this functionality per specific calls, using IP Profiles (IpProfile_ResetSRTPStateUponRekey). For a detailed description of the parameter and for configuring this functionality in the IP Profiles table, see "Configuring IP Profiles" on page 388. <p>Note: If this functionality is configured for a specific IP Profile, the settings of this global parameter is ignored for calls associated with the IP Profile.</p>

55.5.4 TLS Parameters

The Transport Layer Security (TLS) parameters are described in the table below.

Table 55-25: TLS Parameters

Parameter	Description
TLS Contexts Table	
TLS Contexts configure system > tls # [TLSContexts]	Defines SSL/TLS certificates. The format of the ini file table parameter is as follows: <pre>[TLSContexts] FORMAT TLSContexts_Index = TLSContexts_Name, TLSContexts_TLSTVersion, TLSContexts_ServerCipherString, TLSContexts_ClientCipherString, TLSContexts_RequireStrictCert, TLSContexts_OcspEnable, TLSContexts_OcspServerPrimary, TLSContexts_OcspServerSecondary, TLSContexts_OcspServerPort, TLSContexts_OcspDefaultResponse; [\TLSContexts]</pre> For a detailed description of the table, see "Configuring TLS Certificate Contexts" on page 99.
TLS Client Re-Handshake Interval configure network/security-settings/tls-re-hndshk-int [TLSReHandshakeInterval]	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).
TLS Mutual Authentication [SIPSRequireClientCertificate]	Defines the device's mode of operation regarding mutual authentication and certificate verification for TLS connections. <ul style="list-style-type: none"> ▪ [0] Disable = (Default) <ul style="list-style-type: none"> ✓ Device acts as a client: Verification of the server's certificate depends on the VerifyServerCertificate parameter. ✓ Device acts as a server: The device does not request the client certificate. ▪ [1] Enable = <ul style="list-style-type: none"> ✓ Device acts as a client: Verification of the server certificate is required to establish the TLS connection. ✓ Device acts as a server: The device requires the receipt and verification of the client certificate to establish the TLS connection. <p>Note:</p> <ul style="list-style-type: none"> ▪ For the parameter to take effect, a device reset is required. ▪ This feature can be configured per SIP Interface (see "Configuring SIP Interfaces" on page 321). ▪ The SIPS certificate files can be changed using the parameters HTTPSCertFileName and HTTPSRootFileName.
Peer Host Name Verification Mode [PeerHostNameVerificationMode]	Enables the device to verify the Subject Name of a TLS certificate received from SIP entities for authentication and establishing TLS connections. <ul style="list-style-type: none"> ▪ [0] Disable (default).

Parameter	Description
	<ul style="list-style-type: none"> ▪ [1] Server Only = Verify Subject Name only when acting as a client for the TLS connection. ▪ [2] Server & Client = Verify Subject Name when acting as a server or client for the TLS connection. <p>If the device receives a certificate from a SIP entity (IP Group) and the parameter is configured to Server Only or Server & Client, it attempts to authenticate the certificate based on the certificate's address.</p> <p>The device searches for a Proxy Set that contains the same address (IP address or FQDN) as that specified in the certificate's SubjectAltName (Subject Alternative Names). For Proxy Sets with an FQDN, the device checks the FQDN itself and not the DNS-resolved IP addresses. If a Proxy Set is found with a matching address, the device establishes a TLS connection.</p> <p>If a matching Proxy Set is not found, one of the following occurs:</p> <ul style="list-style-type: none"> ▪ If the certificate's SubjectAltName is marked as "critical", the device rejects the call. ▪ If the SubjectAltName is not marked as "critical", the device checks if the FQDN in the certificate's Common Name (CN) of the SubjectName is the same as that configured for the TLSRemoteSubjectName parameter or for the Proxy Set. If they are the same, the device establishes a TLS connection; otherwise, the device rejects the call. <p>Note:</p> <ul style="list-style-type: none"> ▪ If you configure the parameter to Server & Client, you also need to configure the SIPRequireClientCertificate parameter to Enable. ▪ For FQDN, the certificate may use wildcards (*) to replace parts of the domain name.
TLS Client Verify Server Certificate configure network/security-settings/tls-vrfy-srvr-cert [VerifyServerCertificate]	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. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable <p>Note: If Subject Name verification is necessary, the parameter PeerHostNameVerificationMode must be used as well.</p>
TLS Remote Subject Name configure network/security-settings/tls-rmt-sub-name [TLSRemoteSubjectName]	Defines the Subject Name that is compared with the name defined in the remote side certificate when establishing TLS connections. <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>Note: The parameter is applicable only if the parameter PeerHostNameVerificationMode is set to 1 or 2.</p>
TLS Expiry Check Start expiry-check-start [TLSExpiryCheckStart]	Defines the number of days before the installed TLS server certificate is to expire at which the device must send a trap (acCertificateExpiryNotification) to notify of this.

Parameter	Description
	The valid value is 0 to 3650. The default is 60.
TLS Expiry Check Period expiry-check-period [TLSExpiryCheckPeriod]	Defines the periodical interval (in days) for checking the TLS server certificate expiry date. The valid value is 1 to 3650. The default is 7.

55.5.5 SSH Parameters

Secure Shell (SSH) parameters are described in the table below.

Table 55-26: SSH Parameters

Parameter	Description
Enable SSH Server configure system > cli-settings > ssh [SSHServerEnable]	Enables the device's embedded SSH server. <ul style="list-style-type: none"> [0] Disable (default) [1] Enable
Server Port configure system > cli-settings > ssh-port [SSHServerPort]	Defines the port number for the embedded SSH server. Range is any valid port number. The default port is 22.
SSH Admin Key configure system > cli-settings > ssh-admin-key [SSHAdminKey]	Defines the RSA public key for strong authentication for logging in to the SSH interface (if enabled). The value should be a base64-encoded string. The value can be a maximum length of 511 characters.
Public Key configure system > cli-settings > ssh-require-public-key [SSHRequirePublicKey]	Enables RSA public keys for SSH. <ul style="list-style-type: none"> [0] = (Default) RSA public keys are optional if a value is configured for the parameter SSHAdminKey. [1] = RSA public keys are mandatory. Note: To define the key size, use the TLSPkeySize parameter.
Max Payload Size ssh-max-payload-size [SSHMaxPayloadSize]	Defines the maximum uncompressed payload size (in bytes) for SSH packets. The valid value is 550 to 32768. The default is 32768.
Max Binary Packet Size configure system > cli-settings > ssh-max-binary-packet-size [SSHMaxBinaryPacketSize]	Defines the maximum packet size (in bytes) for SSH packets. The valid value is 582 to 35000. The default is 35000.
Maximum SSH Sessions configure system > cli-settings > ssh-max-sessions [SSHMaxSessions]	Defines the maximum number of simultaneous SSH sessions. The valid range is 1 to 5. The default is 5.
Enable Last Login Message configure system > cli-settings > ssh-last-login-message	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"> [0] Disable

Parameter	Description
[SSHEnableLastLoginMessage]	<ul style="list-style-type: none"> [1] Enable (default) <p>Note: The last SSH login information is cleared when the device is reset.</p>
Max Login Attempts configure system > cli-settings > ssh-max-login-attempts [SSHMaxLoginAttempts]	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.

55.5.6 IDS Parameters

The Intrusion Detection System (IDS) parameters are described in the table below.

Table 55-27: IDS Parameters

Parameter	Description
Intrusion Detection System (IDS) enable-ids [EnableIDS]	Enables the IDS feature. <ul style="list-style-type: none"> [0] Disable (default) [1] Enable <p>Note: For the parameter to take effect, a device reset is required.</p>
ids-clear-period [IDSAAlarmClearPeriod]	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 IDSAAlarmClearPeriod is set to 20 sec and the Threshold Window is set to 15 sec, the IDSAAlarmClearPeriod 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.
IDS Policy Table	
IDS Policy Table [IDSPolicy]	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 the table, see "Configuring IDS Policies" on page 164.
IDS Rule Table	
IDS Rule Table [IDSRule]	Defines rules for 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_DenyThreshold, IDSRule_DenyPeriod; [\IDSRule] For a detailed description of the table, see "Configuring IDS Policies" on page 164.

Parameter	Description
IDS Match Table	
IDS Match Table [IDSMATCH]	<p>Defines target rules per IDS Policy.</p> <p>The format of the ini file parameter is:</p> <pre>[IDSMATCH] FORMAT IDSMATCH_Index = IDSMATCH_SIPInterface, IDSMATCH_ProxySet, IDSMATCH_Subnet, IDSMATCH_Policy; [\IDSMATCH]</pre> <p>For a detailed description of the table, see "Assigning IDS Policies" on page 168.</p>

55.5.7 OCSP Parameters

The Online Certificate Status Protocol (OCSP) parameters are described in the table below.

Table 55-28: OCSP Parameters

Parameter	Description
Enable OCSP Server configure network > ocspp > enable [OCSPEnable]	<p>Enables or disables certificate checking using OCSP.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable <p>For a description of OCSP, see Configuring Certificate Revocation Checking (OCSP).</p>
Primary Server IP configure network > ocspp > server-ip [OCSPServerIP]	<p>Defines the IP address of the OCSP server.</p> <p>The default IP address is 0.0.0.0.</p>
Secondary Server IP configure network > ocspp > secondary-server-ip [OCSPSecondaryServerIP]	<p>Defines the IP address (in dotted-decimal notation) of the secondary OCSP server (optional).</p> <p>The default IP address is 0.0.0.0.</p>
Server Port configure network > ocspp > server-port [OCSPServerPort]	<p>Defines the OCSP server's TCP port number.</p> <p>The default port number is 2560.</p>
Default Response When Server Unreachable configure network > ocspp > default-response [OCSPDefaultResponse]	<p>Determines whether the device allows or rejects peer certificates when the OCSP server cannot be contacted.</p> <ul style="list-style-type: none"> ▪ [0] Reject (default) ▪ [1] Allow

55.6 Quality of Experience Parameters

The Quality of Experience (QoE) parameters are described in the table below.

Table 55-29: Quality of Experience Parameters

Parameter	Description
SEM Parameters	
Server IP configure voip > qoe settings > server-ip [QOEServerIP]	Defines the IP address of the primary Session Experience Manager (SEM) server to where the quality experience reports are sent. Note: For the parameter to take effect, a device reset is required.
Redundant Server IP configure voip > qoe settings > set secondary-server-ip [QOESecondaryServerIp]	Defines the IP address of the secondary SEM server to where the quality experience reports are sent. This is applicable when the SEM > EMS server is in Geographical Redundancy HA mode. Note: For the parameter to take effect, a device reset is required.
Interface Name configure voip > qoe settings > interface-name [QOEInterfaceName]	Defines the IP network interface on which the quality experience reports are sent. The default is the OAMP interface. Note: For the parameter to take effect, a device reset is required.
QoE Connection by TLS configure voip > qoe settings > tls-enable [QOEEnableTLS]	Enables a TLS connection with the SEM server. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable Note: For the parameter to take effect, a device reset is required.
QoE TLS Context Name configure voip > qoe settings > tls-context-name [QoETLSContextName]	Selects a TLS Context (configured in the TLS Contexts table) for the TLS connection with the SEM server. The valid value is a string representing the name of the TLS Context as configured in the 'Name' field of the TLS Contexts table. The default is the default TLS Context (ID 0).
QoE Report Mode report-mode [QoeReportMode]	Defines at what stage of the call the device sends the QoE data of the call to the SEM server. <ul style="list-style-type: none"> ▪ [0] Report QoE During Call (default) ▪ [1] Report QoE at End of Call Note: If a QoE traffic overflow between SEM and the device occurs, the device sends the QoE data only at the end of the call, regardless of the settings of the parameter.
Quality of Experience Profile Table	
Quality of Experience Profile configure voip > qoe qoe-profile [QOEProfile]	The table defines Quality of Experience Profiles. The format of the ini file table parameter is as follows: [QOEProfile] FORMAT QOEProfile_Index = QOEProfile_Name, QOEProfile_SensitivityLevel; [QOEProfile] For a detailed description of the table, see "Configuring Quality of Experience Profiles" on page 291.
Quality of Experience Color Rules Table	

Parameter	Description
Quality of Experience Color Rules configure voip > qoe qoe-profile qoe-color-rules [QOECOLORRULES]	The table defines Quality of Experience Color Rules. The format of the ini file table parameter is as follows: [QOECOLORRULES] FORMAT QOECOLORRULES_Index = QOECOLORRULES_QoeProfile, QOECOLORRULES_ColorRuleIndex, QOECOLORRULES_monitoredParam, QOECOLORRULES_direction, QOECOLORRULES_profile, QOECOLORRULES_MinorThreshold, QOECOLORRULES_MinorHysteresis, QOECOLORRULES_MajorThreshold, QOECOLORRULES_MajorHysteresis; [QOECOLORRULES] For a detailed description of the table, see "Configuring Quality of Experience Profiles" on page 291.
Bandwidth Profile Table	
Bandwidth Profile configure voip > qoe bw-profile [BWPROFILE]	The table defines Bandwidth Profiles. The format of the ini file table parameter is as follows: [BWPROFILE] FORMAT BWPROFILE_Index = BWPROFILE_Name, BWPROFILE_EgressAudioBandwidth, BWPROFILE_IngressAudioBandwidth, BWPROFILE_EgressVideoBandwidth, BWPROFILE_IngressVideoBandwidth, BWPROFILE_TotalEgressBandwidth, BWPROFILE_TotalIngressBandwidth, BWPROFILE_WarningThreshold, BWPROFILE_hysteresis, BWPROFILE_GenerateAlarms; [BWPROFILE] For a detailed description of the table, see "Configuring Bandwidth Profiles" on page 296. Note: For the parameter to take effect, a device reset is required.
Quality of Service Rules Table	
Quality of Service Rules configure voip > qoe quality-of-service-rules [QUALITYOFSERVICERULES]	Defines Quality of Service rules. The format of the ini file table parameter is as follows: [QUALITYOFSERVICERULES] FORMAT QualityOfServiceRules_Index = QualityOfServiceRules_IPGroupName, QualityOfServiceRules_RuleMetric, QualityOfServiceRules_Severity, QualityOfServiceRules_RuleAction, QualityOfServiceRules_CallsRejectDuration, QualityOfServiceRules_AltIPProfileName; [\QUALITYOFSERVICERULES] For a detailed description of the table, see "Configuring Quality of Service Rules" on page 300
Performance Profile Table	
Performance Profile configure system > performance-profile [PERFORMANCEPROFILE]	Defines alarm thresholds per metric (ASR, ACD and NER). The format of the ini file table parameter is as follows: [PERFORMANCEPROFILE] FORMAT PerformanceProfile_Index = PerformanceProfile_Entity, PerformanceProfile_IPGroupName, PerformanceProfile_SRDName, PerformanceProfile_PMType, PerformanceProfile_MinorThreshold, PerformanceProfile_MajorThreshold, PerformanceProfile_Hysteresis, PerformanceProfile_MinimumSample, PerformanceProfile_WindowSize;

Parameter	Description
	[\PerformanceProfile] For a detailed description of the table, see "Configuring Performance Profiles" on page 651.

55.7 Control Network Parameters

55.7.1 IP Group, Proxy, Registration and Authentication Parameters

The proxy server, registration and authentication SIP parameters are described in the table below.

Table 55-30: Proxy, Registration and Authentication SIP Parameters

Parameter	Description
IP Groups Table	
IP Groups configure voip > ip-group [IPGroup]	This table configures IP Groups. The format of the ini file table parameter is: [IPGroup] FORMAT IPGroup_Index = IPGroup_Type, IPGroup_Name, IPGroup_ProxySetName, IPGroup_SIPGroupName, IPGroup_ContactUser, IPGroup_SipReRoutingMode, IPGroup_AlwaysUseRouteTable, IPGroup_SRDName, IPGroup_MediaRealm, IPGroup_ClassifyByProxySet, IPGroup_ProfileName, IPGroup_MaxNumOfRegUsers, IPGroup_InboundManSet, IPGroup_OutboundManSet, IPGroup_RegistrationMode, IPGroup_AuthenticationMode, IPGroup_MethodList, IPGroup_EnableSBCClientForking, IPGroup_SourceUriInput, IPGroup_DestUriInput, IPGroup_ContactName, IPGroup_Username, IPGroup_Password, IPGroup_UUIFormat, IPGroup_QOEProfile, IPGroup_BWProfile, IPGroup_AlwaysUseSourceAddr, IPGroup_MsgManUserDef1, IPGroup_MsgManUserDef2, IPGroup_SIPConnect, IPGroup_SBCPSAPMode, IPGroup_DTLSContext, IPGroup_CreatedByRoutingServer, IPGroup_UsedByRoutingServer, IPGroup_SBCOperationMode, IPGroup_SBCRouteUsingRequestURIPort, IPGroup_SBCKeepOriginalCallID, IPGroup_TopologyLocation, IPGroup_SBCDialPlanName, IPGroup_CallSetupRulesSetId; [/IPGroup] For a description of the table, see "Configuring IP Groups" on page 329. Note: For the parameter to take effect, a device reset is required.
Accounts Table	
Accounts configure voip > sip-definition account [Account]	Defines user accounts for registering and/or authenticating (digest) IP Groups (e.g., an IP-PBX) with a Serving IP Group (e.g., a registrar server). The format of the ini file table parameter is as follows: [Account] FORMAT Account_Index = Account_ServedTrunkGroup,

Parameter	Description
	Account_ServedIPGroupName, Account_ServingIPGroupName, Account_Username, Account_Password, Account_HostName, Account_Register, Account_ContactUser, Account_ApplicationType; [Account] For a detailed description of the table, see "Configuring Registration Accounts" on page 355.
Proxy Registration Parameters	
Proxy Name configure voip > sip-definition proxy-and-registration > proxy-name [ProxyName]	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. The valid value is a string of up to 49 characters. Note: The parameter functions together with the UseProxyIPasHost parameter.
Use Proxy IP as Host configure voip > sip-definition settings > use-proxy-ip-as-host [UseProxyIPasHost]	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. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable If the 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 Groups 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. Note: If the 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.
Redundancy Mode configure voip > sip-definition settings > redundancy-mode [ProxyRedundancyMode]	Determines whether the device switches back to the primary Proxy after using a redundant Proxy. <ul style="list-style-type: none"> ▪ [0] 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. ▪ [1] Homing = The device always tries to work with the primary Proxy server (i.e., switches back to the primary Proxy whenever it's available). Note: 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.
Proxy IP List Refresh Time configure voip > sip-definition settings > proxy-ip-lst-rfrsh-time [ProxyIPListRefreshTime]	Defines the time interval (in seconds) between each Proxy IP list refresh. The range is 5 to 2,000,000. The default interval is 60.
Always Use Proxy configure voip > sip-definition proxy-and-registration > always-	Determines whether the device sends SIP messages and responses through a Proxy server.

Parameter	Description
use-proxy [AlwaysSendToProxy]	<ul style="list-style-type: none"> ▪ [0] Disable = (Default) Use standard SIP routing rules. ▪ [1] Enable = All SIP messages and responses are sent to the Proxy server. <p>Note: The parameter is applicable only if a Proxy server is used (i.e., the parameter IsProxyUsed is set to 1).</p>
DNS Query Type configure voip > sip-definition settings > dns-query [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"> ▪ [0] A-Record = (Default) No NAPTR or SRV queries are performed. ▪ [1] SRV = If the Proxy/Registrar IP address parameter, Contact/Record-Route headers, or IP address configured 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. ▪ [2] NAPTR = 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>Note:</p> <ul style="list-style-type: none"> ▪ If the Proxy/Registrar IP address parameter, the domain name in the Contact/Record-Route headers, or the IP address configured in the routing tables contain a domain name with a port definition, the device performs a regular DNS A-record query. ▪ If a specific Transport Type is configured, a NAPTR query is not performed. ▪ To enable NAPTR/SRV queries for Proxy servers only, use the global parameter ProxyDNSQueryType, or use the Proxy Sets table.
Proxy DNS Query Type configure voip > sip-definition proxy-and-registration > proxy- dns-query [ProxyDNSQueryType]	<p>Global parameter that defines the DNS query record type for resolving the Proxy server's configured domain name (FQDN) into an IP address.</p> <ul style="list-style-type: none"> ▪ [0] A-Record (default) = A-record DNS query. ▪ [1] SRV = If 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. Thus, if the first SRV query returns two domain names and the A-record queries return two IP addresses each, no additional searches are performed. ▪ [2] NAPTR = NAPTR query is done. If successful, an SRV query is sent according to the information received in the NAPTR response. If the NAPTR query fails, an SRV query is done according to the configured transport type. If the Proxy IP address parameter contains a domain name with port definition (e.g., ProxyIP = domain.com:5080), the device performs a regular DNS A-record query. If a specific Transport

Parameter	Description
	<p>Type is defined, a NAPTR query is not performed.</p> <p>Note:</p> <ul style="list-style-type: none"> ▪ This functionality can be configured per Proxy Set in the Proxy Sets table (see "Configuring Proxy Sets" on page 341). ▪ When enabled, NAPTR/SRV queries are used to discover Proxy servers even if the parameter DNSQueryType is disabled.
<p>Use Gateway Name for OPTIONS</p> <p>configure voip > sip-definition settings > use-gw-name-for-opt [UseGatewayNameForOptions]</p>	<p>Determines whether the device uses its IP address or string name ("gateway name") in keep-alive SIP OPTIONS messages (host part of the Request-URI). To configure the "gateway name", use the SIPGatewayName parameter. The device uses the OPTIONS request as a keep-alive message with its primary and redundant SIP proxy servers (i.e., the EnableProxyKeepAlive parameter is set to 1).</p> <ul style="list-style-type: none"> ▪ [0] No = (Default) Device's IP address is used in keep-alive OPTIONS messages. ▪ [1] Yes = Device's "gateway name" is used in keep-alive OPTIONS messages. ▪ [2] Server = Device's IP address is used in the From and To headers in keep-alive OPTIONS messages.
<p>Password</p> <p>configure voip > sip-definition proxy-and-registration > password-4-auth [Password]</p>	<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>
<p>Cnonce</p> <p>configure voip > sip-definition proxy-and-registration > cnonce-4-auth [Cnonce]</p>	<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>
<p>Challenge Caching Mode</p> <p>configure voip > sip-definition settings > challenge-caching [SIPChallengeCachingMode]</p>	<p>Enables local caching of SIP message authorization challenges from Proxy servers.</p> <p>The device sends the first request to the Proxy without authorization. The Proxy sends a 401/407 response with a challenge for credentials. The device saves (caches) the response for further uses. The device sends a new request with the appropriate credentials. Subsequent requests to the Proxy are automatically sent with credentials (calculated from the saved challenge). If the Proxy doesn't accept the new request and sends another challenge, the old challenge is replaced with the new one. One of the benefits of the feature is that it may reduce the number of SIP messages transmitted through the network.</p> <ul style="list-style-type: none"> ▪ [0] None = (Default) Challenges are not cached. Every new request is sent without preliminary authorization. If the request is challenged, a new request with authorization data is sent. ▪ [1] INVITE Only = Challenges issued for INVITE requests are cached. This prevents a mixture of REGISTER and INVITE authorizations. ▪ [2] Full = Caches all challenges from the proxies.

Parameter	Description
	<p>Note:</p> <ul style="list-style-type: none"> ▪ Challenge caching is used with all proxies and not only with the active one. ▪ The challenge can be cached per Account or per user whose credentials are known through the User Info table.
Proxy Address Table	
Proxy IP Table configure voip > proxy-ip [ProxyIP]	The table defines proxy addresses per Proxy Set. The format of the ini file table parameter is as follows: [ProxyIP] FORMAT ProxyIp_Index = ProxyIp_ProxySetId, ProxyIp_ProxyIpIndex, ProxyIp_IpAddress, ProxyIp_TransportType; [\ProxyIP] For a description of the table, see "Configuring Proxy Sets" on page 341.
Proxy Sets Table	
Proxy Sets configure voip > proxy-set [ProxySet]	Defines the Proxy Sets. The format of the ini file table parameter is as follows: [ProxySet] FORMAT ProxySet_Index = ProxySet_ProxyName, ProxySet_EnableProxyKeepAlive, ProxySet_ProxyKeepAliveTime, ProxySet_ProxyLoadBalancingMethod, ProxySet_IsProxyHotSwap, ProxySet_SRDName, ProxySet_ClassificationInput, ProxySet_TLSContextName, ProxySet_ProxyRedundancyMode, ProxySet_DNSResolveMethod, ProxySet_KeepAliveFailureResp, ProxySet_GWIPv4SIPInterfaceName, ProxySet_SBCIPv4SIPInterfaceName, ProxySet_GWIPv6SIPInterfaceName, ProxySet_SBCIPv6SIPInterfaceName; [\ProxySet] For a description of the table, see "Configuring Proxy Sets" on page 341.
Registrar Parameters	
Registration Time configure voip > sip-definition proxy-and-registration > registration-time [RegistrationTime]	Defines the time interval (in seconds) for registering to a Proxy server. The value is used in the SIP Expires header. The parameter also defines the time interval between Keep-Alive messages when the parameter EnableProxyKeepAlive is set to 2 (REGISTER). Typically, the device registers every 3,600 sec (i.e., one hour). The device resumes registration according to the parameter RegistrationTimeDivider. The valid range is 10 to 2,000,000. The default is 180.
Re-registration Timing [%] configure voip > sip-definition settings > re-registration-timing [RegistrationTimeDivider]	Defines the re-registration timing (in percentage). The timing is a percentage of the re-register timing set by the Registrar server. The valid range is 50 to 100. The default is 50. For example: If the parameter is set to 70% and the Registration Expires time is 3600, the device re-sends its registration request

Parameter	Description
	<p>after 3600 x 70% (i.e., 2520 sec).</p> <p>Note: The parameter may be overridden if the parameter RegistrationTimeThreshold is greater than 0.</p>
<p>Registration Retry Time configure voip > sip-definition settings > registration-retry-time [RegistrationRetryTime]</p>	<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>
<p>Registration Time Threshold configure voip > sip-definition proxy-and-registration > registration-time-thres [RegistrationTimeThreshold]</p>	<p>Defines a threshold (in seconds) for re-registration timing. If the 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>
<p>ReRegister On Connection Failure configure voip > sip-definition settings > reg-on-conn-failure [ReRegisterOnConnectionFailure]</p>	<p>Enables the device to perform SIP re-registration upon TCP/TLS connection failure.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable
<p>configure voip > sip-definition settings > expl-un-reg [UnregistrationMode]</p>	<p>Enables the device to perform explicit unregisters.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable = 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. <p>Note: 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>
<p>Add Empty Authorization Header configure voip > sip-definition settings > add-empty-author-hdr [EmptyAuthorizationHeader]</p>	<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"> ▪ [0] Disable (default) ▪ [1] Enable <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"> ▪ username - set to the value of the private user identity ▪ realm - set to the domain name of the home network

Parameter	Description
	<ul style="list-style-type: none"> ▪ uri - set to the SIP URI of the domain name of the home network ▪ nonce - set to an empty value ▪ response - set to an empty value <p>For example:</p> <pre>Authorization: Digest username=alice_private@home1.net, realm="home1.net", nonce="", response="e56131d19580cd833064787ecc"</pre> <p>Note: This registration header is according to the IMS 3GPP TS24.229 and PKT-SP-24.220 specifications.</p>
<p>Add initial Route Header configure voip > sip-definition proxy-and-registration > add-init- rte-hdr [InitialRouteHeader]</p>	<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"> ▪ [0] Disable (default) ▪ [1] Enable <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: <sip:10.10.10.10;lr;transport=udp></pre> <p>or</p> <pre>Route: <sip: pcscf- gm.ims.rr.com;lr;transport=udp></pre>
<p>configure voip > sip-definition settings > ping-pong-keep-alive [UsePingPongKeepAlive]</p>	<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"> ▪ [0] Disable (default) ▪ [1] Enable <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 considers the flow failed.</p> <p>Note: 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.</p>

Parameter	Description
configure voip > sip-definition settings > ping-pong-keep-alive- time [PingPongKeepAliveTime]	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.
Max Generated Register Rate configure voip > sip-definition settings > max-gen-reg-rate [MaxGeneratedRegistersRate]	Defines the maximum number of user register requests (REGISTER messages) that the device sends (to a proxy or registrar server) at a user-defined rate configured by the GeneratedRegistersInterval parameter. The parameter is useful in that it may be used to prevent an overload on the device's CPU caused by sending many registration requests at a given time. The valid value is 30 to 300 register requests per second. The default is 150. For configuration examples, see the description of the GeneratedRegistersInterval parameter.
Generated Registers interval gen-reg-int [GeneratedRegistersInterval]	Defines the rate (in seconds) at which the device sends user register requests (REGISTER messages). The parameter is based on the maximum number of REGISTER messages that can be sent at this rate, configured by the MaxGeneratedRegistersRate parameter. The valid value is 1 to 5. The default is 1. Configuration examples: <ul style="list-style-type: none"> ▪ If you configure the MaxGeneratedRegistersRate parameter to 100 and the GeneratedRegistersInterval to 5, the device sends a maximum of 20 REGISTER messages per second (i.e., 100 messages divided by 5 sec; 100 per 5 seconds). ▪ If you configure the MaxGeneratedRegistersRate parameter to 100 and the GeneratedRegistersInterval to 1, the device sends a maximum of a 100 REGISTER messages per second.

55.7.2 Network Application Parameters

The SIP network application parameters are described in the table below.

Table 55-31: SIP Network Application Parameters

Parameter	Description
SRDs Table	
SRDs configure voip > srd [SRD]	Defines Signaling Routing Domains (SRD). The format of the ini file table parameter is as follows: [SRD] FORMAT SRD_Index = SRD_Name, SRD_IntraSRDMediaAnchoring, SRD_BlockUnRegUsers, SRD_MaxNumOfRegUsers, SRD_EnableUnAuthenticatedRegistrations, SRD_SharingPolicy, SRD_UsedByRoutingServer, SRD_SBCOperationMode,

Parameter	Description
	SRD_SBCRoutingPolicyName; [\SRD] For a detailed description of the table, see "Configuring SRDs" on page 311.
SIP Interfaces Table	
SIP Interfaces configure voip > sip- interface [SIPInterface]	Defines SIP Interfaces. The format of the ini file table parameter is as follows: [SIPInterface] FORMAT SIPInterface_Index = SIPInterface_InterfaceName, SIPInterface_NetworkInterface, SIPInterface_ApplicationType, SIPInterface_UDPPort, SIPInterface_TCPPort, SIPInterface_TLSPort, SIPInterface_SRDName, SIPInterface_MessagePolicyName, SIPInterface_TLSContext, SIPInterface_TLSMutualAuthentication, SIPInterface_TCPKeepaliveEnable, SIPInterface_ClassificationFailureResponseType, SIPInterface_PreClassificationManSet, SIPInterface_EncapsulatingProtocol, SIPInterface_MediaRealm, SIPInterface_SBCDirectMedia, SIPInterface_BlockUnRegUsers, SIPInterface_MaxNumOfRegUsers, SIPInterface_EnableUnAuthenticatedRegistrations, SIPInterface_UsedByRoutingServer; [\SIPInterface] For a detailed description of the table, see "Configuring SIP Interfaces" on page 321.
configure voip > sip- definition settings > tcp- keepalive-time [TCPKeepAliveTime]	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. Note: <ul style="list-style-type: none"> ▪ Simple ACKs such as keepalives are not considered data packets. ▪ TCP keepalive is enabled per SIP Interface in the SIP Interfaces table.
configure voip > sip-definition settings > tcp- keepalive-interval [TCPKeepAliveInterval]	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. Note: TCP keepalive is enabled per SIP Interface in the SIP Interfaces table.
configure voip > sip-definition settings > tcp- keepalive-retry [TCPKeepAliveRetry]	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. Note: TCP keepalive is enabled per SIP Interface in the SIP Interfaces table.
NAT Translation Table	
NAT Translation Table configure network > nat-translation [NATTranslation]	Defines NAT rules for translating source IP addresses per VoIP interface (SIP control and RTP media traffic) into NAT IP addresses. The format of the ini file table parameter is as follows: [NATTranslation] FORMAT NATTranslation_Index = NATTranslation_SrcIPInterfaceName,

Parameter	Description
	<p>NATTranslation_TargetIPAddress, NATTranslation_SourceStartPort, NATTranslation_SourceEndPort, NATTranslation_TargetStartPort, NATTranslation_TargetEndPort; [\NATTranslation]</p> <p>For a detailed description of the table, see "Configuring NAT Translation per IP Interface" on page 142.</p>
Media Realms table	
<p>Media Realms configure voip > realm [CpMediaRealm]</p>	<p>Defines Media Realms.</p> <p>The format of the ini file table parameter is as follows: [CpMediaRealm] FORMAT CpMediaRealm_Index = CpMediaRealm_MediaRealmName, CpMediaRealm_IPv4IF, CpMediaRealm_IPv6IF, CpMediaRealm_PortRangeStart, CpMediaRealm_MediaSessionLeg, CpMediaRealm_PortRangeEnd, CpMediaRealm_IsDefault, CpMediaRealm_QoeProfile, CpMediaRealm_BWProfile, CpMediaRealm_TopologyLocation; [\CpMediaRealm]</p> <p>For a detailed description of the table, see "Configuring Media Realms" on page 303.</p>
Remote Media Subnet Table	
<p>Remote Media Subnet configure voip > remote-media-subnet [SubRealm]</p>	<p>Defines Remote Media Subnets.</p> <p>The format of the ini file table parameter is as follows: [RemoteMediaSubnet] FORMAT RemoteMediaSubnet_Index = RemoteMediaSubnet_Realm, RemoteMediaSubnet_RemoteMediaSubnetIndex, RemoteMediaSubnet_RemoteMediaSubnetName, RemoteMediaSubnet_PrefixLength, RemoteMediaSubnet_AddressFamily, RemoteMediaSubnet_DstIPAddress, RemoteMediaSubnet_QOEProfileName, RemoteMediaSubnet_BWProfileName; [\RemoteMediaSubnet]</p> <p>For a detailed description of the table, see "Configuring Remote Media Subnets" on page 306.</p>
Media Realm Extension Table	
<p>Media Realm Extension configure voip > realm-extension [MediaRealmExtension]</p>	<p>Defines Media Realm Extensions.</p> <p>The format of the ini file table parameter is as follows: [MediaRealmExtension] FORMAT MediaRealmExtension_Index = MediaRealmExtension_MediaRealmIndex, MediaRealmExtension_ExtensionIndex, MediaRealmExtension_IPv4IF, MediaRealmExtension_IPv6IF, MediaRealmExtension_PortRangeStart, MediaRealmExtension_PortRangeEnd, MediaRealmExtension_MediaSessionLeg; [\MediaRealmExtension]</p> <p>For a detailed description of the table, see "Configuring Media Realm Extensions" on page 309.</p>

55.8 General SIP Parameters

The general SIP parameters are described in the table below.

Table 55-32: General SIP Parameters

Parameter	Description
Send reject on overload configure voip > sip- definition settings > reject-on-ovrld [SendRejectOnOverload]	<p>Disables the sending of SIP 503 (Service Unavailable) responses upon receipt of new SIP dialog-initiating requests when the device's CPU is overloaded and thus, unable to accept and process new SIP messages.</p> <ul style="list-style-type: none"> ▪ [0] Disable = No SIP 503 response is sent when CPU overloaded. ▪ [1] Enable (default) = SIP 503 response is sent when CPU overloaded. ▪ Note: Even if the parameter is disabled (i.e., 503 is not sent), the device still discards the new SIP dialog-initiating requests when the CPU is overloaded.
SIP 408 Response upon non-INVITE configure voip > sip- definition settings > enbl- non-inv-408 [EnableNonInvite408Rep ly]	<p>Enables the device to send SIP 408 responses (Request Timeout) upon receipt of non-INVITE transactions. Disabling this response complies with RFC 4320/4321. By default, and in certain circumstances such as a timeout expiry, the device sends a SIP 408 Request Timeout in response to non-INVITE requests (e.g., REGISTER).</p> <ul style="list-style-type: none"> ▪ [0] Disable = SIP 408 response is not sent upon receipt of non-INVITE messages (to comply with RFC 4320). ▪ [1] Enable = (Default) SIP 408 response is sent upon receipt of non-INVITE messages, if necessary.
Remote Management by SIP Notify configure voip > sip- definition settings > sip- remote-reset [EnableSIPRemoteReset]	<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"> ▪ [0] Disable (default) ▪ [1] Enable <p>The action depends on the Event header value:</p> <ul style="list-style-type: none"> ▪ 'check-sync;reboot=false': triggers the regular Automatic Update feature (if Automatic Update has been enabled on the device) ▪ 'check-sync;reboot=true': triggers a device reset <p>Note: The Event header value is proprietary to AudioCodes.</p>
Max SIP Message Length [KB] [MaxSIPMessageLength]	<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 100. The default is 100.</p>
[SIPForceRport]	<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"> ▪ [0] = (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. ▪ [1] = 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.
Reject Cancel after Connect configure voip > sip-	<p>Enables or disables the device to accept or reject SIP CANCEL requests received after the receipt of a 200 OK in response to an INVITE (i.e., call established). According to the SIP standard, a CANCEL can be sent only during the INVITE transaction (before 200 OK), and once a 200 OK</p>

Parameter	Description
definition settings > reject-cancel-after- connect [RejectCancelAfterConnect]	response is received the call can be rejected only by a BYE request. <ul style="list-style-type: none"> ▪ [0] Disable = (Default) Accepts a CANCEL request received during the INVITE transaction by sending a 200 OK response and terminates the call session. ▪ [1] Enable = Rejects a CANCEL request received during the INVITE transaction by sending a SIP 481 (Call/Transaction Does Not Exist) response and maintains the call session.
Verify Received RequestURI configure voip > sip- definition settings > verify-rcvd-requiri [VerifyReceeedRequestUri]	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. <ul style="list-style-type: none"> ▪ [0] Disable = (Default) Even if the user is different, the device accepts the SIP request. ▪ [1] 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).
Max Number of Active Calls configure voip > sip- definition settings > max- nb-of--act-calls [MaxActiveCalls]	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. The valid range is 1 to the maximum number of supported channels. The default value is the maximum available channels (i.e., no restriction on the maximum number of calls).
QoS statistics in SIP Release Call configure voip > sip-definition settings > qos- statistics-in- release-msg [QoSStatistics]	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. <ul style="list-style-type: none"> ▪ [0] = Disable (default) ▪ [1] = Enable The X-RTP-Stat header provides the following statistics: <ul style="list-style-type: none"> ▪ Number of received and sent voice packets ▪ Number of received and sent voice octets ▪ Received packet loss, jitter (in ms), and latency (in ms) The X-RTP-Stat header contains the following fields: <ul style="list-style-type: none"> ▪ PS=<voice packets sent> ▪ OS=<voice octets sent> ▪ PR=<voice packets received> ▪ OR=<voice octets received> ▪ PL=<receive packet loss> ▪ JI=<jitter in ms> ▪ LA=<latency in ms> Below is an example of the X-RTP-Stat header in a SIP BYE message: <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: <sip:401@10.33.4.126;user=phone>;tag=1c2113553324 To: <sip:302@company.com>;tag=1c991751121 Call-ID: 991750671245200001912@10.33.4.125 CSeq: 1 BYE </pre>

Parameter	Description
	<p>X-RTP-Stat: PS=207;OS=49680;;PR=314;OR=50240;PL=0;JI=600;LA=40; 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.7.20A.000.038 Reason: Q.850 ;cause=16 ;text="local" Content-Length: 0</p>
PRACK Mode prack-mode [PrackMode]	Determines the PRACK (Provisional Acknowledgment) mechanism mode for SIP 1xx reliable responses. <ul style="list-style-type: none"> ▪ [0] Disable ▪ [1] Supported (default) ▪ [2] Required <p>Note:</p> <ul style="list-style-type: none"> ▪ The Supported and Required headers contain the '100rel' tag. ▪ The device sends PRACK messages if 180/183 responses are received with '100rel' in the Supported or Required headers.
Enable Early Media early-media [EnableEarlyMedia]	Global parameter enabling the Early Media feature for sending media (e.g., ringing) before the call is established. You can also configure this functionality per specific calls, using IP Profiles (IpProfile_EnableEarlyMedia). For a detailed description of the parameter and for configuring the functionality, see "Configuring IP Profiles" on page 388. <p>Note: If the functionality is configured for a specific profile, the settings of the global parameter is ignored for calls associated with the profile.</p>
Session Expires Disconnect Time [SessionExpiresDisconnectTime]	Defines a session expiry timeout. The device disconnects the session (sends a SIP BYE) if the refresher did not send a refresh request before one-third (1/3) of the session expires time, or before the time configured by the parameter (the minimum of the two). The valid range is 0 to 32 (in seconds). The default is 32.
[RemoveToTagInFailureResponse]	Determines whether the device removes the 'to' header tag from final SIP failure responses to INVITE transactions. <ul style="list-style-type: none"> ▪ [0] = (Default) Do not remove tag. ▪ [1] = Remove tag.
[EnableRTCPAttribute]	Enables the use of the 'rtcp' attribute in the outgoing SDP. <ul style="list-style-type: none"> ▪ [0] = Disable (default) ▪ [1] = Enable
[OPTIONSUserPart]	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. A special value is 'empty', indicating that no user part in the Request-URI (host part only) is used. The valid range is a 30-character string. By default, this value is not defined.
Fax Signaling Method	Global parameter defining the SIP signaling method for establishing and transmitting a fax session when the device detects a fax.

Parameter	Description
fax-sig-method [IsFaxUsed]	<p>You can also configure this functionality per specific calls, using IP Profiles (IpProfile_IsFaxUsed). For a detailed description of the parameter, see "Configuring IP Profiles" on page 388.</p> <p>Note: If this functionality is configured for a specific IP Profile or Tel Profile, the settings of this global parameter is ignored for calls associated with the IP Profile or Tel Profile.</p>
fax-vbd-behvr [FaxVBDBehavior]	<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"> ▪ [0] = (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). ▪ [1] = 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 upon fax detection. If the remote party supports T.38, the fax is relayed over T.38. <p>Note:</p> <ul style="list-style-type: none"> ▪ 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. ▪ This feature can be used only if the remote party supports T.38 fax relay; otherwise, the fax fails.
[NoAudioPayloadType]	<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 style="background-color: #f0f0f0; padding: 5px;">a=rtptime:120 NoAudio/8000\r\n</pre> <p>Note: For incoming SDP offers, NoAudio is always supported.</p>
SIP Transport Type configure voip > sip- definition settings > app- sip-transport-type [SIPTransportType]	<p>Determines the default transport layer for outgoing SIP calls initiated by the device.</p> <ul style="list-style-type: none"> ▪ [0] UDP (default) ▪ [1] TCP ▪ [2] TLS (SIPS) <p>Note:</p> <ul style="list-style-type: none"> ▪ It's recommended to use TLS for communication with a SIP Proxy and not for direct device-to-device communication. ▪ For received calls (i.e., incoming), the device accepts all these protocols.
Display Default SIP Port configure voip > sip- definition settings > display-default-sip-port [DisplayDefaultSIPPort]	<p>Enables the device to add the default SIP port 5060 (UDP/TCP) or 5061 (TLS) to outgoing messages that are received without a port. This condition also applies to manipulated messages where the resulting message has no port number. The device adds the default port number to the following SIP headers: Request-Uri, To, From, P-Asserted-Identity, P-Preferred-Identity, and P-Called-Party-ID. If the message is received with a port number other than the default, for example, 5070, the port number is not changed.</p>

Parameter	Description
	<p>An example of a SIP From header with the default port is shown below:</p> <pre data-bbox="533 300 1385 389">From: <sip:+4000@10.8.4.105:5060;user=phone>;tag=f25419a96a;epid=009FAB8F3E</pre> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable
Enable SIPS configure voip > sip- definition settings > enable-sips [EnableSIPS]	<p>Enables secured SIP (SIPS URI) connections over multiple hops.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable <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>Note: If the parameter is enabled and the parameter SIPTransportType is set to 0 (i.e., UDP), the connection fails.</p>
TCP/TLS Connection Reuse tcp-conn-reuse [EnableTCPConnectionR euse]	<p>Enables the reuse of an established TCP or TLS connection between the device and a SIP user agent (UA) for subsequent SIP requests sent to the UA. Any new out-of-dialog requests (e.g., INVITE or REGISTER) use the same secured connection. One of the benefits of enabling the parameter is that it may improve performance by eliminating the need for additional TCP/TLS handshakes with the UA, allowing sessions to be established rapidly.</p> <ul style="list-style-type: none"> ▪ [0] Disable = The device uses a new TCP or TLS connection with the UA. ▪ [1] Enable = (Default) The device uses the same TCP or TLS connection for all SIP requests with the UA. <p>Note: For SIP responses, the device always uses the same TCP/TLS connection, regardless of the parameter settings.</p>
Fake TCP alias configure voip > sip- definition settings > fake- tcp-alias [FakeTCPalias]	<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"> ▪ [0] Disable = (Default) TCP/TLS connection reuse is done only if the "alias" parameter is present in the Via header of the first INVITE. ▪ [1] Enable <p>Note: To enable TCP/TLS connection re-use, set the EnableTCPConnectionReuse parameter to 1.</p>
Reliable Connection Persistent Mode configure voip > sip- definition settings > reliable-conn-persistent [ReliableConnectionPersi stentMode]	<p>Enables setting of all TCP/TLS connections as persistent and therefore, not released.</p> <ul style="list-style-type: none"> ▪ [0] = (Default) Disable. All TCP connections (except those that are set to a proxy IP) are released if not used by any SIP dialog\transaction. ▪ [1] = Enable - TCP connections to all destinations are persistent and not released unless the device reaches 70% of its maximum TCP resources. <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</p>

Parameter	Description
	to establish security associations, in addition to the initial TCP connection set up. Note: If the destination is a Proxy server, the TCP/TLS connection is persistent regardless of the settings of the parameter.
TCP Timeout configure voip > sip- definition settings > tcp- timeout [SIPTCPTimeout]	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. The valid range is 0 to 40 sec. The default is 64 * SipT1Rtx parameter value. For example, if SipT1Rtx is set to 500 msec, then the default of SIPTCPTimeout is 32 sec.
SIP Destination Port configure voip > sip- definition settings > sip- dst-port [SIPDestinationPort]	Defines the SIP destination port for sending initial SIP requests. The valid range is 1 to 65534. The default port is 5060. Note: SIP responses are sent to the port specified in the Via header.
Use user=phone in SIP URL configure voip > sip- definition settings > user=phone-in-url [IsUserPhone]	Determines whether the 'user=phone' string is added to the SIP URI and SIP To header. <ul style="list-style-type: none"> [0] No = 'user=phone' string is not added. [1] Yes = (Default) 'user=phone' string is part of the SIP URI and SIP To header.
Use user=phone in From Header configure voip > sip- definition settings > phone-in-from-hdr [IsUserPhoneInFrom]	Determines whether the 'user=phone' string is added to the From and Contact SIP headers. <ul style="list-style-type: none"> [0] No = (Default) Doesn't add 'user=phone' string. [1] Yes = 'user=phone' string is part of the From and Contact headers.
Use Tel URI for Asserted Identity configure voip > sip- definition settings > uri- for-assert-id [UseTelURIForAssertedI D]	Determines the format of the URI in the P-Asserted-Identity and P-Preferred-Identity headers. <ul style="list-style-type: none"> [0] Disable = (Default) 'sip:' [1] Enable = 'tel:'
Enable GRUU configure voip > sbc settings > enable-gruu [EnableGRUU]	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. <ul style="list-style-type: none"> [0] Disable (default) [1] Enable <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</pre>

Parameter	Description
	<p>To: sip:C@domain.com Refer-To: (URI that identifies B's UA)</p> <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"> ▪ 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"> ✓ If the REGISTER is per the device's client (endpoint), it is the MAC address concatenated with the phone number of the client. ✓ If the REGISTER is per device, it is the MAC address only. ✓ 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. <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. The 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"> ▪ 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.
[IsCiscoSCEMode]	<p>Determines whether a Cisco gateway exists at the remote side.</p> <ul style="list-style-type: none"> ▪ [0] = (Default) No Cisco gateway exists at the remote side. ▪ [1] = A Cisco gateway exists at the remote side. <p>When a Cisco gateway exists at the remote side, the device must set the value of the 'annexb' parameter of the fntp attribute in the SDP to '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>Note: The IsCiscoSCEMode parameter is applicable only when the selected coder is G.729.</p>
User-Agent Information configure voip > sip- definition settings > user- agent-info [UserAgentDisplayInfo]	<p>Defines the string that is used in the SIP User-Agent and Server response headers. When configured, the string <UserAgentDisplayInfo value>/software version' is used, for example:</p> <pre>User-Agent: myproduct/v.7.20A.000.038</pre> <p>If not configured, the default string, <AudioCodes product-name>/software version' is used, for example:</p> <pre>User-Agent: Audiocodes-Sip-Gateway-Mediant Software SBC/v.7.20A.000.038</pre> <p>The maximum string length is 50 characters.</p>

Parameter	Description
	<p>Note: 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>
SDP Session Owner configure voip > sip- definition settings > sdp- session-owner [SIPSDPSessionOwner]	<p>Defines the value of the Owner line ('o' field) in outgoing SDP messages. 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>
configure voip > sip- definition settings > sdp- ver-nego [EnableSDPVersionNegotiation]	<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"> ▪ [0] Disable = (Default) The device negotiates any new SDP re-offer, regardless of the origin field. ▪ [1] Enable = The device negotiates only an SDP re-offer with an incremented origin field.
Subject configure voip > sip- definition settings > usr- def-subject [SIPSubject]	<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>
Multiple Packetization Time Format configure voip > sip- definition settings > mult- ptime-format [MultiPtimeFormat]	<p>Determines whether the 'mptime' attribute is included in the outgoing SDP.</p> <ul style="list-style-type: none"> ▪ [0] None = (Default) Disabled. ▪ [1] PacketCable = Includes the 'mptime' attribute in the outgoing SDP - PacketCable-defined format. <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 the 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>
configure voip > sip- definition settings > enable-ptime [EnablePtime]	<p>Determines whether the 'ptime' attribute is included in the SDP.</p> <ul style="list-style-type: none"> ▪ [0] = Remove the 'ptime' attribute from SDP. ▪ [1] = (Default) Include the 'ptime' attribute in SDP.
3xx Behavior 3xx-behavior [3xxBehavior]	<p>Determines the device's behavior regarding call identifiers when a 3xx response is received for an outgoing INVITE request. The device can use the same call identifiers (Call-ID, To, and From tags) or change them in the new initiated INVITE.</p>

Parameter	Description
	<ul style="list-style-type: none"> ▪ [0] Forward = (Default) Use different call identifiers for a redirected INVITE message. ▪ [1] Redirect = Use the same call identifiers in the new INVITE as the original call.
Enable P-Charging Vector p-charging-vector [EnablePChargingVector]	Enables the inclusion of the P-Charging-Vector header to all outgoing INVITE messages. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable
Retry-After Time configure voip > sip- definition settings > retry- aftr-time [RetryAfterTime]	Defines the time (in seconds) used in the Retry-After header when a 503 (Service Unavailable) response is generated by the device. The time range is 0 to 3,600. The default is 0.
Fake Retry After fake-retry-after [FakeRetryAfter]	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 the parameter. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ Any positive value (in seconds) for defining the period 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. 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. 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.
Enable P-Associated-URI Header p-associated-uri-hdr [EnablePAssociatedURI Header]	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. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable Note: P-Associated-URIs in registration responses is handled only if the device is registered per endpoint (using the User Information file).
Source Number Preference configure voip > sip- definition settings > src- nb-preference [SourceNumberPreference]	Determines from which SIP header the source (calling) number is obtained in incoming INVITE messages. <ul style="list-style-type: none"> ▪ If not configured or if any string other than "From" or "Pai2" is configured, the calling number is obtained from a specific header using the following logic: <ol style="list-style-type: none"> a. P-Preferred-Identity header. b. If the above header is not present, then the first P-Asserted-Identity header is used. c. If the above header is not present, then the Remote-Party-ID header is used. d. If the above header is not present, then the From header is used. ▪ "From" = The calling number is obtained from the From header.

Parameter	Description
	<ul style="list-style-type: none"> ▪ "Pai2" = The calling number is obtained using the following logic: <ol style="list-style-type: none"> a. If a P-Preferred-Identity header is present, the number is obtained from it. 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. c. If only one P-Asserted-Identity header is present, the calling number is obtained from it. <p>Note:</p> <ul style="list-style-type: none"> ▪ The "From" and "Pai2" values are not case-sensitive. ▪ 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.
Enable Reason Header configure voip > sip- definition settings > reason-header [EnableReasonHeader]	Enables the usage of the SIP Reason header. <ul style="list-style-type: none"> ▪ [0] Disable ▪ [1] Enable (default)
Gateway Name configure voip > sip- definition settings > gw- name [SIPGatewayName]	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>Note:</p> <ul style="list-style-type: none"> ▪ Ensure that the parameter value is the one with which the Proxy has been configured with to identify the device. ▪ The parameter can also be configured for an IP Group (in the IP Groups table).
configure voip > sip- definition settings > zero- sdp-behavior [ZeroSDPHandling]	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"). <ul style="list-style-type: none"> ▪ [0] = (Default) Sets the IP address of the outgoing SDP's c= field to 0.0.0.0. ▪ [1] = 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=recvnly" line.
Enable Delayed Offer configure voip > sip- definition settings > delayed-offer [EnableDelayedOffer]	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.) <ul style="list-style-type: none"> ▪ [0] Disable = (Default) The device sends the initial INVITE message with an SDP. ▪ [1] Enable = The device sends the initial INVITE message without an SDP.
configure voip > sip-definition settings > crypto- life-time-in-sdp [DisableCryptoLifeTimeIn]	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:hhQe10yZRcRcpIFPkH5xYY9R1de37ogh9G1MpvNp 2^31", it removes the lifetime parameter "2^31".

Parameter	Description
SDP]	<ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable
Enable Contact Restriction contact-restriction [EnableContactRestriction]	Determines whether the device sets the Contact header of outgoing INVITE requests to 'anonymous' for restricted calls. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable
configure voip > sip-definition settings > use- aor-in-refer-to- header [UseAORInReferToHeader]	Defines the source for the SIP URI set in the Refer-To header of outgoing REFER messages. <ul style="list-style-type: none"> ▪ [0] = (Default) Use SIP URI from Contact header of the initial call. ▪ [1] = Use SIP URI from To/From header of the initial call.
Enable User-Information Usage configure voip > sip- definition settings > user- inf-usage [EnableUserInfoUsage]	Enables the usage of the User Information, which is loaded to the device in the User Information Auxiliary file. For more information on User Information, see "User Information File" on page 593. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable Note: For the parameter to take effect, a device reset is required.
configure voip > sip-definition settings > handle- reason-header [HandleReasonHeader]	Determines whether the device uses the value of the incoming SIP Reason header for Release Reason mapping. <ul style="list-style-type: none"> ▪ [0] = Disregard Reason header in incoming SIP messages. ▪ [1] = (Default) Use the Reason header value for Release Reason mapping.
[EnableSilenceSupplnSDP]	Determines the device's behavior upon receipt of SIP Re-INVITE messages that include the SDP's 'silencesupp:off' attribute. <ul style="list-style-type: none"> ▪ [0] = (Default) Disregard the 'silecesupp' attribute. ▪ [1] = 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. Note: The parameter is applicable only if the G.711 coder is used.
configure voip > sip-definition settings > rport- support [EnableRport]	Enables the usage of the 'rport' parameter in the Via header. <ul style="list-style-type: none"> ▪ [0] = Disabled (default) ▪ [1] = Enabled 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>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.</p> <p>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</p>

Parameter	Description
	destination port of the response is the port indicated in the 'rport' parameter.
configure voip > sip-definition settings > x-channel-header [XChannelHeader]	Enables the device to add the SIP X-Channel header to outgoing SIP messages. The header provides information on the physical channel on which the call is received or sent. <ul style="list-style-type: none"> ▪ [0] Disable = (Default) X-Channel header is not used. ▪ [1] Enable = X-Channel header is generated by the device and sent in SIP INVITE requests and 180, 183, and 200 OK responses. The header includes the channel and the device's IP address, using the following syntax: <pre>x-channel: ds/ds1- /<channel>;IP=<device's IP address></pre> For example, the below shows a call on channel 4 of the device with IP address 192.168.13.1: <pre>x-channel: ds/ds1-1/4;IP=192.168.13.1</pre>
[EnableRekeyAfter181]	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). <ul style="list-style-type: none"> ▪ [0] = Disable (default) ▪ [1] = Enable Note: The parameter is applicable only if SRTP is used.
configure voip > sip-definition settings > number-of-active-dialogs [NumberOfActiveDialogs]	Defines the maximum number of concurrent, outgoing SIP REGISTER dialogs. The parameter is used to control the registration rate. The valid range is 1 to 20. The default is 20. Note: <ul style="list-style-type: none"> ▪ Once a 200 OK is received in response to a REGISTER message, the REGISTER message is not considered in this maximum count limit. ▪ The parameter applies only to outgoing REGISTER messages (i.e., incoming is unlimited).
Network Node ID configure voip > sip-definition settings > net-node-id [NetworkNodeId]	Defines the Network Node Identifier of the device for Avaya UCID. The valid value range is 1 to 0x7FFF. The default is 0. Note: <ul style="list-style-type: none"> ▪ To use this feature, you must set the parameter to any value other than 0. ▪ To enable the generation by the device of the Avaya UCID value and adding it to the outgoing INVITE sent to the IP Group (Avaya entity), use the IP Groups table's parameter 'UUI Format'.
Enable Microsoft Extension configure voip > sip-definition settings > microsoft-ext [EnableMicrosoftExt]	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. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable 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

Parameter	Description
	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., e622125519100 104). 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.
<pre>configure voip > sip-definition settings > sip- uri-for-diversion- header [UseSIPURIForDiversion Header]</pre>	Defines the URI format in the SIP Diversion header. <ul style="list-style-type: none"> ▪ [0] = 'tel:' (default) ▪ [1] = 'sip:'
<pre>configure voip > sip-definition settings > 100-to- 18x-timeout [TimeoutBetween100And 18x]</pre>	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. The valid range is 0 to 180,000 (i.e., 3 minutes). The default is 32000 (i.e., 32 sec).
<pre>configure voip > sip-definition settings > ignore- remote-sdp-mki [IgnoreRemoteSDPMKI]</pre>	Determines whether the device ignores the Master Key Identifier (MKI) if present in the SDP received from the remote side. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable
<pre>configure voip > sip- definition settings > sdp- ecan-frmt [SDPEcanFormat]</pre>	Defines the echo canceller format in the outgoing SDP. The 'ecan' attribute is used in the SDP to indicate the use of echo cancellation. <ul style="list-style-type: none"> ▪ [0] = (Default) The 'ecan' attribute appears on the 'a=gpmrd' line. ▪ [1] = The 'ecan' attribute appears as a separate attribute. ▪ [2] = The 'ecan' attribute is not included in the SDP. ▪ [3] = The 'ecan' attribute and the 'vbd' parameter are not included in the SDP. <p>Note: The 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>
<pre>First Call Ringback Tone ID configure voip > sip- definition settings > 1st- call-rbt-id [FirstCallRBtId]</pre>	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 the parameter). The valid range is -1 to 1,000. The default is -1 (i.e., play standard ringback tone). <p>Note:</p> <ul style="list-style-type: none"> ▪ It is assumed that all ringback tones are defined in sequence in the CPT file. ▪ In case of an MLPP call, the device uses the value of the 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).

Parameter	Description
Media IP Version Preference media-ip-ver-pref [MediaIPVersionPreference]	Global parameter that defines the preferred RTP media IP addressing version (IPv4 or IPv6) for outgoing SIP calls. You can also configure this functionality per specific calls, using IP Profiles (IpProfile_MediaIPVersionPreference). For a detailed description of the parameter and for configuring this functionality in the IP Profiles table, see Configuring IP Profiles on page 388.
WebSocket Keep-Alive Period configure voip > sip-definition settings > websocket-keepalive [WebSocketProtocolKeepAlivePeriod]	<p>Defines how often (in seconds) the device sends ping messages (keep alive) to check whether the WebSocket session with the Web client is still connected.</p> <p>The valid value is 5 to 2000000. The default is 0 (i.e., ping messages are not sent).</p> <p>For more information on WebSocket, see SIP over WebSocket on page 526.</p> <p>Note: The device always replies to WebSocket ping control messages with pong messages.</p>
Retransmission Parameters	
SIP T1 Retransmission Timer configure voip > sip-definition settings > t1-re-tx-time [SipT1Rtx]	<p>Defines the time interval (in msec) between the first transmission of a SIP message and the first retransmission of the same message.</p> <p>The default is 500.</p> <p>Note: 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"> ▪ The first retransmission is sent after 500 msec. ▪ The second retransmission is sent after 1000 (2*500) msec. ▪ The third retransmission is sent after 2000 (2*1000) msec. ▪ The fourth retransmission and subsequent retransmissions until SIPMaxRtx are sent after 4000 (2*2000) msec.
SIP T2 Retransmission Timer configure voip > sip-definition settings > t2-re-tx-time [SipT2Rtx]	<p>Defines the maximum interval (in msec) between retransmissions of SIP messages (except for INVITE requests).</p> <p>The default is 4000.</p> <p>Note: The time interval between subsequent retransmissions of the same SIP message starts with SipT1Rtx and is multiplied by two until SipT2Rtx.</p>
SIP Maximum RTX configure voip > sip-definition settings > sip-max-rtx [SIPMaxRtx]	<p>Defines the maximum number of UDP transmissions of SIP messages (first transmission plus retransmissions).</p> <p>The range is 1 to 30. The default is 7.</p>
Number of RTX Before Hot-Swap configure voip > sip-definition proxy-and-registration > nb-of-rtx-b4-hot-swap [HotSwapRtx]	<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>For example, if configured to 3 and no response is received from an IP destination, the device attempts another three times to send the call to the IP destination. If still unsuccessful, it attempts to redirect the call to another IP destination.</p>

Parameter	Description
	Note: The parameter is also used for alternative routing (see Alternative Routing Based on IP Connectivity).
SIP Message Manipulations Table	
Message Manipulations configure voip > message message-manipulations [MessageManipulations]	Defines manipulation rules for SIP header messages. The format of the ini file table parameter is as follows: [MessageManipulations] FORMAT MessageManipulations_Index = MessageManipulations_ManSetID, MessageManipulations_MessageType, MessageManipulations_Condition, MessageManipulations_ActionSubject, MessageManipulations_ActionType, MessageManipulations_ActionValue, MessageManipulations_RowRole; [/MessageManipulations] For example, the below configuration changes the user part of the SIP From header to 200: MessageManipulations 1 = 0, Invite.Request, , Header.From.Url.User, 2, 200, 0; For a detailed description of the table, see Configuring SIP Message Manipulation on page 362.
Message Policies Table	
Message Policies configure voip > message message-policy [MessagePolicy]	Defines SIP message policy rules for blocking (blacklist) unwanted incoming SIP messages or allowing (whitelist) receipt of desired messages. The format of the ini file table parameter is as follows: [MessagePolicy] FORMAT MessagePolicy_Index = MessagePolicy_Name, MessagePolicy_MaxMessageLength, MessagePolicy_MaxHeaderLength, MessagePolicy_MaxBodyLength, MessagePolicy_MaxNumHeaders, MessagePolicy_MaxNumBodies, MessagePolicy_SendRejection, MessagePolicy_MethodList, MessagePolicy_MethodListType, MessagePolicy_BodyList, MessagePolicy_BodyListType, MessagePolicy_UseMaliciousSignatureDB; [/MessagePolicy] For a detailed description of the table, see Configuring SIP Message Policy Rules.
configure voip > sip- definition settings > message-policy-reject- response-type [MessagePolicyRejectResponse]	Defines the SIP response code that the device sends when it rejects an incoming SIP message due to a matched Message Policy in the Message Policies table, whose 'Send Reject' (MessagePolicy_SendRejection) parameter is configured to Policy Reject [0]. The default is 400 "Bad Request". To configure Message Policies, see Configuring SIP Message Policy Rules.

55.9 Coders and Profile Parameters

The profile parameters are described in the table below.

Table 55-33: Profile Parameters

Parameter	Description
Coder Groups Table	
Coder Groups configure voip > coders- and-profiles audio-coders- groups [AudioCodersGroups] [AudioCoders]	Defines the device's coders. Each group can consist of up to 10 coders. The first Coder Group is the default coder list and the default Coder Group. The format of the ini file table parameter is as follows: [AudioCodersGroups] FORMAT AudioCodersGroups_Index = AudioCodersGroups_Name; [\AudioCodersGroups] [AudioCoders] FORMAT AudioCoders_Index = AudioCoders_AudioCodersGroupId, AudioCoders_AudioCodersIndex, AudioCoders_Name, AudioCoders_pTime, AudioCoders_rate, AudioCoders_PayloadType, AudioCoders_Sce, AudioCoders_CoderSpecific; [\AudioCoders] Note: For a list of supported coders and for configuring Coder Groups, see "Configuring Coder Groups" on page 379.
IP Profiles Table	
IP Profiles configure voip > coders- and-profiles ip-profile [IPProfile]	Defines the IP Profiles table. The format of the ini file table parameter is as follows: [IPProfile] FORMAT IpProfile_Index = IpProfile_ProfileName, IpProfile_IpPreference, IpProfile_CodersGroupName, 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_SBCExtensionCodersGroupName, IpProfile_MediaIPVersionPreference, IpProfile_TranscodingMode, IpProfile_SBCAllowedMediaTypes, IpProfile_SBCAllowedAudioCodersGroupName, IpProfile_SBCAllowedVideoCodersGroupName, 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_SBCFaxCodersGroupName, IpProfile_SBCFaxBehavior, IpProfile_SBCFaxOfferMode, IpProfile_SBCFaxAnswerMode, IpProfile_SbcPrackMode, IpProfile_SBCSessionExpiresMode,

Parameter	Description
	IpProfile_SBCRemoteUpdateSupport, IpProfile_SBCRemoteReinviteSupport, IpProfile_SBCRemoteDelayedOfferSupport, IpProfile_SBCRemoteReferBehavior, IpProfile_SBCRemote3xxBehavior, IpProfile_SBCRemoteMultiple18xSupport, IpProfile_SBCRemoteEarlyMediaResponseType, IpProfile_SBCRemoteEarlyMediaSupport, IpProfile_EnableSymmetricMKI, IpProfile_MKISize, IpProfile_SBCEnforceMKISize, IpProfile_SBCRemoteEarlyMediaRTP, IpProfile_SBCRemoteSupportsRFC3960, IpProfile_SBCRemoteCanPlayRingback, IpProfile_EnableEarly183, IpProfile_EarlyAnswerTimeout, IpProfile_SBC2833DTMFPayloadType, IpProfile_SBCUserRegistrationTime, IpProfile_ResetSRTPStateUponRekey, IpProfile_AmdMode, IpProfile_SBCReliableHeldToneSource, IpProfile_GenerateSRTPKeys, IpProfile_SBCPlayHeldTone, IpProfile_SBCRemoteHoldFormat, IpProfile_SBCRemoteReplacesBehavior, IpProfile_SBCSDPtimeAnswer, IpProfile_SBCPreferredPTime, IpProfile_SBCUseSilenceSupp, IpProfile_SBCRTPRedundancyBehavior, IpProfile_SBCPlayRBTTToTransferee, IpProfile_SBCRTCPMode, IpProfile_SBCJitterCompensation, IpProfile_SBCRemoteRenegotiateOnFaxDetection, IpProfile_JitterBufMaxDelay, IpProfile_SBCUserBehindUdpNATRegistrationTime, IpProfile_SBCUserBehindTcpNATRegistrationTime, IpProfile_SBCSDPHandleRTCPAttribute, IpProfile_SBCRemoveCryptoLifetimeInSDP, IpProfile_SBCIceMode, IpProfile_SBCRTCPMux, IpProfile_SBCMediaSecurityMethod, IpProfile_SBCHandleXDetect, IpProfile_SBCRTCPFeedback, IpProfile_SBCRemoteRepresentationMode, IpProfile_SBCKeepVIAHeaders, IpProfile_SBCKeepRoutingHeaders, IpProfile_SBCKeepUserAgentHeader, IpProfile_SBCRemoteMultipleEarlyDialogs, IpProfile_SBCRemoteMultipleAnswersMode, IpProfile_SBCDirectMediaTag, IpProfile_SBCAdaptRFC2833BWTtoVoiceCoderBW, IpProfile_SBCMaxCallDuration, IpProfile_SBCGenerateRTP, IpProfile_SBCISUPBodyHandling, IpProfile_SBCVoiceQualityEnhancement; [IPProfile] For a description of the table, see "Configuring IP Profiles" on page 388.

55.10 Channel Parameters

This subsection describes the device's channel parameters.

55.10.1 Voice Parameters

The voice parameters are described in the table below.

Table 55-34: Voice Parameters

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

Parameter	Description
Input Gain configure voip > media voice > input-gain [InputGain]	Global parameter defining the pulse-code modulation (PCM) input (received) gain control level (in decibels). You can also configure the functionality per specific calls, using IP Profiles (IpProfile_InputGain). For a detailed description of the parameter and for configuring the functionality, see "Configuring IP Profiles" on page 388. Note: If the functionality is configured for a specific profile, the settings of the global parameter is ignored for calls associated with the profile.
Voice Volume configure voip > media voice > voice-volume [VoiceVolume]	Global parameter defining the voice gain control (in decibels). This defines the level of the transmitted signal. You can also configure the functionality per specific calls, using IP Profiles (IpProfile_VoiceVolume). For a detailed description of the parameter and for configuring the functionality, see "Configuring IP Profiles" on page 388. Note: If the functionality is configured for a specific profile, the settings of the global parameter is ignored for calls associated with the profile.
configure voip > media voice codecs > G726-voice-payload-format [VoicePayloadFormat]	Determines the bit ordering of the G.726 voice payload format. <ul style="list-style-type: none"> ▪ [0] = (Default) Little Endian ▪ [1] = Big Endian Note: To ensure high voice quality when using G.726, both communicating ends should use the same endianness format. Therefore, when the device communicates with a third-party entity that uses the G.726 voice coder and voice quality is poor, change the settings of the parameter (between Big Endian and Little Endian).
MF Transport Type configure voip > media voice > MF-transport-type [MFTransportType]	Currently, not supported.
Silence Suppression configure voip > media voice > silence-compression-mode [EnableSilenceCompression]	Global parameter that enables the Silence Suppression feature. You can also configure this functionality per specific calls, using IP Profiles (IpProfile_SCE). For a detailed description of the parameter and for configuring this functionality in the IP Profiles table, see "Configuring IP Profiles" on page 388. Note: <ul style="list-style-type: none"> ▪ If this functionality is configured for a specific profile, the settings of this global parameter is ignored for calls associated with the profile.
Echo Canceler configure voip > media voice > echo-canceller-enable [EnableEchoCanceller]	Global parameter enabling echo cancellation (i.e., echo from voice calls is removed). You can also configure this functionality per specific calls, using IP Profiles (IpProfile_EnableEchoCanceller). For a detailed description of the parameter and for configuring the functionality, see "Configuring IP Profiles" on page 388. Note: If the functionality is configured for a specific profile, the

Parameter	Description
	settings of this global parameter is ignored for calls associated with the profile.
Network Echo Suppressor Enable configure voip/media voice/acoustic-echo-suppressor-enable [AcousticEchoSuppressorSupport]	Enables the network Acoustic Echo Suppressor feature on SBC calls. This feature removes echoes and sends only the near-end's desired speech signal to the network (i.e., to the far-end party). <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable Note: For the parameter to take effect, a device reset is required.
Echo Canceller Type configure voip/media voice/echo-canceller-type [EchoCancellerType]	Defines the echo canceller type. <ul style="list-style-type: none"> ▪ [0] Line echo canceller = (Default) Echo canceller for Tel side. ▪ [1] Acoustic Echo suppressor - network = Echo canceller for IP side.
Attenuation Intensity configure voip/media voice/acoustic-echo-suppressor-attenuation-intensity [AcousticEchoSupAttenuationIntensity]	Defines the acoustic echo suppressor signals identified as echo attenuation intensity. The valid range is 0 to 3. The default is 0.
Max ERL Threshold - DB configure voip/media voice/acoustic-echo-suppressor-max-ERL [AcousticEchoSupMaxERLThreshold]	Defines the acoustic echo suppressor maximum ratio between signal level and returned echo from the phone (in decibels). The valid range is 0 to 60. The default is 10.
Min Reference Delay x10 msec configure voip/media voice/acoustic-echo-suppressor-min-reference-delay [AcousticEchoSupMinRefDelayx10ms]	Defines the acoustic echo suppressor minimum reference delay (in 10-ms units). The valid range is 0 to 40. The default is 0.
Max Reference Delay x10 msec configure voip/media voice/acoustic-echo-suppressor-max-reference-delay [AcousticEchoSupMaxRefDelayx10ms]	Defines the acoustic echo suppressor maximum reference delay (in 10-ms units). The valid range is 0 to 40. The default is 40 (i.e., 40 x 10 = 400 ms).
configure voip > media voice > echo-canceller-hybrid-loss [ECHybridLoss]	Defines the four-wire to two-wire worst-case Hybrid loss, the ratio between the signal level sent to the hybrid and the echo level returning from the hybrid. <ul style="list-style-type: none"> ▪ [0] = (Default) 6 dB ▪ [1] = N/A ▪ [2] = 0 dB ▪ [3] = 3 dB
configure voip > media voice > echo-canceller-NLP-mode [ECNLPMode]	Global parameter defining the echo cancellation Non-Linear Processing (NLP) mode.

Parameter	Description
	<ul style="list-style-type: none"> ▪ [0] = (Default) NLP adapts according to echo changes ▪ [1] = Disables NLP ▪ [2] = Silence output NLP <p>Note: If the functionality is configured for a specific Tel Profile, the settings of the global parameter is ignored for calls associated with the Tel Profile.</p>
configure voip > media voice > echo-canceller-aggressive-NLP [EchoCancellerAggressiveNLP]	<p>Enables the Aggressive NLP at the first 0.5 second of the call.</p> <ul style="list-style-type: none"> ▪ [0] = Disable ▪ [1] = (Default) Enable. The echo is removed only in the first half of a second of the incoming IP signal. <p>Note: For the parameter to take effect, a device reset is required.</p>
configure voip > media RTP-RTCP > number-of-SID-coefficients [RTPSIDCoeffNum]	<p>Defines the number of spectral coefficients added to an SID packet being sent according to RFC 3389.</p> <p>The valid values are [0] (default), [4], [6], [8] and [10].</p>
Answer Detector (AD) Parameters	
Enable Answer Detector [EnableAnswerDetector]	Currently, not supported.
Answer Detector Activity Delay configure voip > media ipmedia > answer-detector-activity-delay [AnswerDetectorActivityDelay]	<p>Defines the time (in 100-msec resolution) between activating the Answer Detector and the time that the detector actually starts to operate.</p> <p>The valid range is 0 to 1023. The default is 0.</p>
Answer Detector Silence Time [AnswerDetectorSilenceTime]	Currently, not supported.
Answer Detector Redirection [AnswerDetectorRedirection]	Currently, not supported.
Answer Detector Sensitivity configure voip > media ipmedia > answer-detector-sensitivity [AnswerDetectorSensitivity]	<p>Defines the Answer Detector sensitivity.</p> <p>The range is 0 (most sensitive) to 2 (least sensitive). The default is 0.</p>

55.10.2 Coder Parameters

The coder parameters are described in the table below.

Table 55-35: Coder Parameters

Parameter	Description
Silk Tx Inband FEC configure voip > media settings > silk-tx-inband-fec [SilkTxInbandFEC]	<p>Enables forward error correction (FEC) for the SILK coder.</p> <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable

Parameter	Description
Silk Max Average Bit Rate configure voip > media settings > silk-max-average-bitrate [SilkMaxAverageBitRate]	Defines the maximum average bit rate for the SILK coder. The valid value range is 6,000 to 50,000. The default is 50,000. The SILK coder is Skype's default audio codec used for Skype-to-Skype calls.
Opus Max Average Bitrate configure voip > sip-definition settings > opus-max-avg- bitrate [OpusMaxAverageBitRate]	Defines the maximum average bit rate (in bps) for the Opus coder. The valid value range is 6000 to 50,000. The default is 50,000.
AMR Payload Format [AmrOctetAlignedEnable]	Defines the AMR payload format type. <ul style="list-style-type: none"> ▪ [0] Bandwidth Efficient ▪ [1] Octet Aligned (default) Note: The AMR payload type can also be configured per Coder Group (see Configuring Coder Groups on page 379). The Coder Group configuration overrides the parameter.
configure voip > media settings > amr-header-format [AMRCoderHeaderFormat]	Determines the payload format of the AMR header. <ul style="list-style-type: none"> ▪ [0] = Non-standard multiple frames packing in a single RTP frame. Each frame has a CMR and TOC header. ▪ [1] = AMR frame according to RFC 3267 bundling. ▪ [2] = AMR frame according to RFC 3267 interleaving. ▪ [3] = AMR is passed using the AMR IF2 format. Note: Bandwidth Efficient mode is not supported; the mode is always Octet-aligned.

55.10.3 DTMF Parameters

The dual-tone multi-frequency (DTMF) parameters are described in the table below.

Table 55-36: DTMF Parameters

Parameter	Description
DTMF Transport Type configure voip > media voice > DTMF-transport-type [DTMFTransportType]	Determines the DTMF transport type. <ul style="list-style-type: none"> ▪ [0] Mute DTMF = DTMF digits are removed from the voice stream and are not relayed to remote side. ▪ [2] Transparent DTMF = DTMF digits remain in the voice stream. ▪ [3] RFC 2833 Relay DTMF = (Default) DTMF digits are removed from the voice stream and are relayed to remote side according to RFC 2833. ▪ [7] RFC 2833 Relay Decoder Mute = DTMF digits are sent according to RFC 2833 and muted when received. Note: The parameter is automatically updated if the parameters FirstTxDTMFOption or RxDTMFOption are configured.
DTMF Volume (-31 to 0 dB) configure voip > media voice > DTMF-volume [DTMFVolume]	Global parameter defining the DTMF gain control value (in decibels). Note: If the functionality is configured for a specific Tel Profile, the settings of the global parameter is ignored for calls associated with

Parameter	Description
	the Tel Profile.
DTMF Generation Twist configure voip > media voice > DTMF-generation-twist [DTMFGenerationTwist]	Defines the range (in decibels) between the high and low frequency components in the DTMF signal. Positive decibel values cause the higher frequency component to be stronger than the lower one. Negative values cause the opposite effect. For any parameter value, both components change so that their average is constant. The valid range is -10 to 10 dB. The default is 0 dB. Note: For the parameter to take effect, a device reset is required.
inter-digit-interval [DTMFInterDigitInterval]	Defines the time (in msec) between generated DTMF digits (if FirstTxDTMFOption = 1, 2 or 3). The valid range is 0 to 32767. The default is 100.
[DTMFDigitLength]	Defines the time (in msec) for generating DTMF tones (if FirstTxDTMFOption = 1, 2 or 3). It also configures the duration that is sent in INFO (Cisco) messages. The valid range is 0 to 32767. The default is 100.
configure voip > media voice > digit-hangover- time-rx [RxDTMFHangOverTime]	Defines the Voice Silence time (in msec) after playing DTMF or MF digits that arrive as Relay. Valid range is 0 to 2,000 msec. The default is 1,000 msec.
configure voip > media voice > digit-hangover-time-tx [TxDTMFHangOverTime]	Defines the Voice Silence time (in msec) after detecting the end of DTMF or MF digits when the DTMF Transport Type is either Relay or Mute. Valid range is 0 to 2,000 msec. The default is 1,000 msec.
NTE Max Duration configure voip > media voice > telephony-events-max-duration [NTEMaxDuration]	Defines the maximum time for sending Named Telephony Events / NTEs (RFC 4733/2833 DTMF relay), regardless of the DTMF signal duration on the other side. The range is -1 to 200,000,000 msec. The default is -1 (i.e., NTE stops only upon detection of an End event).

55.10.4 RTP, RTCP and T.38 Parameters

The RTP, RTCP and T.38 parameters are described in the table below.

Table 55-37: RTP/RTCP and T.38 Parameters

Parameter	Description
Broken Connection Mode configure voip > sip-definition settings > disc-broken-conn [DisconnectOnBrokenConnection]	Global parameter that defines the device's handling of calls if RTP packets are not received within a user-defined timeout (configured by the BrokenConnectionEventTimeout parameter). You can also configure this functionality per specific calls, using IP Profiles (IpProfile_DisconnectOnBrokenConnection). For a detailed description of the parameter and for configuring this functionality in the IP Profiles table, see 'Configuring IP Profiles' on page 388. Note: If this functionality is configured for a specific IP Profile, the settings of this global parameter is ignored for calls associated with the IP Profile.

Parameter	Description
Broken Connection Timeout configure voip > sip-definition settings > broken-connection- event-timeout [BrokenConnectionEventTimeout]	Defines the timeout interval (in 100-msec units) after which a call is disconnected if an RTP packet is not received during an established call (i.e., RTP flow suddenly stops during the call). The valid range is from 3 (i.e., 300 msec) to an unlimited value (e.g., 20 hours). The default is 100 (i.e., 10000 msec or 10 seconds). Note: The parameter is applicable only if the DisconnectOnBrokenConnection parameter is configured to 1.
configure voip > sbc settings > no- rtp-detection-timeout [NoRTPDetectionTimeout]	Defines the timeout interval (in msec) after which a call is disconnected if RTP packets are not received. The timer begins from call setup and if no packets have been received when the timer expires, the device disconnects the call. The valid range is 0-50000. The default is 0 (i.e., disconnects the call immediately). Note: If a call is established and RTP flow occurs, if at any stage during the call RTP packets are not detected for a user-defined interval (configured by BrokenConnectionEventTimeout), the device disconnects the call (or routes it to an alternative destination, configured by the IpProfile_DisconnectOnBrokenConnection).
Dynamic Jitter Buffer Minimum Delay configure voip > media rtp-rtcp > jitter-buffer-minimum-delay [DJBufMinDelay]	Global parameter defining the minimum delay (in msec) of the device's dynamic Jitter Buffer. You can also configure the functionality per specific calls, using IP Profiles (IpProfile_JitterBufMinDelay). For a detailed description of the parameter and for configuring the functionality, see Configuring IP Profiles on page 388. Note: If the functionality is configured for a specific profile, the settings of the global parameter is ignored for calls associated with the profile.
Dynamic Jitter Buffer Optimization Factor configure voip > media rtp-rtcp > jitter-buffer-optimization-factor [DJBufOptFactor]	Global parameter defining the Dynamic Jitter Buffer frame error/delay optimization factor. You can also configure the functionality per specific calls, using IP Profiles (IpProfile_JitterBufOptFactor). For a detailed description of the parameter and for configuring the functionality, see Configuring IP Profiles on page 388. Note: If the functionality is configured for a specific profile, the settings of the global parameter is ignored for calls associated with the profile.
RTP Redundancy Depth configure voip > media rtp-rtcp > RTP-redundancy-depth [RTPRedundancyDepth]	Global parameter that enables the device to generate RFC 2198 redundant packets. You can also configure this functionality per specific calls, using IP Profiles (IpProfile_RTPRedundancyDepth). For a detailed description of the parameter and for configuring this functionality in the IP Profiles table, see "Configuring IP Profiles" on page 388. Note: If this functionality is configured for a specific IP Profile, the settings of this global parameter is ignored for calls associated with the IP Profile.
RFC 2198 Payload Type configure voip > media rtp-rtcp > RTP-redundancy-payload-type	Defines the RTP redundancy packet payload type (according to RFC 2198). The valid value is 96 to 127. The default is 104.

Parameter	Description
[RFC2198PayloadType]	Note: The parameter is applicable only if the RTPRedundancyDepth parameter is set to 1.
Packing Factor [RTPPackingFactor]	N/A. Controlled internally by the device according to the selected coder.
RFC 2833 TX Payload Type configure voip > gateway dtmf- supp-service dtmf-and-dialing > telephony-events-payload-type-tx [RFC2833TxPayloadType]	Defines the Tx RFC 2833 DTMF relay dynamic payload type for outbound calls. The valid range is 96 to 127. The default is 96. Note: When RFC 2833 payload type negotiation is used (i.e., the parameter FirstTxDTMFOption is set to 4), this payload type is used for the received DTMF packets. If negotiation isn't used, this payload type is used for receive and for transmit.
RFC 2833 RX Payload Type telephony-events-payload-type-rx [RFC2833RxPayloadType]	Defines the Rx RFC 2833 DTMF relay dynamic payload type for inbound calls. The valid range is 96 to 127. The default is 96. Note: When RFC 2833 payload type negotiation is used (i.e., the parameter FirstTxDTMFOption is set to 4), this payload type is used for the received DTMF packets. If negotiation isn't used, this payload type is used for receive and for transmit.
[EnableDetectRemoteMACChange]	Determines whether the device changes the RTP packets according to the MAC address of received RTP packets and according to Gratuitous Address Resolution Protocol (GARP) messages. <ul style="list-style-type: none"> ▪ [0] = Nothing is changed. ▪ [1] = If the device receives RTP packets with a different source MAC address (than the MAC address of the transmitted RTP packets), then it sends RTP packets to this MAC address and removes this IP entry from the device's ARP cache table. ▪ [2] = (Default) The device uses the received GARP packets to change the MAC address of the transmitted RTP packets. ▪ [3] = Options 1 and 2 are used. Note: <ul style="list-style-type: none"> ▪ For the parameter to take effect, a device reset is required. ▪ If the device is located in a network subnet which is connected to other gateways using a router that uses Virtual Router Redundancy Protocol (VRRP) for redundancy, then set the parameter to 0 or 2.
RTP Base UDP Port configure voip > media rtp-rtcp > base-udp-port [BaseUDPport]	Global parameter that defines the lower boundary of the UDP port used for RTP, RTCP (RTP port + 1) and T.38 (RTP port + 2). For more information on configuring the UDP port range, see "Configuring RTP Base UDP Port" on page 187. The range of possible UDP ports is 6,000 to 65,535. The default base UDP port is 6000. Note: For the parameter to take effect, a device reset is required.
configure voip > media rtp-rtcp > udp-port-spacing	Defines the port spacing ("jumps") of local UDP ports allocated by the device to media channels (legs) within the configured

Parameter	Description
[UdpPortSpacing]	<p>port range.</p> <ul style="list-style-type: none"> [4] = The device allocates ports in "jumps" of 4 ports. [5] = (Default) The device allocates ports in "jumps" of 5 ports. [10] = The device allocates ports in "jumps" of 10 ports. <p>Note:</p> <ul style="list-style-type: none"> A device reset is required for the parameter to take effect. For more information on configuring the UDP port range, see Configuring RTP Base UDP Port on page 187.
No-Op Packets Parameters	
no-operation-enable [NoOpEnable]	<p>Enables the transmission of RTP or T.38 No-Op packets.</p> <ul style="list-style-type: none"> [0] = Disable (default) [1] = Enable <p>This mechanism ensures that the NAT binding remains open during RTP or T.38 silence periods.</p>
[NoOpInterval]	<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>Note: To enable No-Op packet transmission, use the NoOpEnable parameter.</p>
no-operation-interval [RTPNoOpPayloadType]	<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>Note: When defining the parameter, ensure that it doesn't cause collision with other payload types.</p>
RTP Control Protocol Extended Reports (RTCP XR) Parameters	
For more information on RTCP XR, see "Configuring RTCP XR" on page 665.	
Enable RTCP XR configure voip > media rtp-rtcp > voice-quality-monitoring-enable [VQMonEnable]	<p>Enables voice quality monitoring and RTCP XR, according to RFC 3611.</p> <ul style="list-style-type: none"> [0] Disable (default) [1] Enable Fully = Calculates voice quality metrics, uses them for QoE calculations, reports them to SEM (if configured), and sends them to remote side using RTCP XR. [2] Enable Calculation Only = Calculates voice quality metrics, uses them for QoE calculations, reports them to SEM (if configured), but does not send them to remote side using RTCP XR. <p>Note: For the parameter to take effect, a device reset is required.</p>
Minimum Gap Size [VQMonGMin]	<p>Defines the voice quality monitoring - minimum gap size (number of frames).</p> <p>The default is 16.</p>
Burst Threshold [VQMonBurstHR]	<p>Defines the voice quality monitoring - excessive burst alert threshold.</p> <p>The default is -1 (i.e., no alerts are issued).</p>

Parameter	Description
Delay Threshold [VQMonDelayTHR]	Defines the voice quality monitoring - excessive delay alert threshold. The default is -1 (i.e., no alerts are issued).
R-Value Delay Threshold [VQMonEOCRValTHR]	Defines the voice quality monitoring - end of call low quality alert threshold. The default is -1 (i.e., no alerts are issued).
RTCP XR Packet Interval configure voip > media rtp-rtcp > rtp-interval [RTCPInterval]	Defines the time interval (in msec) between adjacent RTCP XR reports. This interval starts from call establishment. Thus, the device can send RTCP XR reports during the call, in addition to at the end of the call. If the duration of the call is shorter than this interval, RTCP XR is sent only at the end of the call. The valid value range is 0 to 65,535. The default is 5,000.
Disable RTCP XR Interval Randomization configure voip > media rtp-rtcp > disable-RTCP-randomization [DisableRTCPRandomize]	Determines whether RTCP report intervals are randomized or whether each report interval accords exactly to the parameter RTCPInterval. <ul style="list-style-type: none"> ▪ [0] Disable = (Default) Randomize ▪ [1] Enable = No Randomize
SBC RTCP XR Report Mode configure voip > sip-definition settings > sbc-rtcpxr-report-mode [SBCRtcpXrReportMode]	Enables the sending of RTCP XR reports of QoE metrics at the end of each call session (i.e., after a SIP BYE). The RTCP XR is sent in the SIP PUBLISH message. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] End of Call
publication-ip-group-id [PublicationIPGroupID]	Defines the IP Group to where the RTCP XR is sent.

55.11 SBC Parameters

The SBC and CRP parameters are described in the table below.

Table 55-38: SBC and CRP Parameters

Parameter	Description
CRP-specific Parameters	
CRP Application configure voip > application > enable-crp [EnableCRPApplication]	Enables the CRP application. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable Note: For the parameter to take effect, a device reset is required.
CRP Survivability Mode configure voip > sbc settings > crp-survivability-mode	Defines the CRP mode. <ul style="list-style-type: none"> ▪ [0] Standard Mode (default) ▪ [1] Always Emergency Mode

Parameter	Description
[CRPSurvivabilityMode]	<ul style="list-style-type: none"> [2] Auto-answer REGISTER
configure voip > sbc settings > crp-gw-fallback [CRPGatewayFallback]	Enables fallback routing from the proxy server to the Gateway (PSTN). <ul style="list-style-type: none"> [0] = Disable (default) [1] = Enable
SBC-specific Parameters	
Enable SBC configure voip > application > enable-sbc [EnableSBCApplication]	Enables the Session Border Control (SBC) application. <ul style="list-style-type: none"> [0] Disable (default) [1] Enable Note: <ul style="list-style-type: none"> For the parameter to take effect, a device reset is required. In addition to enabling the parameter, the number of maximum SBC/IP-to-IP sessions must be included in the License Key.
SBC and CRP Parameters	
Unclassified Calls configure voip > sbc settings > unclassified-calls [AllowUnclassifiedCalls]	Determines whether incoming calls that cannot be classified (i.e. classification process fails) to a Source IP Group are rejected or processed. <ul style="list-style-type: none"> [0] Reject = (Default) Call is rejected if classification fails. [1] Allow = If classification fails, the incoming packet is assigned to a source IP Group (and subsequently processed) as follows: <ul style="list-style-type: none"> ✓ 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. ✓ 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.
SBC Max Call Duration configure voip > sbc settings > sbc-mx-call-duration [SBCMaxCallDuration]	Defines the maximum duration (in minutes) per SBC call (global). If the duration is reached, the device terminates the call. The valid range is 0 to 35,791, where 0 is unlimited duration. The default is 0. Note: You can also configure this functionality per specific calls, using IP Profiles (IpProfile_SBCMaxCallDuration). For a detailed description of the parameter and for configuring this functionality in the IP Profiles table, see "Configuring IP Profiles" on page 388. If this functionality is configured for a specific IP Profile, the settings of this global parameter is ignored for calls associated with the IP Profile.
SBC No Answer Timeout configure voip > sbc settings > sbc-no-arelt-timeout [SBCAlertTimeout]	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.

Parameter	Description
	The valid range is 0 to 3600 seconds. the default is 600.
configure voip > sbc settings > num-of-subscribes [NumOfSubscribes]	Defines the maximum number of concurrent SIP SUBSCRIBE sessions permitted on the device. The valid value is any value between 0 and the maximum supported SUBSCRIBE sessions. When set to -1, the device uses the default value. For more information, contact your AudioCodes sales representative. Note: <ul style="list-style-type: none"> ▪ For the parameter to take effect, a device reset is required. ▪ The maximum number of SUBSCRIBE sessions can be increased by reducing the maximum number of SBC channels in the License Key. For every reduced SBC session, the device gains two SUBSCRIBE sessions.
configure voip > sbc settings > sbc-dialog-subsc-route-mode [SBCInDialogSubscribeRouteMode]	Enables the device to route in-dialog, refresh SIP SUBSCRIBE requests to the "working" (has connectivity) proxy. <ul style="list-style-type: none"> ▪ [0] = (Default) Disable – the device sends in-dialog, refresh SUBSCRIBES according to the address in the Contact header of the 200 OK response received from the proxy to which the initial SUBSCRIBE was sent (as per the SIP standard). ▪ [1] = Enable – the device routes in-dialog, refresh SUBSCRIBES to the "working" proxy (regardless of the Contact header). The "working" proxy (address) is determined by the device's keep-alive mechanism for the Proxy Set that was used to route the initial SUBSCRIBE. Note: For this feature to be functional, ensure the following: <ul style="list-style-type: none"> ▪ Keep-alive mechanism is enabled for the Proxy Set ('Proxy Keep-Alive' parameter is set to any value other than Disable). ▪ Load-balancing between proxies is disabled ('Proxy Load Balancing Method' parameter is set to Disable).
configure voip > sbc settings > sbc-max-fwd-limit [SBCMaxForwardsLimit]	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. The parameter affects the Max-Forwards header in the received message as follows: <ul style="list-style-type: none"> ▪ If the received header's original value is 0, the message is not passed on and is rejected. ▪ If the received header's original value is less than the parameter's value, the header's value is decremented before being sent on. ▪ 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. The valid value range is 1-70. The default is 10.
SBC Session-Expires configure voip > sbc settings > sbc-	Defines the SBC session refresh timer (in seconds) in the Session-Expires header of outgoing INVITE messages.

Parameter	Description
sess-exp-time [SBCSessionExpires]	The valid value range is 90 (according to RFC 4028) to 86400. The default is 180.
Minimum Session-Expires configure voip > sbc settings > min-session-expire [SBCMinSE]	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. The valid range is 0 (default) to 1,000,000, where 0 means that the device does not limit Session-Expires.
configure voip > sbc settings > sbc-session-refresh-policy [SBCSessionRefreshingPolicy]	Defines the SIP user agent responsible for periodically sending refresh requests for established sessions (active calls). The session refresh allows SIP UAs or proxies to determine the status of the SIP session. When a session expires, the session is considered terminated by the UAs, regardless of whether a SIP BYE was sent by one of the UAs. The SIP Session-Expires header conveys the lifetime of the session, which is sent in re-INVITE or UPDATE requests (session refresh requests). The 'refresher=' parameter in the Session-Expires header (sent in the initial INVITE or subsequent 2xx response) indicates who sends the session refresh requests. If the parameter contains the value 'uac', the device performs the refreshes; if the parameter contains the value 'uas', the remote proxy performs the refreshes. An example of the Session-Expires header is shown below: <pre style="background-color: #f0f0f0; padding: 5px;">Session-Expires: 4000;refresher=uac</pre> Thus, the parameter is useful when a UA does not support session refresh requests or does not support the indication of who performs session refresh requests. In such a scenario, the device can be configured to perform the session refresh requests. <ul style="list-style-type: none"> ▪ [0] Remote Refresher = (Default) The UA (proxy) performs the session refresh requests. The device indicates this to the UA by sending the SIP message with the 'refresher=' parameter in the Session-Expires header set to 'uas'. ▪ [1] SBC Refresher = The device performs the session refresh requests. The device indicates this to the UA by sending the SIP message with the 'refresher=' parameter in the Session-Expires header set to 'uac'. <p>Note: The time values of the Session-Expires (session refresh interval) and Min-SE (minimum session refresh interval) headers can be configured using the SBCSessionExpires and SBCMinSE parameters, respectively.</p>
User Registration Grace Time configure voip > sbc settings > sbc-usr-reg-grace-time [SBCUserRegistrationGraceTime]	Defines additional time (in seconds) to add to the registration expiry time users that are registered in the device's Users Registration database. The valid value is 0 to 2,000,000. The default is 0. For more information, see Registration Refreshes on page 429.
SBC DB Routing Search Mode configure voip > sbc settings > sbc-db-route-mode [SBCDBRoutingSearchMode]	Defines the method for searching a registered user in the device's User Registration database when a SIP INVITE message is received for routing to a user. If the registered user is found (i.e., destination URI in INVITE), the device routes the call to the user's corresponding contact address specified in the

Parameter	Description
	<p>database.</p> <ul style="list-style-type: none"> ▪ [0] All permutations = (Default) Device searches for the user in the database using the entire Request-URI (user@host). If not found, it searches for the user part of the Request-URI. For example, it first searches for "4709@joe.company.com" and if not found, it searches for "4709". ▪ [1] Dest URI dependant = Device searches for the user in the database using the entire Request-URI (user@host) only. For example, it searches for "4709@joe.company.com". <p>Note: If the Request-URI contains the "tel:" URI or "user=phone" parameter, the device searches only for the user part.</p>
<p>Handle P-Asserted-Identity configure voip > sbc settings > p-assert-id [SBCAssertIdentity]</p>	<p>Global parameter that defines the handling of the SIP P-Asserted-Identity header. You can also configure this functionality per specific calls, using IP Profiles (IpProfile_SBCAssertIdentity). For a detailed description of the parameter and for configuring this functionality in the IP Profiles table, see "Configuring IP Profiles" on page 388.</p> <p>Note: If this functionality is configured for a specific IP Profile, the settings of this global parameter is ignored for calls associated with the IP Profile.</p>
<p>Keep original user in Register configure voip > sbc settings > keep-contact-user-in-reg [SBCKeepContactUserinRegister]</p>	<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"> ▪ [0] Disable = (Default) The device replaces the original Contact user with a unique Contact user, for example: <ul style="list-style-type: none"> ✓ Received Contact: <sip:123@domain.com> ✓ Outgoing (unique) Contact: <sip:FEU1_7_1@SBC> ▪ [1] Enable = The original Contact user is retained and used in the outgoing REGISTER request. <p>Note: The parameter is applicable only to REGISTER messages received from User-type IP Groups and that are sent to Server-type IP Groups.</p>
<p>SBC Remote Refer Behavior configure voip > sbc settings > sbc-refer-bhvr [SBCReferBehavior]</p>	<p>Global parameter that defines the handling of SIP REFER requests. You can also configure this functionality per specific calls, using IP Profiles (IpProfile_SBCRemoteReferBehavior). For a detailed description of the parameter and for configuring this functionality in the IP Profiles table, see "Configuring IP Profiles" on page 388.</p> <p>Note: If this functionality is configured for a specific IP Profile, the settings of this global parameter is ignored for calls associated with the IP Profile.</p>
<p>configure voip > sbc settings > sbc-xfer-prefix [SBCXferPrefix]</p>	<p>When the SBCReferBehavior is set to 1, the device, while interworking the SIP REFER message, adds the prefix "T-&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>

Parameter	Description
	By default, no value is defined. Note: This feature is also applicable to 3xx redirect responses. The device adds the prefix "T-&R-" to the URI user part in the Contact header if the SBC3xxBehavior parameter is set to 1.
configure voip > sbc settings > sbc-3xx-bhvt [SBC3xxBehavior]	Global parameter that defines the handling of SIP 3xx redirect responses. You can also configure this functionality per specific calls, using IP Profiles (IpProfile_SBCRemote3xxBehavior). For a detailed description of the parameter and for configuring this functionality in the IP Profiles table, see "Configuring IP Profiles" on page 388. Note: If this functionality is configured for a specific IP Profile, the settings of this global parameter is ignored for calls associated with the IP Profile.
configure voip > sbc settings > enforce-media-order [SBCEnforceMediaOrder]	Enables the device to include all previously negotiated media lines within the current session ('m=' line) in the SDP offer-answer exchange (RFC 3264). <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable For example, assume a call (audio) has been established between two endpoints and one endpoint wants to subsequently send an image in the same call session. If the parameter is enabled, the endpoint includes the previously negotiated media type (i.e., audio) with the new negotiated media type (i.e., image) in its SDP offer: <pre style="background-color: #f0f0f0; padding: 5px;">v=0 o=bob 2890844730 2890844731 IN IP4 host.example.com s= c=IN IP4 host.example.com t=0 0 m=audio 0 RTP/AVP 0 m=image 12345 udpt1 t38</pre> If the parameter is disabled, the only 'm=' line included in the SDP is the newly negotiated media (i.e., image).
SBC Diversion URI Type configure voip > sbc settings > sbc-diversion-uri-type [SBCDiversionUriType]	Defines the URI type to use in the SIP Diversion header of the outgoing SIP message. <ul style="list-style-type: none"> ▪ [0] Transparent = (Default) The device does not change the URI and leaves it as is. ▪ [1] Sip = The "sip" URI is used. ▪ [2] Tel = The "tel" URI is used. Note: The parameter is applicable only if the Diversion header is used. The SBCDiversionMode and SBCHistoryInfoMode parameters in the IP Profiles table determine the call redirection (diversion) SIP header to use - History-Info or Diversion.
SBC Server Auth Mode configure voip > sbc settings > sbc-server-auth-mode [SBCServerAuthMode]	Defines whether authentication of the SIP client is done locally (by the device) or by a RADIUS server. <ul style="list-style-type: none"> ▪ [0] (default) = Authentication is done by the device (locally). ▪ [1] = Authentication is done by the RFC 5090 compliant RADIUS server. ▪ [2] = Authentication is done according to the Draft Sterman-aaa-sip-01 method.

Parameter	Description
	Note: Currently, option [1] is not supported.
Lifetime of the nonce in seconds configure voip > sbc settings > lifetime-of-nonce [AuthNonceDuration]	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. The 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.
Authentication Challenge Method configure voip > sbc settings > auth-chlng-mthd [AuthChallengeMethod]	Defines the type of server-based authentication challenge. <ul style="list-style-type: none"> ▪ [0] 0 = (Default) Send SIP 401 "Unauthorized" with a WWW-Authenticate header as the authentication challenge response. ▪ [1] 1 = Send SIP 407 "Proxy Authentication Required" with a Proxy-Authenticate header as the authentication challenge response.
Authentication Quality of Protection configure voip > sbc settings > auth-qop [AuthQOP]	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. <ul style="list-style-type: none"> ▪ [0] 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). ▪ [1] 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. ▪ [2] 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. ▪ [3] 3 = No 'qop' parameter is offered in the SIP 401 challenge message.
SBC User Registration Time configure voip > sbc settings > sbc-usr-rgstr-time [SBCUserRegistrationTime]	Global parameter that defines the duration (in seconds) of the periodic registrations that occur between the user and the device (the device responds with this value to the user). You can also configure this functionality per specific calls, using IP Profiles (IpProfile_SBCUserRegistrationTime). For a detailed description of the parameter and for configuring this functionality in the IP Profiles table, see "Configuring IP Profiles" on page 388. Note: If this functionality is configured for a specific IP Profile,

Parameter	Description
	the settings of this global parameter is ignored for calls associated with the IP Profile.
SBC Proxy Registration Time configure voip > sbc settings > sbc-prxy-rgstr-time [SBCProxyRegistrationTime]	Defines the duration (in seconds) for which the user is registered in the proxy database (after the device forwards the REGISTER message). This value is sent in the Expires header. When set to 0, the device sends the Expires header's value as received from the user to the proxy. The valid range is 0 to 2,000,000 seconds. The default is 0.
configure voip > sbc settings > sbc-rand-expire [SBCRandomizeExpires]	Defines a value (in seconds) that is used to calculate a new value for the expiry time in the Expires header of SIP 200 OK responses for user registration and subscription requests from users. The expiry time value appears in the Expires header in REGISTER and SUBSCRIBE SIP messages. When the device receives such a request from a user, it forwards it to the proxy or registrar server. Upon a successful registration or subscription, the server sends a SIP 200 OK response. If the expiry time was unchanged by the server, the device applies this feature and changes the expiry time in the SIP 200 OK response before forwarding it to the user; otherwise, the device does not change the expiry time. This feature is useful in scenarios where multiple users may refresh their registration or subscription simultaneously, thereby causing the device to handle many such sessions at a given time. This may result in an overload of the device (reaching maximum session capacity), thereby preventing the establishment of new calls or preventing the handling of some user registration or subscription requests. When this feature is enabled, the device assigns a random expiry time to each user registration or subscription and thus, ensuring future user registration and subscription requests are more distributed over time (i.e., do not all occur simultaneously). The device takes any random number between 0 and the value configured by the parameter, and then subtracts this random number from the original expiry time value. For example, assume that the original expiry time is 120 and the parameter is set to 10. If the device randomly chooses the number 5 (i.e., between 0 and 10), the resultant expiry time will be 115 (120 minus 5). The valid value is 0 to 20. The default is 10. If set to 0, the device does not change the expiry time. Note: <ul style="list-style-type: none"> ▪ The lowest expiry time that the device sends in the 200 OK, regardless of the resultant calculation, is 10 seconds. For example, if the original expiry time is 12 seconds and the parameter is set to 5, theoretically, the new expiry time can be less than 10 (e.g., $12 - 4 = 8$). However, the expiry time will be set to 10. ▪ The expiry time received from the user can be changed by the device before forwarding it to the proxy. This is configured by the SBCUserRegistrationTime parameter.
SBC Survivability Registration Time	Defines the duration of the periodic registrations between the user and the device, when the device is in survivability state

Parameter	Description
configure voip > sbc settings > sbc-surv-rgstr-time [SBCSurvivabilityRegistrationTime]	(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. The valid range is 0 to 2,000,000 seconds. The default is 0.
configure voip > sbc settings > sas-notice [SBCEnableSurvivabilityNotice]	Enables the device to notify Aastra IP phones that the device is currently operating in Survivability mode. <ul style="list-style-type: none"> ▪ [0] = Disable ▪ [1] = Enable For more information, see "Enabling Survivability Display on Aastra IP Phones" on page 537.
SBC Dialog-Info Interworking configure voip > sbc settings > sbc-dialog-info-interwork [EnableSBCDialogInfoInterworking]	Enables the interworking of dialog information (parsing of call identifiers in XML body) in SIP NOTIFY messages received from a remote application server. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable For more information, see "Interworking Dialog Information in SIP NOTIFY Messages" on page 455.
configure voip > sbc settings > sbc-keep-call-id [SBCKeepOriginalCallId]	Global parameter that enables the device to use the same call identification (SIP Call-ID header value) received in incoming messages for the call identification in outgoing messages. The call identification value is contained in the SIP Call-ID header. You can also configure the functionality per specific calls, using IP Profiles. For a detailed description of the parameter and for configuring the functionality in the IP Profiles table, see Configuring IP Profiles on page 388.
SBC GRUU Mode configure voip > sbc settings > sbc-gruu-mode [SBCGruuMode]	Determines the Globally Routable User Agent (UA) URI (GRUU) support, according to RFC 5627. <ul style="list-style-type: none"> ▪ [0] None = No GRUU is supplied to users. ▪ [1] As Proxy = (Default) The device provides same GRUU types as the proxy provided the device's GRUU clients. ▪ [2] Temporary only = Supply only temporary GRUU to users. (Currently not supported.) ▪ [3] Public only = The device provides only public GRUU to users. ▪ [4] Both = The device provides temporary and public GRUU to users. (Currently not supported.) The 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. 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). Public-GRUU: sip:userA@domain.com;gr=unique-

Parameter	Description
	id
Bye Authentication configure voip > sbc settings > sbc-by-auth [SBCEnableByeAuthentication]	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. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] 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.
SBC Enable Subscribe Trying configure voip > sbc settings > sbc-subs-try [SBCSendTryingToSubscribe]	Enables the device to send SIP 100 Trying responses upon receipt of SUBSCRIBE or NOTIFY messages. <ul style="list-style-type: none"> ▪ [0] Disable (Default) ▪ [1] Enable
BroadWorks Survivability Feature configure voip > sbc settings > sbc-broadworks-survivability [SBCExtensionsProvisioningMode]	Enables SBC user registration for interoperability with BroadSoft's BroadWorks server, to provide call survivability in case of connectivity failure with the BroadWorks server. <ul style="list-style-type: none"> ▪ [0] Disable = (Default) Normal processing of REGISTER messages. ▪ [1] Enable = 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). <p>Note: For a detailed description of this feature, see "Enabling Auto-Provisioning of Subscriber-Specific Information of BroadWorks Server for Survivability" on page 532.</p>
SBC Direct Media configure voip > sip-interface > sbc-direct-media [SBCDirectMedia]	Enables the Direct Media feature (i.e., no Media Anchoring) for all SBC calls, whereby SIP signaling is handled by the device without handling the RTP/SRTP (media) flow between the 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 <ul style="list-style-type: none"> ▪ [0] Disable = (Default) All calls traverse the device (i.e., no direct media). ▪ [1] Enable = Direct media flow between endpoints for all SBC calls. <p>Note:</p> <ul style="list-style-type: none"> ▪ The setting of direct media in the SIP Interfaces table overrides this global parameter. In other words, even if the parameter is disabled for direct media (i.e., Media Anchoring is enabled), if direct media is enabled for a SIP Interface (in the SIP Interfaces table), calls between endpoints belonging to the SIP Interface employ direct media. ▪ For more information on No Media Anchoring, see "Direct Media" on page 432.
Transcoding Mode	Global parameter that defines the voice transcoding mode

Parameter	Description
configure voip > sbc settings > transcoding-mode [TranscodingMode]	<p>(media negotiation). You can also configure this functionality per specific calls, using IP Profiles (IpProfile_TranscodingMode). For a detailed description of the parameter and for configuring this functionality in the IP Profiles table, see Configuring IP Profiles on page 388.</p> <p>Note: If this functionality is configured for a specific IP Profile, the settings of this global parameter is ignored for calls associated with the IP Profile.</p>
Preferences Mode configure voip > sbc settings > sbc-preferences [SBCPreferencesMode]	<p>Determines the order of the Extension coders (coders added if there are no common coders between SDP offered coders and Allowed coders) and Allowed coders (configured in the Allowed Audio Coders Groups table) in the outgoing SIP message (in the SDP).</p> <ul style="list-style-type: none"> ▪ [0] Doesn't Include Extensions = (Default) Extension coders are added at the end of the coder list. ▪ [1] Include Extensions = Extension coders and Allowed coders are arranged according to their order of appearance in the Allowed Audio Coders Groups table. <p>Note: The parameter is applicable only if a Coders Group for Extension coders is assigned to the IP Profile (IPProfile_SBCExtensionCodersGroupName).</p>
SBC RTCP Mode configure voip > sbc settings > sbc-rtcp-mode [SBCRTCPMode]	<p>Global parameter that defines the handling of RTCP packets. You can also configure this functionality per specific calls, using IP Profiles (IPProfile_SBCRTCPMode). For a detailed description of the parameter and for configuring this functionality in the IP Profiles table, see "Configuring IP Profiles" on page 388.</p> <p>Note: If this functionality is configured for a specific IP Profile, the settings of this global parameter is ignored for calls associated with the IP Profile.</p>
SBC Send Invite To All Contacts configure voip > sbc settings > sbc-send-invite-to-all-contacts [SBCSendInviteToAllContacts]	<p>Enables call forking of INVITE message received with a Request-URI of 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"> ▪ [0] Disable (default) = Sends the INVITE only to the contact of the received Request-URI. ▪ [1] Enable <p>To configure call forking initiated by the device, see "Initiating SIP Call Forking" on page 531.</p>
SBC Shared Line Registration Mode configure voip > sbc settings > sbc-shared-line-reg-mode [SBCSharedLineRegMode]	<p>Enables the termination on the device of SIP REGISTER messages from secondary lines that belong to the Shared Line feature.</p> <ul style="list-style-type: none"> ▪ [0] Disable = (Default) Device forwards the REGISTER messages as is (i.e., not terminated on the device). ▪ [1] Enable = REGISTER messages of secondary lines are terminated on the device. <p>Note: The device always forwards REGISTER messages of the primary line.</p>
SBC Forking Handling Mode configure voip > sbc settings > sbc-	<p>Defines the handling of SIP 18x responses that are received due to call forking of an INVITE.</p>

Parameter	Description
forking-handling-mode [SBCForkingHandlingMode]	<ul style="list-style-type: none"> ▪ [0] 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 sends it to the other side. ▪ [1] 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.
configure voip > sbc settings > sbc-media-sync [EnableSBCMediaSync]	Enables synchronization of media between two SIP user agents when a call is established between them. Media synchronization means that the media is properly negotiated (SDP offer/answer) between the user agents. In some scenarios, the call is established despite the media not being synchronized. This may occur, for example, in call transfer (SIP REFER) where the media between the transfer target and transferee are not synchronized. The device performs media synchronization by sending a re-INVITE immediately after the call is established in order for the user agents to negotiate the media (SDP offer/answer). <ul style="list-style-type: none"> ▪ [0] Disable = (Default) Media synchronization is performed only if the RTP mode (e.g., a=sendrecv, a=sendrecv, a=sendonly, a=recvonly, and a=inactive) between the user agents are different and synchronization is required. ▪ [1] Enable = Media synchronization is performed if the media, including RTP mode or any other media such as coders, is different and has not been negotiated between the user agents. ▪ [2] Never = Media synchronization is never performed.
SBC Fax Detection Timeout [SBCFaxDetectionTimeout]	Defines the duration (in seconds) for which the device attempts to detect fax (CNG tone) immediately upon the establishment of a voice session. The interval starts from the establishment of the voice call. The valid value is 1 to any integer. The default is 10. The feature applies to faxes that are sent immediately after the voice channel is established (i.e., after 200 OK). You can configure the handling of fax negotiation by the device for specific calls, using IP Profiles configured in the IP Profiles table (see the IpProfile_SBCRemoteRenegotiateOnFaxDetection parameter in Configuring IP Profiles on page 388).
Admission Control Table	
Admission Control configure voip > sbc sbc-admission-control [SBCAdmissionControl]	Defines Call Admission Control (CAC) rules. The format of the ini file table parameter is as follows: [SBCAdmissionControl] FORMAT SBCAdmissionControl_Index = SBCAdmissionControl_AdmissionControlName, SBCAdmissionControl_LimitType, SBCAdmissionControl_IPGroupName, SBCAdmissionControl_SRDName,

Parameter	Description
	SBCAdmissionControl_SIPInterfaceName, SBCAdmissionControl_RequestType, SBCAdmissionControl_RequestDirection, SBCAdmissionControl_Limit, SBCAdmissionControl_LimitPerUser, SBCAdmissionControl_Rate, SBCAdmissionControl_MaxBurst, SBCAdmissionControl_Reservation; [SBCAdmissionControl] For a description of the table, see "Configuring Admission Control" on page 457.
Allowed Audio Coders Table	
Allowed Audio Coders configure voip > coders-and-profiles allowed-audio-coders <group index > coder index> [AllowedAudioCoders]	Defines audio coders for the Allowed Audio Coders Group. The format of the ini file table parameter is as follows: [AllowedAudioCoders] FORMAT AllowedAudioCoders_Index = AllowedAudioCoders_AllowedAudioCodersGroupName, AllowedAudioCoders_AllowedAudioCodersIndex, AllowedAudioCoders_CoderID, AllowedAudioCoders_UserDefineCoder; [\AllowedAudioCoders] For a description of the table, see "Configuring Allowed Audio Coder Groups" on page 384.
Allowed Audio Coders Groups Table	
Allowed Audio Coders Groups configure voip > coders-and-profiles allowed-audio-coders-groups [AllowedAudioCodersGroups]	Defines the index and name of the Allowed Audio Coders Group. The format of the ini file table parameter is as follows: [AllowedAudioCodersGroups] FORMAT AllowedAudioCodersGroups_Index = AllowedAudioCodersGroups_Name; [\AllowedAudioCodersGroups] For a description of the table, see "Configuring Allowed Audio Coder Groups" on page 384.
Allowed Video Coders Groups Table	
Allowed Video Coders Groups configure voip > coders-and-profiles allowed-video-coders-groups [AllowedVideoCodersGroups]	Defines the index and name of the Allowed Video Coders Group. The format of the ini file table parameter is as follows: [AllowedVideoCodersGroups] FORMAT AllowedVideoCodersGroups_Index = AllowedVideoCodersGroups_Name; [\AllowedVideoCodersGroups] For a description of the table, see "Configuring Allowed Video Coder Groups" on page 387.
Allowed Video Coders Table	
Allowed Video Coders coders-and-profiles allowed-video-coders <group index > coder index>	Defines video coders for the Allowed Video Coders Group. The format of the ini file table parameter is as follows: [AllowedVideoCoders] FORMAT AllowedVideoCoders_Index =

Parameter	Description
[AllowedVideoCoders]	AllowedVideoCoders_AllowedVideoCodersGroupName, AllowedVideoCoders_AllowedVideoCodersIndex, AllowedVideoCoders_UserDefineCoder; [\AllowedVideoCoders] For a description of the table, see "Configuring Allowed Audio Coder Groups" on page 384.
Classification Table	
Classification Table configure voip > sbc classification [Classification]	Defines call Classification rules. The format of the ini file table parameter is as follows: [Classification] FORMAT Classification_Index = Classification_ClassificationName, Classification_MessageConditionName, Classification_SRDName, Classification_SrcSIPInterfaceName, Classification_SrcAddress, Classification_SrcPort, Classification_SrcTransportType, Classification_SrcUsernamePrefix, Classification_SrcHost, Classification_DestUsernamePrefix, Classification_DestHost, Classification_ActionType, Classification_SrcIPGroupName, Classification_DestRoutingPolicy, Classification_IpProfileName; [\Classification] For a description of the table, see "Configuring Classification Rules" on page 461.
Condition Table	
Condition Table configure voip > sbc routing condition-table [ConditionTable]	Defines SIP Message Condition rules. [ConditionTable] FORMAT ConditionTable_Index = ConditionTable_Condition, ConditionTable_Description; [\ConditionTable] For a description of the table, see "Configuring Message Condition Rules" on page 469.
SBC IP-to-IP Routing Table	
IP-to-IP Routing Table configure voip > sbc routing ip2ip- routing [IP2IPRouting]	Defines SBC IP-to-IP routing rules. The format of the ini file table parameter is as follows: [IP2IPRouting] FORMAT IP2IPRouting_Index = IP2IPRouting_RouteName, IP2IPRouting_RoutingPolicyName, IP2IPRouting_SrcIPGroupName, IP2IPRouting_SrcUsernamePrefix, IP2IPRouting_SrcHost, IP2IPRouting_DestUsernamePrefix, IP2IPRouting_DestHost, IP2IPRouting_RequestType, IP2IPRouting_MessageConditionName, IP2IPRouting_ReRouteIPGroupName, IP2IPRouting_Trigger, IP2IPRouting_CallSetupRulesSetId, IP2IPRouting_DestType, IP2IPRouting_DestIPGroupName, IP2IPRouting_DestSIPInterfaceName, IP2IPRouting_DestAddress, IP2IPRouting_DestPort, IP2IPRouting_DestTransportType, IP2IPRouting_AltRouteOptions, IP2IPRouting_GroupPolicy, IP2IPRouting_CostGroup, IP2IPRouting_DestTags, IP2IPRouting_SrcTags, IP2IPRouting_IPGroupSet;

Parameter	Description
	[\IP2IPRouting] For a description of the table, see "Configuring SBC IP-to-IP Routing Rules" on page 470.
IP Group Set Table	
IP Group Set [PGroupSet]	Defines IP Group Sets for call load-balancing. The format of the ini file table parameter is as follows: [IPGroupSet] FORMAT IPGroupSet_Index = IPGroupSet_Name, IPGroupSet_Policy; [\IPGroupSet] For a description of the table, see Configuring IP Group Sets on page 487.
IP Group Set Member Table	
IP Group Set Member [IPGroupSetMember]	Defines IP Groups for IP Group Sets for call load-balancing. The format of the ini file table parameter is as follows: [IPGroupSetMember] FORMAT IPGroupSetMember_Index = IPGroupSetMember_IPGroupSetId, IPGroupSetMember_IPGroupSetMemberIndex, IPGroupSetMember_IPGroupName, IPGroupSetMember_Weight; [\IPGroupSetMember] For a description of the table, see Configuring IP Group Sets on page 487.
Alternative Routing Reasons Table	
Alternative Routing Reasons configure voip > sbc routing sbc- alternative-routing-reasons [SBCAlternativeRoutingReasons]	Defines SBC alternative routing reason rules. The format of the ini file table parameter is as follows: [SBCAlternativeRoutingReasons] FORMAT SBCAlternativeRoutingReasons_Index = SBCAlternativeRoutingReasons_ReleaseCause; [\SBCAlternativeRoutingReasons] For a description of the table, see "Configuring SIP Response Codes for Alternative Routing Reasons" on page 482.
Inbound Manipulations Table	
Inbound Manipulations configure voip > sbc manipulation ip-inbound-manipulation [IPInboundManipulation]	Defines Inbound Manipulation rules. The format of the ini file table parameter is as follows: [IPInboundManipulation] FORMAT IPInboundManipulation_Index = IPInboundManipulation_ManipulationName IPInboundManipulation_IsAdditionalManipulation, IPInboundManipulation_ManipulatedURI, IPInboundManipulation_ManipulationPurpose, IPInboundManipulation_SrcIPGroupName, IPInboundManipulation_SrcUsernamePrefix, IPInboundManipulation_SrcHost, IPInboundManipulation_DestUsernamePrefix, IPInboundManipulation_DestHost,

Parameter	Description
	IPInboundManipulation_RequestType, IPInboundManipulation_RemoveFromLeft, IPInboundManipulation_RemoveFromRight, IPInboundManipulation_LeaveFromRight, IPInboundManipulation_Prefix2Add, IPInboundManipulation_Suffix2Add; [IPInboundManipulation] For a description of the table, see "Configuring IP-to-IP Inbound Manipulations" on page 493.
Outbound Manipulations Table	
Outbound Manipulations configure voip > sbc manipulation ip-outbound-manipulation [IPOutboundManipulation]	Defines outbound manipulation rules. The format of the ini file table parameter is as follows: [IPOutboundManipulation] FORMAT IPOutboundManipulation_Index = IPOutboundManipulation_ManipulationName, IPOutboundManipulation_RoutingPolicyName, IPOutboundManipulation_IsAdditionalManipulation, IPOutboundManipulation_SrcIPGroupName, IPOutboundManipulation_DestIPGroupName, IPOutboundManipulation_SrcUsernamePrefix, IPOutboundManipulation_SrcHost, IPOutboundManipulation_DestUsernamePrefix, IPOutboundManipulation_DestHost, IPOutboundManipulation_CallingNamePrefix, IPOutboundManipulation_MessageConditionName, IPOutboundManipulation_RequestType, IPOutboundManipulation_ReRouteIPGroupName, IPOutboundManipulation_Trigger, IPOutboundManipulation_ManipulatedURI, IPOutboundManipulation_RemoveFromLeft, IPOutboundManipulation_RemoveFromRight, IPOutboundManipulation_LeaveFromRight, IPOutboundManipulation_Prefix2Add, IPOutboundManipulation_Suffix2Add, IPOutboundManipulation_PrivacyRestrictionMode, IPOutboundManipulation_DestTags, IPOutboundManipulation_SrcTags; [IPOutboundManipulation] For a description of the table, see "Configuring IP-to-IP Outbound Manipulations" on page 497.
Routing Policies Table	
Routing Policies configure voip > sbc routing sbc- routing-policy [SBCRoutingPolicy]	Defines Routing Policies. The format of the ini file table parameter is as follows: [SBCRoutingPolicy] FORMAT SBCRoutingPolicy_Index = SBCRoutingPolicy_Name, SBCRoutingPolicy_LCREnable, SBCRoutingPolicy_LCRAverageCallLength, SBCRoutingPolicy_LCRDefaultCost, SBCRoutingPolicy_LdapServerGroupName; [SBCRoutingPolicy] For a description of the table, see "Configuring SBC Routing Policy Rules" on page 484.

Parameter	Description
Dial Plan Table	
Dial Plan configure voip > sbc dial-plan [DialPlans]	Defines the name of the Dial Plan. The format of the ini file table parameter is as follows: [DialPlan] FORMAT DialPlan_Index = DialPlan_Name; [\DialPlan] For a description of the table, see "Configuring Dial Plans" on page 503.
Dial Plan Rule Table	
Dial Plan Rule configure voip > sbc dial-plan-rule [DialPlanRule]	Defines the dial plan rules per Dial Plan. For a description of the table, see "Configuring Dial Plans" on page 503. Note: <ul style="list-style-type: none"> The table is hidden in the ini file. To configure Dial Plan rules from a file, see "Importing and Exporting Dial Plans" on page 507.
Malicious Signature Table	
Malicious Signature configure voip > sbc malicious-signature-database [MaliciousSignatureDB]	Defines the malicious signature patterns The format of the ini file table parameter is as follows: [MaliciousSignatureDB] FORMAT MaliciousSignatureDB_Index = MaliciousSignatureDB_Name, MaliciousSignatureDB_Pattern; [\MaliciousSignatureDB] For a description of the table, see "Configuring Malicious Signatures" on page 517.

55.11.1 Supplementary Services

The SBC and CRP supplementary services parameters are described in the table below.

Table 55-39: SBC and CRP Supplementary Services Parameters

Parameter	Description
Emergency Call Preemption Parameters For more information on SBC emergency call preemption, "Configuring Call Preemption for SBC Emergency Calls" on page 519.	
SBC Preemption Mode configure voip > sbc settings > sbc-preemption-mode [SBCPreemptionMode]	Enables SBC emergency call preemption. <ul style="list-style-type: none"> [0] Disable (default) [1] Enable
Emergency Message Condition configure voip > sbc settings > sbc-emerg-condition [SBCEmergencyCondition]	Defines the index of the Message Condition rule in the Message Conditions table that is used to identify emergency calls. Note: The device applies the rule only after call classification (but before inbound manipulation).

Parameter	Description
Emergency RTP DiffServ configure voip > sbc settings > sbc-emerg-rtp-diffserv [SBCEmergencyRTPDiffServ]	Defines DiffServ bits sent in the RTP for SBC emergency calls. The valid value is 0 to 63. The default is 46.
Emergency Signaling DiffServ configure voip > sbc settings > sbc-emerg-sig-diffserv [SBCEmergencySignalingDiffServ]	Defines DiffServ bits sent in SIP signaling messages for SBC emergency calls. This is included in the SIP Resource-Priority header. The valid value is 0 to 63. The default is 40.

55.12 IP Media Parameters

The IP media parameters are described in the table below.

Table 55-40: IP Media Parameters

Parameter	Description
IPMedia Detectors configure voip > media ipmedia > ipm-detectors-enable [EnableDSPIPMDetectors]	Enables the device's DSP detectors for detection features such as AMD. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable Note: <ul style="list-style-type: none"> ▪ For the parameter to take effect, a device reset is required. ▪ The DSP Detectors feature is available only if the device is installed with a License Key that includes this feature. For installing a License Key, see "License Key" on page 597.
Number of Media Channels configure voip > sbc settings > media-channels [MediaChannels]	Defines the maximum number of DSP channels allocated for various functionalities such as transcoding, . The default is 0. Note: <ul style="list-style-type: none"> ▪ For the parameter to take effect, a device reset is required. ▪ 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.
Automatic Gain Control (AGC) Parameters	
Enable AGC configure voip > media ipmedia > agc-enable [EnableAGC]	Global parameter enabling the AGC feature. Note: If the functionality is configured for a specific Tel Profile, the settings of the global parameter is ignored for calls associated with the Tel Profile. Enables the AGC mechanism. The AGC mechanism adjusts the level of the received signal to maintain a steady (configurable) volume level. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable For a description of AGC, see Automatic Gain Control (AGC)

Parameter	Description
	on page 195.
AGC Slope configure voip > media ipmedia > agc-gain-slope [AGCGainSlope]	Determines the AGC convergence rate: <ul style="list-style-type: none"> ▪ [0] 0 = 0.25 dB/sec ▪ [1] 1 = 0.50 dB/sec ▪ [2] 2 = 0.75 dB/sec ▪ [3] 3 = 1.00 dB/sec (default) ▪ [4] 4 = 1.25 dB/sec ▪ [5] 5 = 1.50 dB/sec ▪ [6] 6 = 1.75 dB/sec ▪ [7] 7 = 2.00 dB/sec ▪ [8] 8 = 2.50 dB/sec ▪ [9] 9 = 3.00 dB/sec ▪ [10] 10 = 3.50 dB/sec ▪ [11] 11 = 4.00 dB/sec ▪ [12] 12 = 4.50 dB/sec ▪ [13] 13 = 5.00 dB/sec ▪ [14] 14 = 5.50 dB/sec ▪ [15] 15 = 6.00 dB/sec ▪ [16] 16 = 7.00 dB/sec ▪ [17] 17 = 8.00 dB/sec ▪ [18] 18 = 9.00 dB/sec ▪ [19] 19 = 10.00 dB/sec ▪ [20] 20 = 11.00 dB/sec ▪ [21] 21 = 12.00 dB/sec ▪ [22] 22 = 13.00 dB/sec ▪ [23] 23 = 14.00 dB/sec ▪ [24] 24 = 15.00 dB/sec ▪ [25] 25 = 20.00 dB/sec ▪ [26] 26 = 25.00 dB/sec ▪ [27] 27 = 30.00 dB/sec ▪ [28] 28 = 35.00 dB/sec ▪ [29] 29 = 40.00 dB/sec ▪ [30] 30 = 50.00 dB/sec ▪ [31] 31 = 70.00 dB/sec
AGC Redirection configure voip > media ipmedia > agc-redirection [AGCRedirection]	Determines the AGC direction. <ul style="list-style-type: none"> ▪ [0] 0 = (Default) AGC works on signals from the TDM side. ▪ [1] 1 = AGC works on signals from the IP side.
AGC Target Energy configure voip > media ipmedia > agc-target-energy [AGCTargetEnergy]	Defines the signal energy value (dBm) that the AGC attempts to attain. The valid range is 0 to -63 dBm. The default is -19 dBm.
AGC Minimum Gain configure voip > media ipmedia > agc-min-gain [AGCMinGain]	Defines the minimum gain (in dB) by the AGC when activated. The range is 0 to -31. The default is -20. Note: For the parameter to take effect, a device reset is required.

Parameter	Description
AGC Maximum Gain configure voip > media ipmedia > agc-max-gain [AGCMaxGain]	Defines the maximum gain (in dB) by the AGC when activated. The range is 0 to 18. The default is 15. Note: For the parameter to take effect, a device reset is required.
Disable Fast Adaptation configure voip > media ipmedia > agc-disable-fast-adaptation [AGCDisableFastAdaptation]	Enables the AGC Fast Adaptation mode. <ul style="list-style-type: none"> ▪ [0] = Disable (default) ▪ [1] = Enable Note: For the parameter to take effect, a device reset is required.
Answering Machine Detector (AMD) Parameters For more information on AMD, see "Answering Machine Detection (AMD)" on page 192.	
Answer Machine Detector Sensitivity Parameter Suite configure voip > media ipmedia > amd-sensitivity-parameter-suit [AMDSensitivityParameterSuit]	Global parameter that defines the AMD Parameter Suite to use. You can also configure this functionality per specific calls, using IP Profiles (IpProfile_AMDSensitivityParameterSuit). For a detailed description of the parameter and for configuring this functionality in the IP Profiles table, see "Configuring IP Profiles" on page 388. Note: If this functionality is configured for a specific IP Profile, the settings of this global parameter is ignored for calls associated with the IP Profile.
Answer Machine Detector Sensitivity Level configure voip > media ipmedia > amd-sensitivity-level [AMDSensitivityLevel]	Global parameter that defines the AMD detection sensitivity level of the selected AMD Parameter Suite. You can also configure this functionality per specific calls, using IP Profiles (IpProfile_AMDSensitivityLevel). For a detailed description of the parameter and for configuring this functionality in the IP Profiles table, see "Configuring IP Profiles" on page 388. Note: If this functionality is configured for a specific IP Profile, the settings of this global parameter is ignored for calls associated with the IP Profile.
AMD Sensitivity File [AMDSensitivityFileName]	Defines the name of the AMD Sensitivity file that contains the AMD Parameter Suites. Note: <ul style="list-style-type: none"> ▪ This file must be in binary format (.dat). You can use the DConvert utility to convert the original file format from XML to .dat. ▪ You can load this file using the Web interface (see "Loading Auxiliary Files" on page 585).
[AMDSensitivityFileUrl]	Defines the URL path to the AMD Sensitivity file for downloading from a remote server.
[AMDMinimumVoiceLength]	Defines the AMD minimum voice activity detection duration (in 5-ms units). Voice activity duration below this threshold is ignored and considered as non-voice. The valid value range is 10 to 100. The default is 42 (i.e., 210 ms).
[AMDMaxGreetingTime]	Global parameter that defines the maximum duration that the device can take to detect a greeting message. You can also configure this functionality per specific calls, using IP Profiles (IpProfile_AMDMaxGreetingTime). For a detailed description of

Parameter	Description
	<p>the parameter and for configuring this functionality in the IP Profiles table, see "Configuring IP Profiles" on page 388.</p> <p>Note: If this functionality is configured for a specific IP Profile, the settings of this global parameter is ignored for calls associated with the IP Profile.</p>
[AMDMaxPostGreetingSilenceTime]	<p>Global parameter that defines the maximum duration of silence from after the greeting time is over (defined by AMDMaxGreetingTime) until the device's AMD decision. You can also configure this functionality per specific calls, using IP Profiles (IpProfile_AMDMaxPostSilenceGreetingTime). For a detailed description of the parameter and for configuring this functionality in the IP Profiles table, see "Configuring IP Profiles" on page 388.</p> <p>Note: If this functionality is configured for a specific IP Profile, the settings of this global parameter is ignored for calls associated with the IP Profile.</p>
[AMDTimeout]	<p>Defines the timeout (in msec) between receiving Connect messages from the Tel side and sending AMD results.</p> <p>The valid range is 1 to 30,000. The default is 2,000 (i.e., 2 seconds).</p>
<p>AMD Beep Detection Mode configure voip > sip-definition settings > amd-beep-detection [AMDBeepDetectionMode]</p>	<p>Determines the AMD beep detection mode. This mode detects the beeps played at the end of an answering machine message, by using the X-Detect header extension. The device sends a SIP INFO message containing the field values Type=AMD and SubType=Beep. This feature allows users of certain third-party, Application server to leave a voice message after an answering machine plays the "beep".</p> <ul style="list-style-type: none"> ▪ [0] Disabled (default) ▪ [1] Start After AMD ▪ [2] Start Immediately
<p>Answer Machine Detector Beep Detection Timeout configure voip > media ipmedia > amd-beep-detection-timeout [AMDBeepDetectionTimeout]</p>	<p>Defines the AMD beep detection timeout (i.e., the duration that the beep detector functions from when detection is initiated). This is used for detecting beeps at the end of an answering machine message.</p> <p>The valid value is in units of 100 milliseconds, from 0 to 1638. The default is 200 (i.e., 20 seconds).</p>
<p>Answer Machine Detector Beep Detection Sensitivity configure voip > media ipmedia > amd-beep-detection-sensitivity [AMDBeepDetectionSensitivity]</p>	<p>Defines the AMD beep detection sensitivity for detecting beeps at the end of an answering machine message.</p> <p>The valid value is 0 to 3, where 0 (default) is the least sensitive.</p>
<p>AMD Mode configure voip > sip-definition settings > amd-mode [AMDmode]</p>	<p>Global parameter that enables the device to disconnect the IP-to-Tel call upon detection of an answering machine on the Tel side. You can also configure this functionality per specific calls, using IP Profiles (IpProfile_AmdMode). For a detailed description of the parameter and for configuring this functionality in the IP Profiles table, see "Configuring IP Profiles" on page 388.</p> <p>Note: If this functionality is configured for a specific IP Profile,</p>

Parameter	Description
	the settings of this global parameter is ignored for calls associated with the IP Profile.

55.13 Services

55.13.1 SIP-based Media Recording Parameters

The SIP-based media recording parameters are described in the table below.

Table 55-41: SIP-based Media Recording Parameters

Parameter	Description
SIP Recording Application configure voip > sip-definition sip-recording settings > enable-sip-rec [EnableSIPRec]	Enables the SIP-based Media Recording feature: <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable Note: For the parameter to take effect, a device reset is required.
Recording Server (SRS) Destination Username configure voip > sip-definition sip-recording settings > siprec-server-dest-username [SIPRecServerDestUsername]	Defines the SIP user part for the recording server. This user part is added in the SIP To header of the INVITE message that the device sends to the recording server. The valid value is a string of up to 50 characters. By default, no user part is defined.
SIP Recording Rules Table	
SIP Recording Rules configure voip > sip-definition sip-recording sip-rec-routing [SIPRecRouting]	Defines SIP Recording Routing rules (for siprec). The format of the ini file table parameter is as follows: [SIPRecRouting] FORMAT SIPRecRouting_Index = SIPRecRouting_RecordedIPGroupName, SIPRecRouting_RecordedSourcePrefix, SIPRecRouting_RecordedDestinationPrefix, SIPRecRouting_PeerIPGroupName, SIPRecRouting_PeerTrunkGroupID, SIPRecRouting_Caller, SIPRecRouting_SRSIPGroupName; [\SIPRecRouting] For a description of the table, see "Configuring SIP Recording Rules" on page 215.

55.13.2 RADIUS and LDAP Parameters

55.13.2.1 General Parameters

The general RADIUS and LDAP parameters are described in the table below.

Table 55-42: General RADIUS and LDAP Parameters

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

Parameter	Description
Use Local Users Database configure system > mgmt-auth > use-local-users-db [MgmtUseLocalUsersDatabase]	<p>Defines when the device uses the Local Users table or an LDAP/RADIUS server for authenticating the login credentials (username-password) of users when logging into the device's management interface (e.g., Web or CLI).</p> <ul style="list-style-type: none"> ▪ [0] When No Auth Server Defined = (Default) The device authenticates the users using the Local Users table in the following scenarios: <ul style="list-style-type: none"> ✓ If no LDAP/RADIUS server is configured. ✓ If an LDAP/RADIUS server is configured, but connectivity with the server is down. If there is connectivity with the server, the device uses the server to authenticate the user. ▪ [1] Always = The device first attempts to authenticate the user using the Local Users table. If no user is found (based on the username-password combination), it attempts to authenticate the user using the LDAP/RADIUS server.
Behavior upon Authentication Server Timeout configure system > mgmt-auth > timeout-behavior [MgmtBehaviorOnTimeout]	<p>Defines the device's response when a connection timeout occurs with the LDAP/RADIUS server.</p> <ul style="list-style-type: none"> ▪ [0] Deny Access = User is denied access to the management platform. ▪ [1] Verify Access Locally = (Default) Device verifies the user's credentials in its Local Users table (local database). <p>Note: The parameter is applicable to LDAP- and RADIUS-based management-user login authentication.</p>
Default Access Level configure system > mgmt-auth > default-access-level [DefaultAccessLevel]	<p>Defines the default access level for the device when the LDAP/RADIUS response doesn't include an access level attribute for determining the user's management access level.</p> <p>The valid range is 0 to 255. The default is 200 (i.e., Security Administrator).</p> <p>Note: The parameter is applicable to LDAP- or RADIUS-based management-user login authentication and authorization.</p>

55.13.2.2 RADIUS Parameters

The RADIUS parameters are described in the table below.

Table 55-43: RADIUS Parameters

Parameter	Description
General RADIUS Parameters	
Enable RADIUS Access Control configure system > radius settings > enable [EnableRADIUS]	<p>Enables the RADIUS application.</p> <ul style="list-style-type: none"> ▪ [0] Disable (Default) ▪ [1] Enable <p>Note: For the parameter to take effect, a device reset is required.</p>
[RadiusTrafficType]	<p>Defines the device's network interface for communicating (RADIUS traffic) with the RADIUS server(s).</p> <ul style="list-style-type: none"> ▪ [0] OAMP (default)

Parameter	Description
	<ul style="list-style-type: none"> [1] Control <p>Note: If set to Control, only one Control interface must be configured in the IP Interfaces table; otherwise, RADIUS communication will fail.</p>
RADIUS VSA Vendor ID configure system > radius settings > vsa-vendor-id [RadiusVSAVendorID]	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.
[MaxRADIUSSessions]	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.
RADIUS Packets Retransmission [RADIUSRetransmission]	Defines the number of RADIUS retransmission retries when no response is received from the RADIUS server. See also the RadiusTo parameter. The valid range is 1 to 10. The default is 3.
RADIUS Response Time Out [RadiusTO]	Defines the time interval (in seconds) that the device waits for a response before it performs a RADIUS retransmission. See also the RADIUSRetransmission parameter. The valid range is 1 to 30. The default is 10.
RADIUS Accounting Parameters	
RADIUS Accounting Type configure voip > sip- definition settings > radius- accounting [RADIUSAccountingType]	Defines at what stage of the call that RADIUS accounting messages are sent to the RADIUS accounting server. <ul style="list-style-type: none"> [0] At Call Release = (Default) Sent at call release only. [1] At Connect & Release = Sent at call connect and release. [2] At Setup & Release = Sent at call setup and release.
AAA Indications configure system > cdr > aaa-indications [AAAIndications]	Enables the Authentication, Authorization and Accounting (AAA) indications. <ul style="list-style-type: none"> [0] None = (Default) No indications. [3] Accounting Only = Only accounting indications are used.
RADIUS User Authentication Parameters	
Use RADIUS for Web/Telnet Login configure system > radius settings > enable-mgmt- login [WebRADIUSLogin]	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. <ul style="list-style-type: none"> [0] Disable (default) [1] Enable <p>Note:</p> <ul style="list-style-type: none"> For RADIUS login authentication to function, you must also configure the EnableRADIUS parameter to 1 (Enable). 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 to force the use of HTTPS, since the transport is encrypted.
Password Local Cache Mode	Defines the device's mode of operation regarding the timer (configured by the parameter RadiusLocalCacheTimeout) that determines the

Parameter	Description
configure system > radius settings > local-cache-mode [RadiusLocalCacheMode]	validity of the username and password (verified by the RADIUS server). <ul style="list-style-type: none"> [0] Absolute Expiry Timer = When you access a Web page, the timeout doesn't reset, instead it continues decreasing. [1] Reset Timer Upon Access = (Default) Upon each access to a Web page, the timeout always resets (reverts to the initial value configured by RadiusLocalCacheTimeout).
Password Local Cache Timeout configure system > radius settings > local-cache-timeout [RadiusLocalCacheTimeout]	Defines the time (in seconds) the locally stored username and password (verified by the RADIUS server) are valid. When this time expires, the username 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"> [-1] = Never expires. [0] = Each request requires RADIUS authentication.
RADIUS VSA Access Level Attribute configure system > radius settings > vsa-access-level [RadiusVSAAccessAttribute]	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.
RADIUS Servers Table	
RADIUS Servers configure system > radius servers [RadiusServers]	Defines RADIUS servers. The format of the ini file table parameter is as follows: [RadiusServers] FORMAT RadiusServers_Index = RadiusServers_ServerGroup, RadiusServers_IPAddress, RadiusServers_AuthenticationPort, RadiusServers_AccountingPort, RadiusServers_SharedSecret; [\RadiusServers] For a detailed description of this table, see "Configuring RADIUS Servers" on page 219.

55.13.2.3 LDAP Parameters

The Lightweight Directory Access Protocol (LDAP) parameters are described in the table below.

Table 55-44: LDAP Parameters

Parameter	Description
LDAP Service configure system > ldap settings > ldap-service [LDAPServiceEnable]	Enables the LDAP feature. <ul style="list-style-type: none"> [0] Disable (default) [1] Enable Note: For the parameter to take effect, a device reset is required.
LDAP Authentication Filter configure system > ldap settings > auth-filter	Defines the LDAP search filter attribute for searching the login username in the directory's subtree for LDAP-based user authentication and authorization.

Parameter	Description
[LDAPAuthFilter]	You can use the dollar (\$) sign to represent the username. For example, if the parameter is set to "(sAMAccountName=*)" and the user logs in with the username "SueM", the LDAP query is run for sAMAccountName=SueM.
Use LDAP for Web > Telnet Login configure system > ldap settings > enable-mgmt-login [MgmtLDAPLogin]	Enables LDAP-based management-user login authentication and authorization. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable Note: For the parameter to take effect, a device reset is required.
[LDAPDebugMode]	Determines whether to enable the LDAP task debug messages. This is used for providing debug information regarding LDAP tasks. The valid value range is 0 to 3. The default is 0.
LDAP Numeric Attribute ldap-numeric-attr [LDAPNumericAttributes]	Defines up to five LDAP Attributes (separated by commas) for which the device employs LDAP query searches in the AD for numbers that may have characters between the digits. For more information, see "Enabling LDAP Searches for Numbers with Characters" on page 248.
MS LDAP OCS Number attribute name configure voip > sip-definition settings > ldap-ocs-nm-attr [MSLDAPOCSNumAttributeName]	Defines the name of the attribute that represents the user's Skype for Business number in the Microsoft AD database. The valid value is a string of up to 49 characters. The default is "msRTCSIP-Line".
MS LDAP PBX Number attribute name configure voip > sip-definition settings > ldap-pbx-nm-attr [MSLDAPPBXNumAttributeName]	Defines the name of the attribute that represents the user PBX number in the Microsoft AD database. The valid value is a string of up to 49 characters. The default is "telephoneNumber".
MS LDAP MOBILE Number attribute name configure voip > sip-definition settings > ldap-mobile-nm-attr [MSLDAPMobileNumAttributeName]	Defines the name of the attribute that represents the user Mobile number in the Microsoft AD database. The valid value is a string of up to 49 characters. The default is "mobile".
configure voip > sip-definition settings > ldap-private-nm-attr [MSLDAPPrivateNumAttributeName]	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, the parameter is not used as a search key. The default is "msRTCSIP-PrivateLine".
MS LDAP DISPLAY Name Attribute Name configure voip > sip-definition settings > ldap-display-nm-attr [MSLDAPDisplayNameAttributeName]	Defines the attribute name that represents the Calling Name in the AD for LDAP queries based on calling number. The valid value is a string of up to 49 characters. The default is "displayName".

Parameter	Description
configure voip > sip-definition settings > ldap-primary-key [MSLDAPPrimaryKey]	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.
configure voip > sip-definition settings > ldap-secondary-key [MSLDAPSecondaryKey]	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 configure system > ldap settings > ldap-cache-enable [LDAPCacheEnable]	Enables the LDAP cache service. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable Note: <ul style="list-style-type: none"> ▪ For the parameter to take effect, a device reset is required. ▪ For more information on LDAP caching, see "Configuring the Device's LDAP Cache" on page 238.
LDAP Servers Table	
LDAP Servers configure system > ldap ldap-configuration [LdapConfiguration]	Defines LDAP servers. The format of the ini file table parameter is as follows: [LdapConfiguration] FORMAT LdapConfiguration_Index = LdapConfiguration_Group, LdapConfiguration_LdapConfServerIp, LdapConfiguration_LdapConfServerPort, LdapConfiguration_LdapConfServerMaxRespondTime, LdapConfiguration_LdapConfServerDomainName, LdapConfiguration_LdapConfPassword, LdapConfiguration_LdapConfBindDn, LdapConfiguration_Interface, LdapConfiguration_MngmAuthAtt, LdapConfiguration_useTLS, LdapConfiguration_ConnectionStatus; [\LdapConfiguration] For a description of the table, see "Configuring LDAP Servers" on page 231.
LDAP Server Search Base DN Table	
LDAP Server Search Base DN Table configure system > ldap ldap-servers-search-dns [LdapServersSearchDNs]	Defines the full base path (i.e., distinguished name / DN) to the objects in the AD where the query is done, per LDAP server. The format of the ini file table parameter is as follows: [LdapServersSearchDNs] FORMAT LdapServersSearchDNs_Index = LdapServersSearchDNs_Base_Path, LdapServersSearchDNs_LdapConfigurationIndex, LdapServersSearchDNs_SearchDnInternalIndex; [\LdapServersSearchDNs] For a detailed description of the table, see "Configuring LDAP DN (Base Paths) per LDAP Server" on page 234.

Parameter	Description
Management LDAP Groups Table	
Management LDAP Groups Table configure system > ldap mgmt-ldap-groups [MgmtLDAPGroups]	Defines the users group attribute in the AD and corresponding management access level. The format of the ini file table parameter is as follows: [MgmtLDAPGroups] FORMAT MgmtLDAPGroups_Index = MgmtLDAPGroups_LdapConfigurationIndex, MgmtLDAPGroups_GroupIndex, MgmtLDAPGroups_Level, MgmtLDAPGroups_Group; [\MgmtLDAPGroups] For a description of the table, see "Configuring Access Level per Management Groups Attributes" on page 236.
LDAP Server Groups Table	
LDAP Server Groups Table configure system > ldap ldap-server-groups [LDAPServerGroups]	Defines LDAP Server Groups. The format of the ini file table parameter is as follows: [LdapServerGroups] FORMAT LdapServerGroups_Index = LdapServerGroups_Name, LdapServerGroups_ServerType, LdapServerGroups_SearchMethod, LdapServerGroups_CacheEntryTimeout, LdapServerGroups_CacheEntryRemovalTimeout, LdapServerGroups_SearchDnsMethod; [\LdapServerGroups] For a description of the table, see "Configuring LDAP Server Groups" on page 228.

55.13.3 Least Cost Routing Parameters

The Least Cost Routing (LCR) parameters are described in the table below.

Table 55-45: LCR Parameters

Parameter	Description
Cost Groups Table configure voip > sip-definition least-cost-routing cost-group [CostGroupTable]	Defines 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). [CostGroupTable] FORMAT CostGroupTable_Index = CostGroupTable_CostGroupName, CostGroupTable_DefaultConnectionCost, CostGroupTable_DefaultMinuteCost; [\CostGroupTable] For example: CostGroupTable 2 = "Local Calls", 2, 1; For a description of the table, see "Configuring Cost Groups" on page 256.
Cost Groups > Time Band Table configure voip > sip-definition least-cost-routing	Defines time bands and associates them with Cost Groups. [CostGroupTimebands] FORMAT CostGroupTimebands_TimebandIndex = CostGroupTimebands_StartTime, CostGroupTimebands_EndTime,

Parameter	Description
cost-group-time-bands [CostGroupTimebands]	CostGroupTimebands_ConnectionCost, CostGroupTimebands_MinuteCost; [CostGroupTimebands] For a description of the table, see "Configuring Time Bands for Cost Groups" on page 257.

55.13.4 Call Setup Rules Parameters

The Call Setup Rules parameters are described in the table below.

Table 55-46: Call Setup Rules Parameters

Parameter	Description
Call Setup Rules configure voip > message call-setup-rules [CallSetupRules]	Defines Call Setup Rules that the device runs at call setup for LDAP-based routing and other advanced routing logic requirements including manipulation. [CallSetupRules] FORMAT CallSetupRules_Index = CallSetupRules_RulesSetID, CallSetupRules_QueryType, CallSetupRules_QueryTarget, CallSetupRules_AttributesToQuery, CallSetupRules_AttributesToGet, CallSetupRules_RowRole, CallSetupRules_Condition, CallSetupRules_ActionSubject, CallSetupRules_ActionType, CallSetupRules_ActionValue; [\CallSetupRules] For a description of the table, see "Configuring Call Setup Rules" on page 370.

55.13.5 HTTP-based Services

The HTTP-based service parameters are described in the table below.

Table 55-47: HTTP-based Service Parameters

Parameter	Description
Topology Status configure system > http-services > routing-server- group-status [RoutingServerGroupStatus]	Enables the reporting of the device's topology status (using the REST TopologyStatus API command) to HTTP remote hosts. <ul style="list-style-type: none"> [0] Disable (default) [1] Enable For more information, see "Configuring HTTP Services" on page 259.
Remote Web Services Table	
Remote Web Services configure system > http- services > http-remote- services [HTTPRemoteServices]	Defines remote Web services. The format of the ini file table parameter is as follows: [HTTPRemoteServices] FORMAT HTTPRemoteServices_Index = HTTPRemoteServices_Name, HTTPRemoteServices_Path, HTTPRemoteServices_HTTPType, HTTPRemoteServices_Policy, HTTPRemoteServices_LoginNeeded,

Parameter	Description
	HTTPRemoteServices_PersistentConnection, HTTPRemoteServices_NumOfSockets, HTTPRemoteServices_AuthUserName, HTTPRemoteServices_AuthPassword, HTTPRemoteServices_TLSContext, HTTPRemoteServices_VerifyCertificate, HTTPRemoteServices_TimeOut, HTTPRemoteServices_KeepAliveTimeOut, HTTPRemoteServices_ServiceStatus; [HTTPRemoteServices] For a description of the table, see "Configuring Remote Web Services" on page 259.
HTTP Remote Hosts Table	
HTTP Remote Hosts configure system > http-services > http-remote-hosts [HTTPRemoteHosts]	Defines remote HTTP hosts per remote Web service. The format of the ini file table parameter is as follows: [HTTPRemoteHosts] FORMAT HTTPRemoteHosts_Index = HTTPRemoteHosts_HTTPRemoteServiceIndex, HTTPRemoteHosts_RemoteHostIndex, HTTPRemoteHosts_Name, HTTPRemoteHosts_Address, HTTPRemoteHosts_Port, HTTPRemoteHosts_Interface, HTTPRemoteHosts_HTTPTransportType, HTTPRemoteHosts_HostStatus; [HTTPRemoteHosts] For a description of the table, see "Configuring Remote HTTP Hosts" on page 263.

55.13.6 HTTP Proxy Parameters

The HTTP Proxy service parameters are described in the table below.

Table 55-48: HTTP Proxy Service Parameters

Parameter	Description
HTTP Proxy Application configure network > http-proxy settings > http-proxy-app [HTTPProxyApplication]	Enables the HTTP Proxy application. <ul style="list-style-type: none"> ▪ [0] Disable (default) ▪ [1] Enable Note: For the parameter to take effect, a device reset is required.
HTTP Interfaces Table	
HTTP Interfaces configure network > http-proxy > http-interface [HTTPInterface]	Defines local listening interfaces for receiving HTTP/S requests from Web clients for HTTP/S-based services. The format of the ini file table parameter is as follows: [HTTPInterface] FORMAT HTTPInterface_Index = HTTPInterface_InterfaceName, HTTPInterface_NetworkInterface, HTTPInterface_Protocol, HTTPInterface_Port, HTTPInterface_TLSContext, HTTPInterface_VerifyCert; [\HTTPInterface] For a description of the table, see "Configuring HTTP Interfaces" on

Parameter	Description
	page 270.
HTTP Proxy Services Table	
HTTP Proxy Services configure network > http-proxy http-proxy- serv [HTTPProxyService]	Defines HTTP Proxy based services. The format of the ini file table parameter is as follows: [HTTPProxyService] FORMAT HTTPProxyService_Index = HTTPProxyService_ServiceName, HTTPProxyService_ListeningInterface, HTTPProxyService_URLPrefix, HTTPProxyService_KeepAliveMode; [\HTTPProxyService] For a description of the table, see "Configuring HTTP Proxy Services" on page 272.
HTTP Proxy Hosts Table	
HTTP Proxy Hosts configure network > http-proxy http-proxy- host [HTTPProxyHost]	Defines HTTP Proxy hosts. The table is a "child" of the HTTP Proxy Services table (HTTPProxyService). An HTTP Proxy Host represents the HTTP-based managed equipment (e.g., IP Phone). The format of the ini file table parameter is as follows: [HTTPProxyHost] FORMAT HTTPProxyHost_Index = HTTPProxyHost_HTTPProxyServiceId, HTTPProxyHost_HTTPProxyHostId, HTTPProxyHost_NetworkInterface, HTTPProxyHost_IpAddress, HTTPProxyHost_Protocol, HTTPProxyHost_Port, HTTPProxyHost_TLSContext, HTTPProxyHost_VerifyCert; [\HTTPProxyHost] For a description of the table, see "Configuring HTTP Proxy Hosts" on page 273.
EMS Services Table	
EMS Services configure network > http-proxy ems-serv [EMSService]	Defines an HTTP-based EMS Service so that the device can act as an HTTP Proxy that enables AudioCodes EMS to manage AudioCodes equipment (such as IP Phones) over HTTP when the equipment is located behind NAT (e.g., in the LAN) and EMS is located in a public domain (e.g., in the WAN). The format of the ini file table parameter is as follows: [EMSService] FORMAT EMSService_Index = EMSService_ServiceName, EMSService_PrimaryServer, EMSService_SecondaryServer, EMSService_DeviceLoginInterface, EMSService_EMSServiceInterface; [\EMSService] For a description of the table, see "Configuring an HTTP-based EMS Service" on page 275.

This page is intentionally left blank.

56 Channel Capacity

The following below lists the maximum capacity figures for SIP signaling, media sessions, and registered users.

Table 56-1: Maximum Signaling, Media Sessions and Registered Users

Product		Signaling Sessions	Media Sessions			Registered Users	
			RTP-RTP or TDM-RTP	SRTP-RTP or TDM-SRTP	Codec Transcoding		
Mediant SE SBC	DL320e G8 4-cores 3.1 GHz 16 GB RAM	15,000	10,000	6,500	N/A	75,000	
	DL360p G8 20-cores 2.8 GHz 64 GB RAM	24,000	16,000	12,000	N/A	120,000	
	- or - DL360 G9 8-cores 2.6 GHz 32 GB RAM	24,000	24,000	12,000	N/A	0	
Mediant VE SBC	VMware	1 vCPU, 2 GB RAM	250	250	250	N/A	1,000
		1/2/4 vCPU, 8 GB RAM	3,000	3,000	2,000	<ul style="list-style-type: none"> 1 vCPU: N/A 2 vCPU: 2-vCPU Mediant VE SBC on page 847 4 vCPU: 4-vCPU Mediant VE SBC on page 848 	15,000
		4/8 vCPU 16 GB RAM	9,000	6,000	5,000	<ul style="list-style-type: none"> See 8-vCPU Mediant VE SBC on page 851 	75,000
	KVM	1 vCPU 2 GB RAM	250	250	250	N/A	1,000
		1/2/4 vCPU 4 GB RAM	1,800	1,800	1,400	<ul style="list-style-type: none"> 1 vCPU: N/A 2 vCPU: 2-vCPU Mediant VE SBC on page 847 4 vCPU: 4-vCPU Mediant VE SBC on page 848 	9,000
		4/8 vCPU 16 GB RAM	4,000	2,700	2,700	See 8-vCPU Mediant VE SBC on page 851	75,000
		8 vCPU 64 GB RAM SR-IOV Intel NICs	10,000	10,000	10,000	N/A	75,000
	Hyper-V	1 vCPU 2 GB RAM	250	250	250	N/A	1,000
		1/2/4 vCPU	900	600	600	<ul style="list-style-type: none"> 1 vCPU: N/A 	10,000

Product			Signaling Sessions	Media Sessions			Registered Users
				RTP-RTP or TDM-RTP	SRTP-RTP or TDM-SRTP	Codec Transcoding	
		4 GB RAM				<ul style="list-style-type: none"> ▪ 2 vCPU: 2-vCPU Mediant VE SBC on page 853 ▪ 4 vCPU: 4-vCPU Mediant VE SBC on page 855 	
	AWS / EC2	c4.2xlarge	2,000	2,000	2,000	See Table 56-6	20,000

Note:

- Installation and use of voice coders is subject to obtaining the appropriate license and royalty payments.
- The figures listed in the table are accurate at the time of publication of this document. However, these figures may change due to a later software update. For the latest figures, please contact your AudioCodes sales representative.
- *Registered Users* is the maximum number of users that can be registered with the device. This applies to the supported application (SBC or CRP).
- The capacity figures for Mediant VE are for running on the recommended platforms only, when there are no other virtual machines (VM) running on these platforms.
- Regarding signaling, media, and transcoding session resources:
 - ✓ A signaling session is a SIP dialog session between two SIP entities, traversing the SBC and using one signaling session resource.
 - ✓ A media session is an audio (RTP or SRTP), fax (T.38), or video session between two SIP entities, traversing the SBC and using one media session resource.
 - ✓ In case of direct media (i.e., anti-tromboning / Non-Media Anchoring), where only SIP signaling traverses the SBC and media flows directly between the SIP entities, only a signaling session resource is used. Thus, for products with a greater signaling session capacity than media, even when media session resources have been exhausted, additional signaling sessions can still be handled for direct-media calls.
 - ✓ For call sessions requiring transcoding, one transcoding session resource is also used. For example, for a non-direct media call in which one leg uses G.711 and the other leg G.729, one signaling resource, one media session resource, and one transcoding session resource is used.
- The capacity figures for Mediant VE are for VMware.



56.1 Mediant VE SBC

The maximum number of supported SBC sessions is listed in "Channel Capacity" on page 845. These SBC sessions also support SRTP and RTCP XR. When DSP capabilities are required, the number of sessions that can use DSP capabilities is reduced, as shown in the tables in this section.

56.1.1 Mediant VE SBC for KVM and VMware Hypervisors

The following tables list maximum channel capacity for Mediant VE SBC 2.8 GHz running on KVM or VMware hypervisors.

56.1.1.1 2-vCPU Mediant VE SBC

The following table lists maximum channel capacity for the 2-vCPU (1 vCPU reserved for DSP) Mediant VE SBC.

Table 56-2: Channel Capacity for 2-vCPU Mediant VE SBC on KVM/VMware

Session Coders		Number of Sessions	
From Coder Profile	To Coder	Extended	Basic
1	Profile 1	200	250
2	Profile 1	75	125
2	Profile 2	50	75
1	Profile 2 + AMR-NB / G.722	75	100
2	Profile 2 + AMR-NB / G.722	50	75
1	Profile 2 + AMR-WB	25	25
2	Profile 2 + AMR-WB	25	25
1	Profile 2 + SILK-NB	75	100
2	Profile 2 + SILK-NB	50	75
1	Profile 2 + SILK-WB	50	50
2	Profile 2 + SILK-WB	25	50
1	Profile 2 + Opus-NB	50	75
2	Profile 2 + Opus-NB	25	50
1	Profile 2 + Opus-WB	25	50
2	Profile 2 + Opus-WB	25	25



Note:

- *Profile 1:* G.711 at 20ms only, without T.38 support.
- *Profile 2:* G.711, G.726, G.729, G.723.1, T.38.
- *Basic:* excludes in-band signaling (in voice channel), VAD, Silence Suppression and fax detection.
- *Extended:* includes in-band signaling (in voice channel), VAD, Silence Suppression and fax detection
- Acoustic Echo Suppressor may reduce capacity. For more information, contact your AudioCodes sales representative.

The table below lists the maximum number of concurrent sessions per detection feature. The figures are based on the following assumptions:

- Timeout for fax detection is 10 seconds (default)
- Call duration is 100 seconds
- Fax detection is required on both legs of the SBC call
- Answer Detection (AD), Answering Machine Detection (AMD), Beep Detection, and Call Progress Tone Detection (CP) is only on one leg of the SBC call (should this not be the case, figures will be reduced)
- Sessions are only for forwarding sessions (i.e., no transcoding)

Table 56-3: Channel Capacity per Detection Feature for 2-vCPU Mediant VE SBC on KVM/VMware

Special Detection Features	Number of Sessions
Fax Detection	2,400
AD/AMD/Beep Detection	2,400
CP Detection	2,400
Jitter Buffer	200

56.1.1.2 4-vCPU Mediant VE SBC

The following table lists maximum channel capacity for the 4-vCPU (3 vCPUs reserved for DSP) Mediant VE SBC.

Table 56-4: Channel Capacity for 4-vCPU Mediant VE SBC on KVM/VMware

Session Coders		Number of Sessions	
From Coder Profile	To Coder	Extended	Basic
1	Profile 1	600	750
2	Profile 1	275	375
2	Profile 2	175	250
1	Profile 2 + AMR-NB / G.722	250	325
2	Profile 2 + AMR-NB / G.722	175	225
1	Profile 2 + AMR-WB	100	100

Session Coders		Number of Sessions	
From Coder Profile	To Coder	Extended	Basic
2	Profile 2 + AMR-WB	75	75
1	Profile 2 + SILK-NB	225	300
2	Profile 2 + SILK-NB	150	225
1	Profile 2 + SILK-WB	150	175
2	Profile 2 + SILK-WB	100	150
1	Profile 2 + Opus-NB	175	250
2	Profile 2 + Opus-NB	125	175
1	Profile 2 + Opus-WB	125	150
2	Profile 2 + Opus-WB	100	125

Note:

- *Profile 1*: G.711 at 20ms only, without T.38 support.
- *Profile 2*: G.711, G.726, G.729, G.723.1, T.38.
- *Basic*: excludes in-band signaling (in voice channel), VAD, Silence Suppression and fax detection.
- *Extended*: includes in-band signaling (in voice channel), VAD, Silence Suppression and fax detection
- Acoustic Echo Suppressor may reduce capacity. For more information, contact your AudioCodes sales representative.

The table below lists the maximum number of concurrent sessions per detection feature. The figures are based on the following assumptions:

- Timeout for fax detection is 10 seconds (default)
- Call duration is 100 seconds
- Fax detection is required on both legs of the SBC call
- Answer Detection (AD), Answering Machine Detection (AMD), Beep Detection, and Call Progress Tone Detection (CP) is only on one leg of the SBC call (should this not be the case, figures will be reduced)
- Sessions are only for forwarding sessions (i.e., no transcoding)

Table 56-5: Channel Capacity per Detection Feature for 4-vCPU Mediant VE SBC on KVM/VMware

Special Detection Features	Number of Sessions
Fax Detection	7,200
AD/AMD/Beep Detection	7,200
CP Detection	7,200
Jitter Buffer	650

56.1.1.3 Amazon AWS EC2

The following table lists maximum channel capacity for Mediant VE SBC on the Amazon EC2 platform.

Table 56-6: Channel Capacity for Mediant VE SBC on Amazon EC2

Session Coders		Number of Sessions	
From Coder Profile	To Coder	Extended	Basic
1	Profile 1	600	750
2	Profile 1	275	375
2	Profile 2	175	250
1	Profile 2 + AMR-NB / G.722	250	325
2	Profile 2 + AMR-NB / G.722	175	225
1	Profile 2 + AMR-WB	100	100
2	Profile 2 + AMR-WB	75	75
1	Profile 2 + SILK-NB	225	300
2	Profile 2 + SILK-NB	150	225
1	Profile 2 + SILK-WB	150	175
2	Profile 2 + SILK-WB	100	150
1	Profile 2 + Opus-NB	175	250
2	Profile 2 + Opus-NB	125	175
1	Profile 2 + Opus-WB	125	150
2	Profile 2 + Opus-WB	100	125

Notes:

- *Profile 1*: G.711 at 20ms only, without T.38 support.
- *Profile 2*: G.711, G.726, G.729, G.723.1, T.38.
- *Basic*: excludes in-band signaling (in voice channel), VAD, Silence Suppression and fax detection.
- *Extended*: includes in-band signaling (in voice channel), VAD, Silence Suppression and fax detection
- Acoustic Echo Suppressor may reduce capacity. For more information, contact your AudioCodes sales representative.



The table below lists the maximum number of concurrent sessions per detection feature. The figures are based on the following assumptions:

- Timeout for fax detection is 10 seconds (default)
- Call duration is 100 seconds
- Fax detection is required on both legs of the SBC call
- Answer Detection (AD), Answering Machine Detection (AMD), Beep Detection, and Call Progress Tone Detection (CP) is only on one leg of the SBC call (should this not be the case, figures will be reduced)
- Sessions are only for forwarding sessions (i.e., no transcoding)

Table 56-7: Channel Capacity per Detection Feature for Mediant VE SBC on Amazon EC2

Special Detection Features	Number of Sessions
Fax Detection	2,000
AD/AMD/Beep Detection	2,000
CP Detection	2,000
Jitter Buffer	650

56.1.1.4 8-vCPU Mediant VE SBC

The following table lists maximum channel capacity for the 8-vCPU (4 vCPUs reserved for DSP) Mediant VE SBC.

Table 56-8: Channel Capacity for 8-vCPU Mediant VE SBC on KVM/VMware

Session Coders		Number of Sessions	
From Coder Profile	To Coder	Extended	Basic
1	Profile 1	800	1,000
2	Profile 1	375	500
2	Profile 2	250	350
1	Profile 2 + AMR-NB / G.722	350	450
2	Profile 2 + AMR-NB / G.722	225	300
1	Profile 2 + AMR-WB	125	150
2	Profile 2 + AMR-WB	100	125
1	Profile 2 + SILK-NB	300	425
2	Profile 2 + SILK-NB	200	300
1	Profile 2 + SILK-WB	200	225
2	Profile 2 + SILK-WB	150	200
1	Profile 2 + Opus-NB	225	325
2	Profile 2 + Opus-NB	175	250
1	Profile 2 + Opus-WB	150	200
2	Profile 2 + Opus-WB	125	175



Note:

- *Profile 1:* G.711 at 20ms only, without T.38 support.
- *Profile 2:* G.711, G.726, G.729, G.723.1, T.38.
- *Basic:* excludes in-band signaling (in voice channel), VAD, Silence Suppression and fax detection.
- *Extended:* includes in-band signaling (in voice channel), VAD, Silence Suppression and fax detection
- Acoustic Echo Suppressor may reduce capacity. For more information, contact your AudioCodes sales representative.

The table below lists the maximum number of concurrent sessions per detection feature. The figures are based on the following assumptions:

- Timeout for fax detection is 10 seconds (default)
- Call duration is 100 seconds
- Fax detection is required on both legs of the SBC call
- Answer Detection (AD), Answering Machine Detection (AMD), Beep Detection, and Call Progress Tone Detection (CP) is only on one leg of the SBC call (should this not be the case, figures will be reduced)
- Sessions are only for forwarding sessions (i.e., no transcoding)

Table 56-9: Channel Capacity per Detection Feature for 8-vCPU Mediant VE SBC on KVM/VMware

Special Detection Features	Number of Sessions
Fax Detection	9,600
AD/AMD/Beep Detection	9,600
CP Detection	9,600
Jitter Buffer	875

56.1.2 Mediant VE SBC for Hyper-V Hypervisor

The following tables lists maximum channel capacity for Mediant VE SBC 2.1 GHz running on Hyper-V hypervisor.

56.1.2.1 2-vCPU Mediant VE SBC

The following table lists maximum channel capacity for the 2-vCPU (1 vCPU reserved for DSP) Mediant VE SBC.

Table 56-10: Channel Capacity for 2-vCPU Mediant VE SBC on Hyper-V

Session Coders		Number of Sessions	
From Coder Profile	To Coder	Extended	Basic
1	Profile 1	150	175
2	Profile 1	50	75
2	Profile 2	25	50
1	Profile 2 + AMR-NB / G.722	50	75
2	Profile 2 + AMR-NB / G.722	25	50
1	Profile 2 + AMR-WB	25	25
2	Profile 2 + AMR-WB	0	25
1	Profile 2 + SILK-NB	50	75
2	Profile 2 + SILK-NB	25	50
1	Profile 2 + SILK-WB	25	25
2	Profile 2 + SILK-WB	25	25
1	Profile 2 + Opus-NB	25	50
2	Profile 2 + Opus-NB	25	25
1	Profile 2 + Opus-WB	25	25
2	Profile 2 + Opus-WB	25	25

Note:

- *Profile 1*: G.711 at 20ms only, without T.38 support.
- *Profile 2*: G.711, G.726, G.729, G.723.1, T.38.
- *Basic*: excludes in-band signaling (in voice channel), VAD, Silence Suppression and fax detection.
- *Extended*: includes in-band signaling (in voice channel), VAD, Silence Suppression and fax detection
- Acoustic Echo Suppressor may reduce capacity. For more information, contact your AudioCodes sales representative.



The table below lists the maximum number of concurrent sessions per detection feature. The figures are based on the following assumptions:

- Timeout for fax detection is 10 seconds (default)
- Call duration is 100 seconds
- Fax detection is required on both legs of the SBC call
- Answer Detection (AD), Answering Machine Detection (AMD), Beep Detection, and Call Progress Tone Detection (CP) is only on one leg of the SBC call (should this not be the case, figures will be reduced)
- Sessions are only for forwarding sessions (i.e., no transcoding)

Table 56-11: Channel Capacity per Detection Feature for 2-vCPU Mediant VE SBC on Hyper-V

Special Detection Features	Number of Sessions
Fax Detection	1,800
AD/AMD/Beep Detection	1,800
CP Detection	1,800
Jitter Buffer	150

56.1.2.2 4-vCPU Mediant VE SBC

The following table lists maximum channel capacity for the 4-vCPU (3 vCPUs reserved for DSP) Mediant VE SBC.

Table 56-12: Channel Capacity for 4-vCPU Mediant VE SBC on Hyper-V

Session Coders		Number of Sessions	
From Coder Profile	To Coder	Extended	Basic
1	Profile 1	450	550
2	Profile 1	200	275
2	Profile 2	125	175
1	Profile 2 + AMR-NB / G.722	175	250
2	Profile 2 + AMR-NB / G.722	125	175
1	Profile 2 + AMR-WB	75	75
2	Profile 2 + AMR-WB	50	75
1	Profile 2 + SILK-NB	150	225
2	Profile 2 + SILK-NB	100	150
1	Profile 2 + SILK-WB	100	125
2	Profile 2 + SILK-WB	75	100
1	Profile 2 + Opus-NB	125	175
2	Profile 2 + Opus-NB	100	125
1	Profile 2 + Opus-WB	75	100
2	Profile 2 + Opus-WB	75	75



Note:

- *Profile 1*: G.711 at 20ms only, without T.38 support.
- *Profile 2*: G.711, G.726, G.729, G.723.1, T.38.
- *Basic*: excludes in-band signaling (in voice channel), VAD, Silence Suppression and fax detection.
- *Extended*: includes in-band signaling (in voice channel), VAD, Silence Suppression and fax detection
- Acoustic Echo Suppressor may reduce capacity. For more information, contact your AudioCodes sales representative.

The table below lists the maximum number of concurrent sessions per detection feature. The figures are based on the following assumptions:

- Timeout for fax detection is 10 seconds (default)
- Call duration is 100 seconds
- Fax detection is required on both legs of the SBC call
- Answer Detection (AD), Answering Machine Detection (AMD), Beep Detection, and

Call Progress Tone Detection (CP) is only on one leg of the SBC call (should this not be the case, figures will be reduced)

- Sessions are only for forwarding sessions (i.e., no transcoding)

Table 56-13: Channel Capacity per Detection Feature for 4-vCPU Mediant VE SBC on Hyper-V

Special Detection Features	Number of Sessions
Fax Detection	5,400
AD/AMD/Beep Detection	5,400
CP Detection	5,400
Jitter Buffer	500

56.2 Mediant SE SBC



Note: Mediant SE SBC does not implement digital signal processing (DSP). Therefore, it supports only SBC functionalities that do not require media signal processing

57 Technical Specifications

The device's technical specifications are listed in the table below.



Note:

- 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 57-1: Technical Specifications

Function	Specification
Security	
Access Control	DoS/DDoS line rate protection, bandwidth throttling, dynamic blacklisting
VoIP Firewall	RTP pinhole management, rogue RTP detection and prevention, SIP message policy, advanced RTP latching
Encryption and Authentication	TLS, DTLS, SRTP, HTTPS, SSH, client/server SIP Digest authentication, RADIUS Digest
Privacy	Topology hiding, user privacy
Traffic Separation	VLAN/physical interface separation for multiple media, control and OAMP interfaces
Intrusion Detection System	Detection and prevention of VoIP attacks, theft of service and unauthorized access
Interoperability	
SIP B2BUA	Full SIP transparency, mature & broadly deployed SIP stack, stateful proxy mode
SIP Interworking	3xx redirect, REFER, PRACK, session timer, early media, call hold, delayed offer
Registration and Authentication	User registration restriction control, registration and authentication on behalf of users, SIP authentication server for SBC users
Transport Mediation	SIP over UDP/TCP/TLS/WebSocket, IPv4-IPv6, RTP-SRTP (SDS/DTLS)
Message Manipulation	Ability to add/modify/delete SIP headers and message body using advanced regular expressions (regex)
URI and Number Manipulations	URI user and host name manipulations, ingress and egress digit manipulation
Transcoding and Vocoders	Coder normalization including transcoding, coder enforcement and re-prioritization, extensive vocoder support: G.711, G.723.1, G.726, G.729, GSM-FR, AMR-NB/WB, SILK-NB/WB, Opus-NB/WB
Signal Conversion	DTMF/RFC 2833/SIP, T.38 fax, packet-time conversion
WebRTC Controller	Interworking between WebRTC devices and SIP networks Supports WebSocket, Opus, VP8 video coder, lite ICE, DTLS, RTP multiplexing, secure RTCP with feedback

Function	Specification
NAT	Local and far-end NAT traversal for support of remote workers
Voice Quality and SLA	
Call Admission Control	Based on bandwidth, session establishment rate, number of connections/registrations
Packet Marking	802.1p/Q VLAN tagging, DiffServ, TOS
Standalone Survivability	Maintain local calls in the event of WAN failure.
Impairment Mitigation	Packet Loss Concealment, Dynamic Programmable Jitter Buffer, Silence Suppression/Comfort Noise Generation, RTP redundancy, broken connection detection
Voice Enhancement	Transrating, RTCP-XR, acoustic echo cancellation, replacing voice profile due to impairment detection, fixed and dynamic voice gain control
Direct Media (No Media Anchoring)	Hair-pinning of local calls to avoid unnecessary media delays and bandwidth consumption
Voice Quality Monitoring	RTCP-XR, AudioCodes Session Experience Manager (SEM)
High Availability (Redundancy)	SBC high availability with two-box redundancy, active calls preserved
Quality of Experience	Access control and media quality enhancements based on QoE and bandwidth utilization
Test Agent	Ability to remotely verify connectivity, voice quality and SIP message flow between SIP UAs
SIP Routing	
Routing Methods	Request URL, IP address, FQDN, ENUM, advanced LDAP, third-party routing control through REST API
Advanced Routing Criteria	QoE, bandwidth, SIP message (SIP request, coder type, etc.), Layer-3 parameters
Redundancy	Detection of proxy failures and subsequent routing to alternative proxies
Routing Features	Least-cost routing, call forking, load balancing, E911 gateway support, emergency call detection and prioritization
SIPRec	IETF standard SIP recording interface
Management	
OAM&P	Browser-based GUI, CLI, SNMP, EMS, INI Configuration file, REST API
Multi Tenancy	Advanced multi-tenant SBC partitioning.
Mediant VE SBC - Hardware Requirements	
Refer to the <i>Mediant Virtual Edition SBC Installation Manual</i> .	
Mediant SE SBC - Hardware Requirements	
Refer to the <i>Mediant Server Edition SBC Installation Manual</i> .	

This page is intentionally left blank.

International Headquarters

1 Hayarden Street,
Airport City
Lod 7019900, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.

27 World's Fair Drive,
Somerset, NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: www.audiocodes.com/info

Website: www.audiocodes.com



Document #: LTRT-41866

